Ivanti Patch for Windows® Servers

Quick Start Guide

Copyright and Trademarks

Document Information and Print History

Document number: N/A

Date	Version	Description
October 2011	VMware vCenter Protect 8.0	Initial release of the Vmware vCenter Protect Quick Start Guide
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 Nav pane and menu changes. Add Virtual Inventory feature.
April 2014	Shavlik Protect 9.1	Update Web links and system requirements.
September 2015	Shavlik Protect 9.2	Update to match user interface changes.
Fall 2016	Shavlik Protect 9.3	Remove references to AV.
April 2017	Ivanti Patch for Windows® Servers 9.3	Rebrand to Ivanti.

Table of Contents

This page intentionally left blank.

The document is designed for duplex printing.

WELCOME

Thank you for choosing Ivanti Patch for Windows® Servers, a unified IT management platform used for managing and protecting Wndows-based machines and VMware ESXi hypervisors. Ivanti Patch for Windows® Servers provides you with one centralized and common interface that you can use to perform several essential IT management functions, including patch management, asset inventory, power management, virtualization management, IT management tools, extensive reporting, and more.

Ivanti Patch for Windows® Servers is available within two different product bundles.

- **Ivanti Patch for Windows® Servers Standard:** This is the basic product offering that includes patch management, asset inventory and a limited number of scripts for IT management.
- **Ivanti Patch for Windows® Servers Advanced:** This is the full-featured product offering that includes patch management, asset inventory, power management and full ITScripts capabilities.

To quickly get you up and running with Ivanti Patch for Windows® Servers we have created this quick start guide. To learn how to use the product simply follow the directions in this document.

Beyond This Quick Start Guide

If after using this quick start guide you are interested in learning even more about Ivanti Patch for Windows® Servers, go to the Ivanti Help channel on YouTube:

https://www.youtube.com/channel/UCVSRxZB9ZDCiwwv4djlUCrA/videos

This YouTube channel contains a number of video tutorials. The tutorials walk you through the product interface, showing you exactly how easy it is to use Ivanti Patch for Windows® Servers and how to get the maximum benefit from the product.

INSTALLING IVANTI PATCH FOR WINDOWS® SERVERS

Downloading Ivanti Patch for Windows® Servers

Ivanti Patch for Windows® Servers can be downloaded from the following Web page:

http://www.shavlik.com/downloads/

Installing Ivanti Patch for Windows® Servers

When you purchased Ivanti Patch for Windows® Servers or registered for the trial version, you received download instructions and one or more license keys. To install Ivanti Patch for Windows® Servers, simply follow the on-screen instructions. If you need assistance, please refer to the *Ivanti Patch for Windows® Servers Installation Guide* available at:
https://www.ivanti.com/en-US/support/product-documentation

Activating Ivanti Patch for Windows® Servers

In order to use the full product you must activate it by entering the license key(s). Simply select **Help -> Enter/refresh license key** and follow the on-screen instructions. The license key is contained in the e-mail message sent to you by Ivanti.

Note: Without entering a license key, many of the important features in the product will be unavailable. If you have not already received a license key, please contact your sales representative.

USING IVANTI PATCH FOR WINDOWS® SERVERS

Agentless Patch Management Tasks

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

Performing a Patch Scan

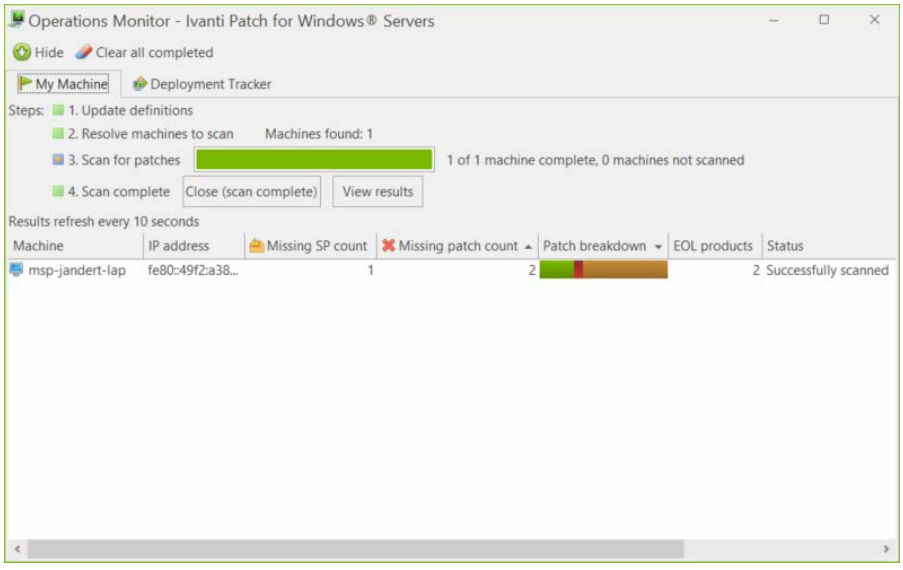
Performing a scan is only a click away. The Ivanti Patch for Windows® Servers interface allows you to work with the application in several different ways. Quick and simple scans can be performed directly from the home page. More advanced scans can be enabled by creating unique machine groups and scan templates. For complete details on performing patch scans see **Agentless Patch Management Tasks > Performing Patch Scans** in the Help system.

Try it yourself:

1. On the home page, in the **Select/confirm targets** area, select **My Machine**.
2. In the **Select schedule** area verify that **Now** is selected, and in the **Select/confirm operation** area verify that **Security Patch Scan** is selected.
3. Click **Scan now**.

Note: The scan is performed using the credentials of the currently logged on user. Valid credentials must be specified when performing scans and deployments on other machines.

This will immediately begin a scan of your machine using the default scan template. During the scan process the latest patch data files are automatically downloaded and the **Operations Monitor** dialog shows the current status of the scan.



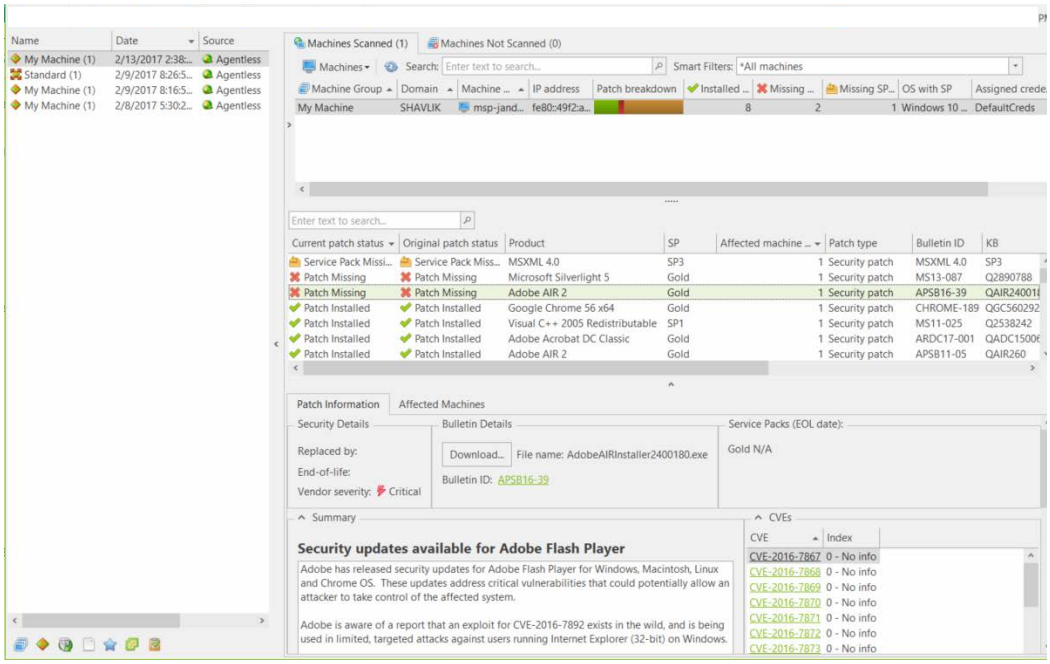
4. Review the scan results by clicking the **View results** link.

Note: For information on performing scheduled scans, see the tutorial available at: https://www.youtube.com/channel/UCVSRxZB9ZDCiwwv4djlUCrA/videos

Reviewing Scan Results

You can access scan results a couple of different ways:

- You can view the results for a scan you just performed by clicking the **View results** link from within the Operations Monitor.
- You can view the results for prior scans by selecting **Results** at the top of the navigation pane and then selecting the desired scan.



This view is called Scan View and provides detailed information about a scan.

1. In the top-right pane, select the machine you just scanned.
2. In the middle pane you can view a variety of information, including:
    - The number of service packs that are missing
    - The number of patches that are missing
    - The number of patches that are installed
    - The products (applications) that were scanned on the machine
    - The number of patches that are missing for each of the scanned products
3. In the bottom pane you can view detailed information about any patch you select in the middle pane.
4. For more information on interpreting scan results, press **F1** to view the Help system.

    Complete information on interpreting patch scan results is available within the Help system at **Agentless Patch Management Tasks > Interpreting Patch Scan Results (Scan View)**.
5. To view scan results using Machine View, select **View > Machines**.

    Complete information on using Machine View is available in the online Help system at **Administration > Using Machine View**.

Deploying Patches

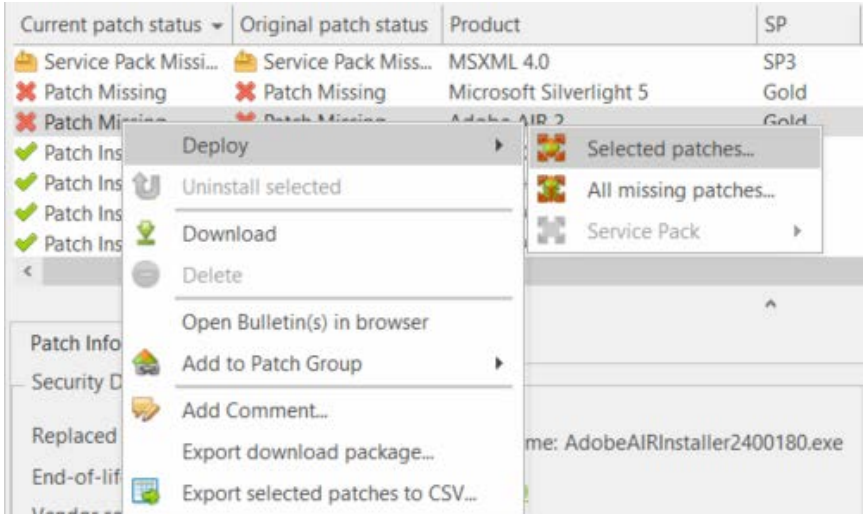
Once you've identified a missing patch that you'd like to deploy, simply right-click the patch and then deploy the patch to the selected machine. You can choose to deploy with the default deployment template, or you can create your own custom deployment template. Patches can be deployed immediately, at a specified future time, upon next reboot, or can be copied to remote machines for manual deployment at a later time. Missing patches can also be automatically deployed upon completion of an immediate or scheduled scan.

Try it yourself:

Patches can be deployed from either Machine View or Scan View. The Machine View process is illustrated here; the process within Scan View is very similar.

1. To get to Machine View, select **View > Machines**.
2. In the top pane, select the machine you just scanned.
3. In the middle pane, expand the **Patch Missing** list.
4. Identify a missing patch that you would like to deploy.
5. Right-click the missing patch and select **Deploy > Selected Patches**.

   For example:



6. If prompted to assign default credentials, click **New**, specify administrative credentials for the machine, click **Save** and then click **Assign**.

   Complete information on specifying and using credentials can be found in the online Help system at **Quick Start > Setup > Supplying and Managing Credentials**.

7. On the **Deployment Configuration** dialog, make sure **Install immediately** is selected and then click **Deploy**.
8. Watch the **Operations Monitor** dialog for detailed information about each step being performed in the deployment process.

   Assuming you used the default deployment template, the final step in the deployment will be to reboot your machine. While you are waiting for the reboot to occur, you can view the pending deployment task by selecting **View > Deployment Tracker**.
9. After your machine reboots, start Ivanti Patch for Windows® Servers again.
10. Within the navigation pane, in the **Results** list, select the deployment you just performed.

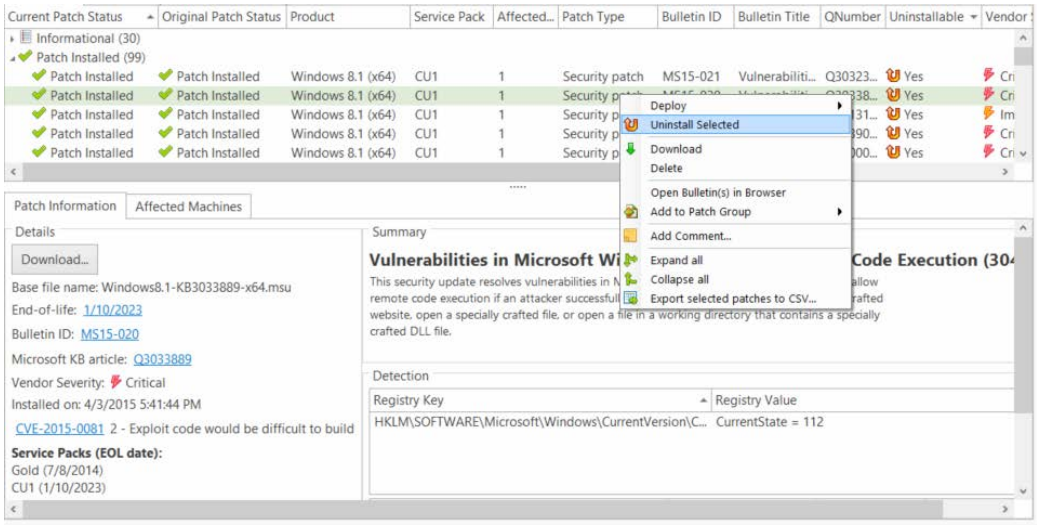
    Details about the deployment are displayed on the right side of the window. The top pane displays a list machines involved in the deployment and shows how many patches each machine received. The lower pane provides information about how the patches were deployed.

For more detailed information, see **Patch Management > Deploying Patches** in the online Help system.

Rolling Back Patches

Ivanti Patch for Windows® Servers provides the ability to uninstall selected patches. Not all patches can be uninstalled. The ability to "roll back" a patch is dependent upon the patch vendor. Only patches identified by the rollback icon can be uninstalled.

You can uninstall a patch from Scan View or Machine View. You simply right-click the patch and then select **Uninstall Selected**. For example:



Generating Reports

Once you've completed a patch scan and deployment, you can generate any of a number of customizable reports to provide analysis of the state of your desktop and network security. Reports can be customized by scan date, machine group, or risk level. Once a report is generated, you can view, print, or save the report. You can also export the report to different formats or e-mail it to designated recipients. Ivanti Patch for Windows® Servers reports are robust, gathering all information stored in the console, not just the information generated in the most recent scan/patch implementation. This function allows administrators to track the history of all patch activity on each machine.

Try it yourself:

1. From the program menu select **Tools > Create report**.
2. In the **Select report to view** box select the report you want to generate (for example, **Executive Summary**).
3. Near the bottom of the **Reports** dialog click **Generate report**.

For detailed information about generating reports, see **Administration > Reports** in the onliine Help system.

Agent-based Tasks

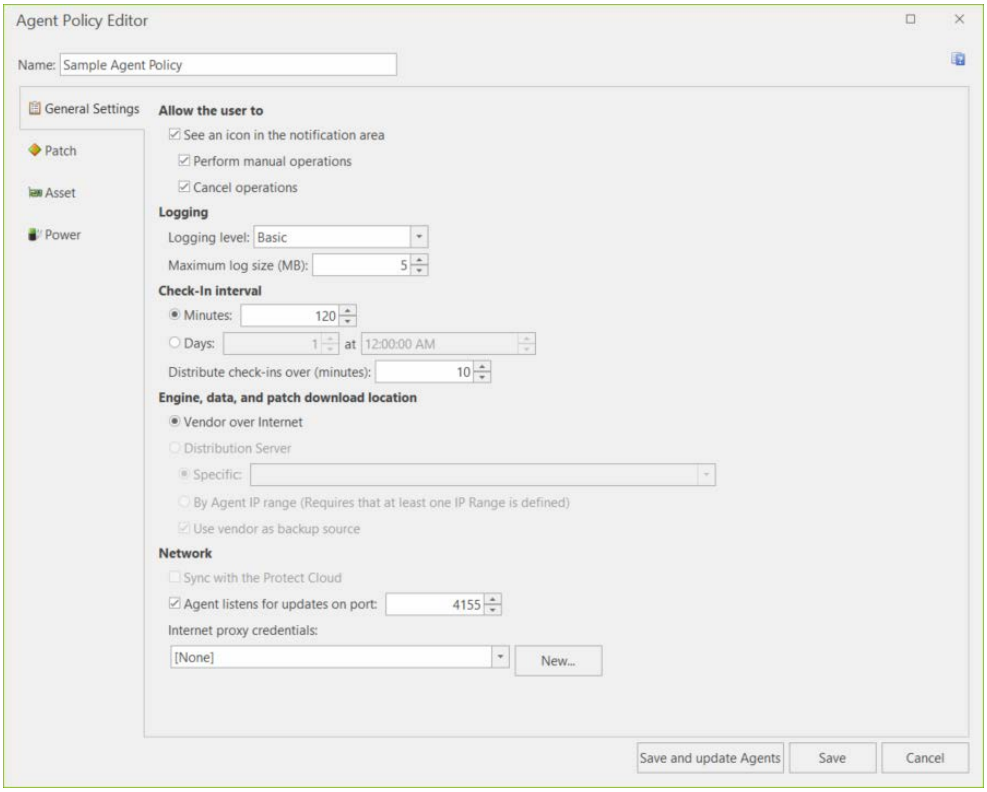
You can perform patch tasks (as well as asset and power tasks) using agents. Simply create an agent policy and then install the agent on a machine.

Create an Agent Policy

To create a new Ivanti Patch for Windows® Servers Agent policy:

1. From the main menu select **New > Agent Policy**.

   The **Agent Policy Editor** is displayed.



2. Type a name for the new agent policy.

Configure an Agent Policy

There are many different configuration options for an agent policy. For this example you will configure a policy with a simple patch task, a basic asset task and a basic power management task.

On the Patch Tab

Click **Add a Patch Task** and type a name for the task. For example, you might name it *Eval Patch Task*. The patch task options are displayed. Feel free to simply use the default values. You might consider clearing the **Deploy patches** check box on the **Scan and deploy options** sub-tab if you do not want all missing patches to be deployed later on when you test the agent. Do not click **Save and update Agents** just yet.

On the Asset Tab

Click **Add an Asset Task** and type a name for the task. For example, you might name it *Eval Asset Task*. The asset task options are displayed. Feel free to simply use the default values. The default asset scan template (**Full Asset Scan**) will perform a software asset scan and a hardware asset scan on the agent machine whenever the asset task is run.

On the Power Tab

Click **Add a Power State Task** and type a name for the task. For example, you might name it *Eval Power Task*. The power state task options are displayed. Feel free to simply use the default values. The default power state template (**Standard Power**) will perform a restart of the agent machine whenever the power task is scheduled to run or is initiated manually from the console.

Save the Agent Policy

In the bottom-right corner of the **Agent Policy Editor** dialog, click **Save and update Agents**.

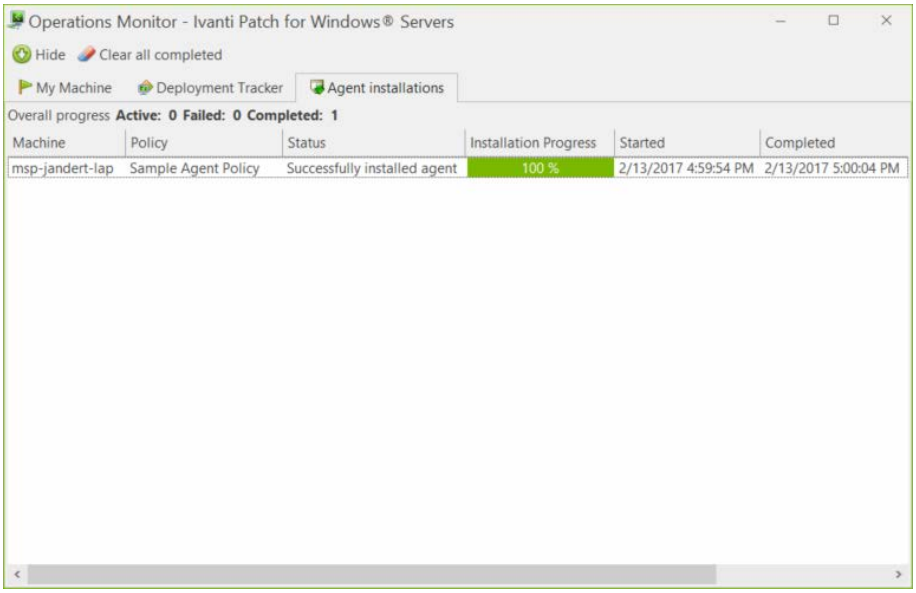
Tip: To view a video tutorial on this topic, click the video icon.

Install the Agent on the Console Machine

For simplicity, in this example you will install the agent onto your console machine. You can, of course, install the agent on any of the machines in your organization.

1. Go to Machine View by selecting **View > Machines**.
2. Select the machine you scanned previously (this should be your console machine).
3. Right-click the machine and then select **Agents > Install / Reinstall with Policy** and then select the agent policy you just created.

   The Operations Monitor is displayed. It shows the status of the different steps involved in the installation process. For example:

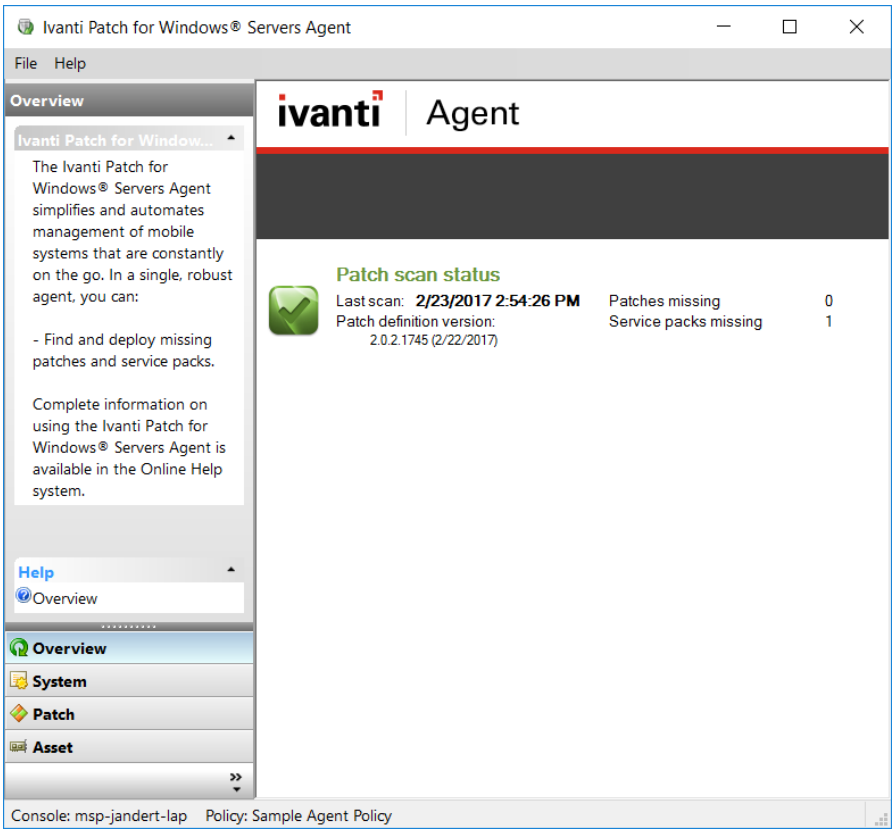


Using the Agent

The agent should now be installed on your console machine. You can launch the agent a number of different ways:

- Select **Start > Ivanti Patch for Windows® Servers > Ivanti Patch for Windows® Servers Agent**
- Tap or click the Ivanti Patch for Windows® Servers Agent icon on the desktop
- Double-click the Ivanti Patch for Windows® Servers Agent service icon that resides in your machine's system tray

The Ivanti Patch for Windows® Servers Agent client program is displayed. For example:



1. In the button tray located in the lower-left corner, click **Patch**.
2. In the Active Function pane located immediately above the button tray, click the patch task you created earlier (e.g. Eval Patch Task).

   Wait for the patch scan to complete. You can review the results in the right-hand pane. Click **Overview** in the button tray to view the patch status of your machine.
3. Click the asset task you created earlier (e.g. Eval Asset Task) and review the results in the right-hand pane.

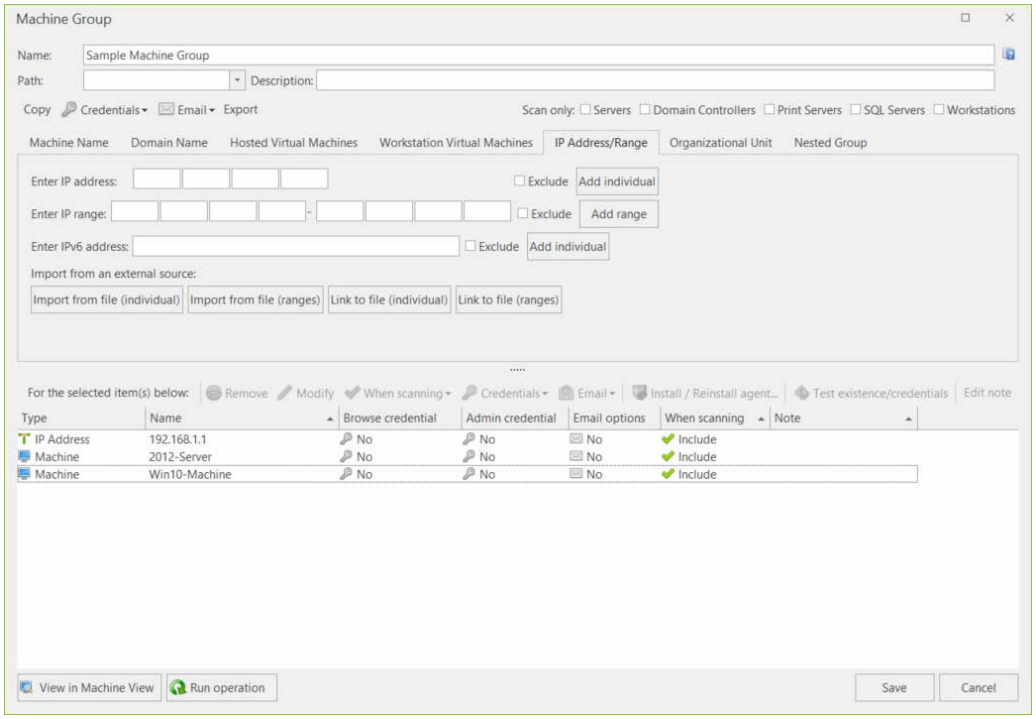
Results from agent-based tasks are also rolled up to the console and can be viewed using Machine View.

EXPLORING THE MANY OTHER POWERFUL FEATURES OF IVANTI PATCH FOR WINDOWS® SERVERS

The topics discussed up until now are designed to get you up and running quickly with Ivanti Patch for Windows® Servers and get a feel for the core capabilities of the product. There are of course many, many other powerful features and we encourage you to explore them on your own.

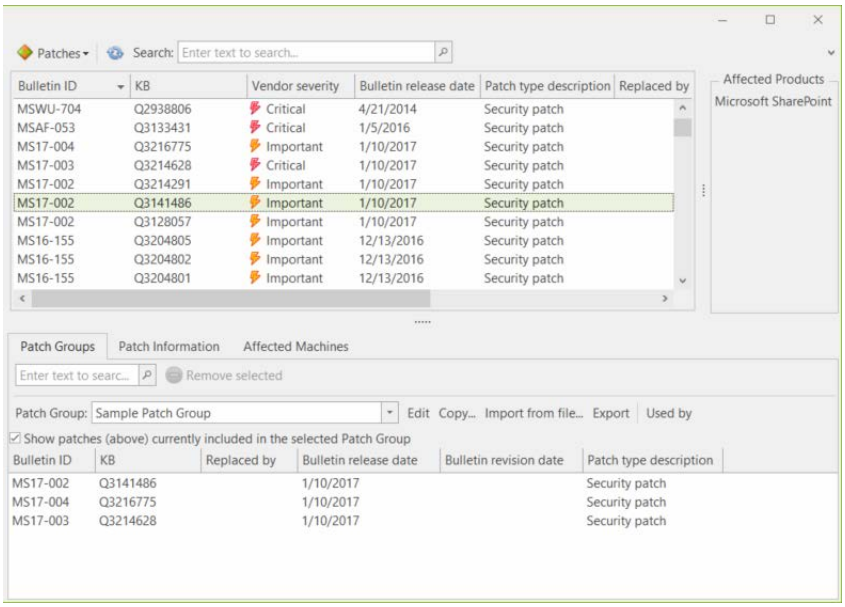
Machine Groups

Create a machine group and see how easy it is to manage the different physical machines, virtual machines, domains, and organizational units in your organization. For details, access the online Help system and read the **Quick Start > Setup > Using Machine Groups** topics.



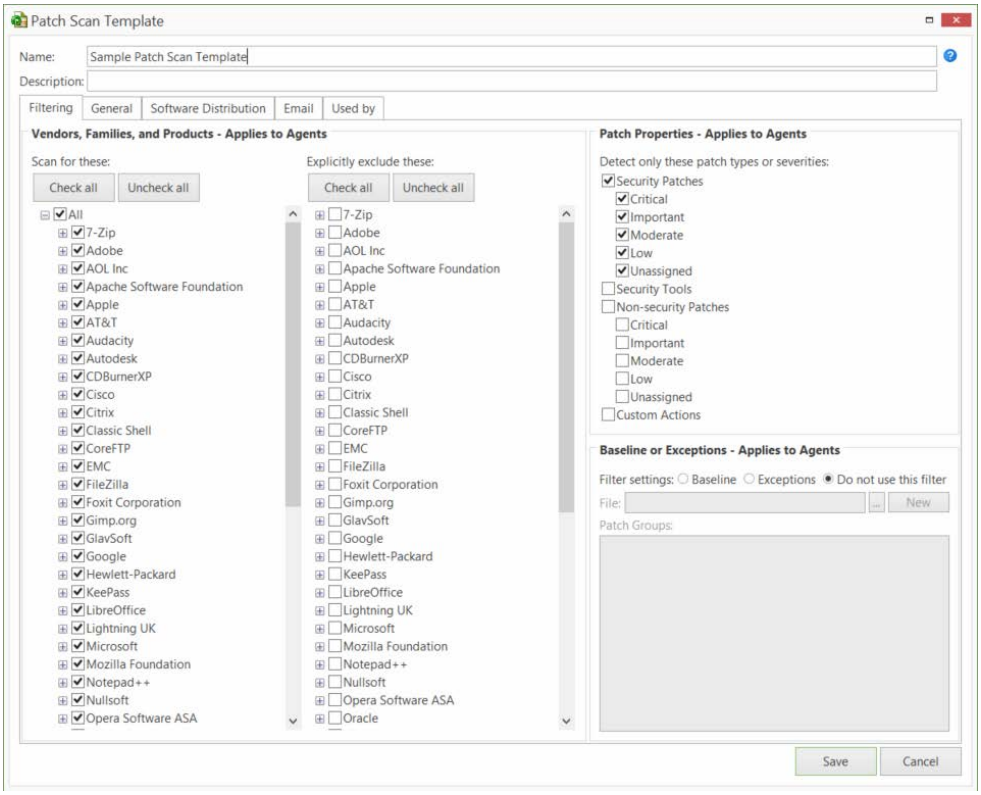
Patch Groups

Create a patch group and see how they can be used to control exactly which patches are scanned for and deployed to the machines in your organization. For details, access the online Help system and read the **Patch Management > Creating Patch Groups** topics.



Patch Scan Templates

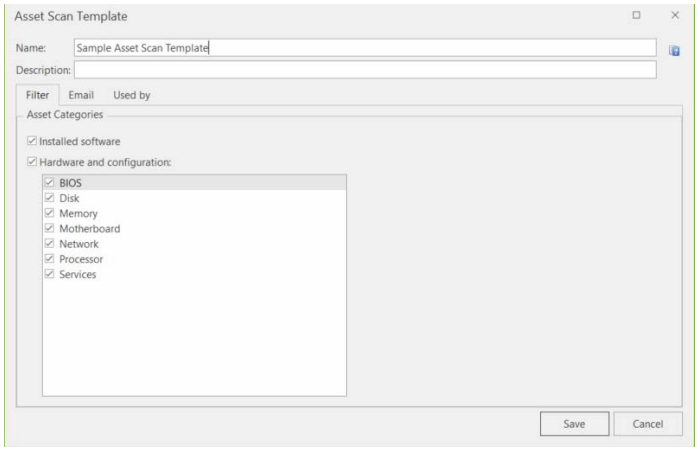
Create a new patch scan template and learn about all the ways it can be configured in order to address your specific scanning needs. For details, access the Help system and read the **Patch Management > Patch Scan Templates** topics.



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

Asset Inventory Features

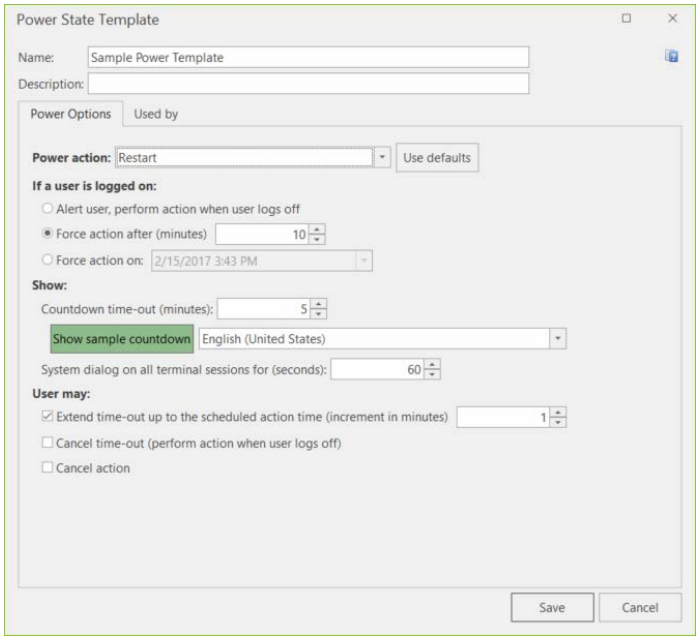
Create a new asset scan template and then use it in a scan to learn about your software, hardware, and virtual assets. For details, access the online Help system and read the **Asset Inventory** topics.



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

Power Management Features

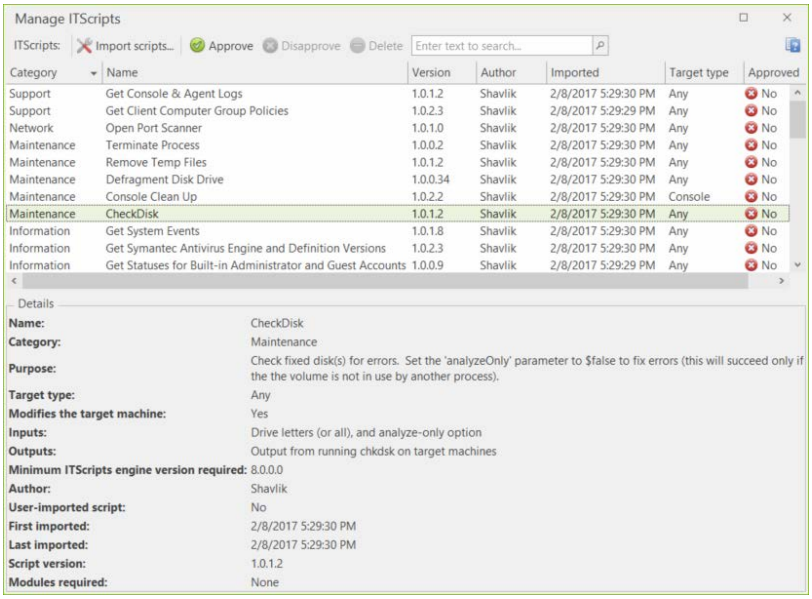
Read through the **Power Management** topics in the online Help system to learn how you can use Ivanti Patch for Windows® Servers to prepare your machines for maintenance tasks and to reduce power consumption and operating costs. If you decide to test the reboot or shut down feature be sure to do so on a non-critical target machine.



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

ITScripts Feature

The ITScripts feature supports the use of PowerShell 4.0 and WinRM 2.0, enabling you to execute a variety of scripts on the console and on remote target machines. It also enables you to start a Windows PowerShell session between the console and a selected machine. For details see **Administration > ITScripts** in the online Help system.



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

Virtual Inventory Feature

The Virtual Inventory feature is used to manage and track the vCenter Servers and the ESXi hypervisors (ESXi hosts) that are used in your organization. You can use the Virtual Inventory feature to:

- Add vCenter Servers and ESXi hypervisors to Ivanti Patch for Windows® Servers
- View basic configuration information about the vCenter Servers and the ESXi hypervisors
- Perform a scan of the managed and unmanaged ESXi hypervisors
- View the security bulletins that have already been installed on the managed and unmanaged ESXi hypervisors
- View the security bulletins that are missing on the managed and unmanaged ESXi hypervisors
- Deploy any missing security bulletins to the ESXi hypervisors

For details, access the online Help system and read the **Quick Start > Setup > Managing Your vCenter Server and ESXi Hypervisors** topics.