

Quick Start Guide

VMware vCenter™ Protect 8.0

vmware®

Copyright

Copyright ©2011 VMware Inc. All rights reserved.

No part of this document may be reproduced or retransmitted in any form or by any means electronic, mechanical, or otherwise, including photocopying and recording for any purpose other than the purchaser's personal use without written permission of VMware Inc.

Trademarks

VMware vCenter Protect, VMware vCenter Protect Essentials, VMware vCenter Protect Essentials Plus, and the VMware logo are trademarks or registered trademarks of VMware Inc. Microsoft and Windows are registered trademarks of Microsoft Corporation.

All other trademarks, tradenames, or images mentioned herein belong to their respective owners.

Document Information and Print History

Document number: N/A

Date	Version	Description
October 2011	VMware vCenter Protect 8.0	Initial release of the VMware vCenter Protect Quick Start Guide

Table of Contents

WELCOME	1
Beyond This Quick Start Guide.....	1
INSTALLING VMWARE vCENTER PROTECT	2
Downloading VMware vCenter Protect	2
Installing VMware vCenter Protect	2
Activating VMware vCenter Protect	2
USING VMWARE vCENTER PROTECT	3
Agentless Patch Management Tasks	3
Performing a Patch Scan.....	3
Reviewing Scan Results	4
Deploying Patches	5
Rolling Back Patches.....	6
Generating Reports	7
Antivirus and Antispyware Tasks.....	8
Create an Agent Policy	8
Configure an Agent Policy	9
On the Patch Tab	9
On the Threat Tab.....	9
On the Exceptions Sub-Tab.....	9
On the Active Protection Sub-Tab.....	9
Save the Agent Policy.....	9
Install the Agent on the Console Machine.....	10
Using the Agent.....	10
Performing AV Scans on Specific Files, Folders, or Drives	12
EXPLORING THE MANY OTHER POWERFUL FEATURES OF VMWARE vCENTER PROTECT	13
Machine Groups	13
Patch Groups	13
Patch Scan Templates.....	14
Asset Inventory Features	15
Power Management Features.....	15
ITScripts Feature	16
Remote Desktop Protocol.....	16

This page intentionally left blank.
The document is designed for duplex printing.

WELCOME

Thank you for choosing VMware vCenter™ Protect, a next generation security management program used for managing and protecting Microsoft-based machines. VMware vCenter Protect provides you with one centralized and common interface that you can use to perform several essential security operations, including patch management, antivirus, antispysware, Active Protection, virtualization management, asset inventory, power management, IT management tools, extensive reporting, and more.

VMware vCenter Protect is available within two different product bundles.

- **VMware vCenter Protect Essentials:** This is the basic product offering that includes patch management, asset inventory, and a limited number of scripts for IT management.
- **VMware vCenter Protect Essentials Plus:** This is the full-featured product offering that includes patch management, asset inventory, antivirus & antispysware, power management, configuration management and full ITScripts capabilities.

To quickly get you up and running with VMware vCenter Protect 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 VMware vCenter Protect, please see the following Web pages:

<http://www.shavlik.com/training-on-demand.aspx>

This Web page contains a number of video tutorials. The tutorials walk you through the product interface, showing you exactly how easy it is to use VMware vCenter Protect and how to get the maximum benefit from the product.

INSTALLING VMWARE vCENTER PROTECT

Downloading VMware vCenter Protect

VMware vCenter Protect can be downloaded from the following Web page:

<http://www.shavlik.com/pDownloadForm4.aspx?productid=74>

Installing VMware vCenter Protect

When you purchased VMware vCenter Protect or registered for the trial version, you received an email that contained download instructions and a license key. To install VMware vCenter Protect, simply follow the on-screen instructions. If you need assistance please refer to the *VMware vCenter Protect Installation Guide* available at: <http://www.shavlik.com/support/onlinehelp.aspx>

Activating VMware vCenter Protect

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

Please 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 shavlik-sales@vmware.com.

USING VMWARE vCENTER PROTECT

Agentless Patch Management Tasks

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



Performing a Patch Scan

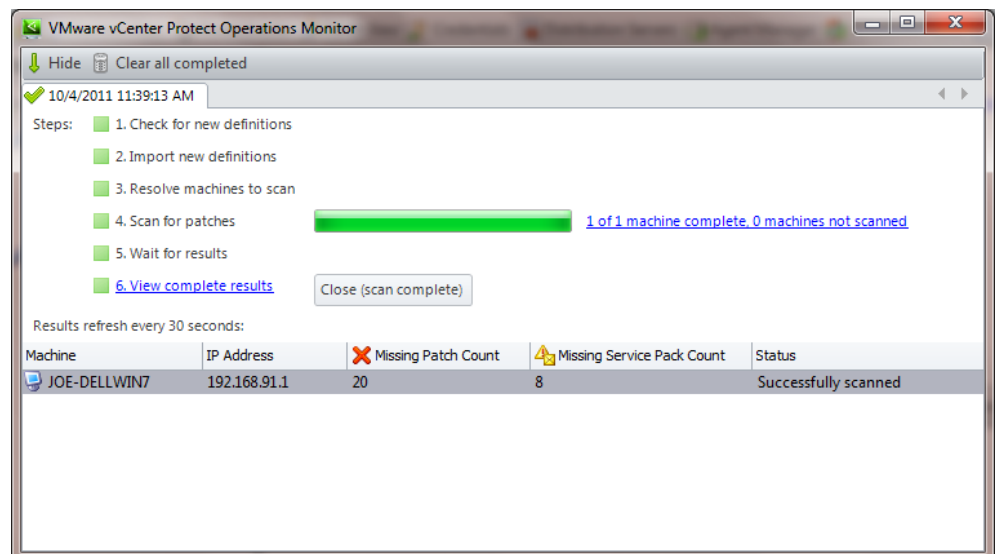
Performing a scan is only a click away. The VMware vCenter Protect interface allows you to work with the application in several different ways. Quick and simple scans can be performed directly from the home page. More advanced scans can be enabled by creating unique machine groups and scan templates. 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.



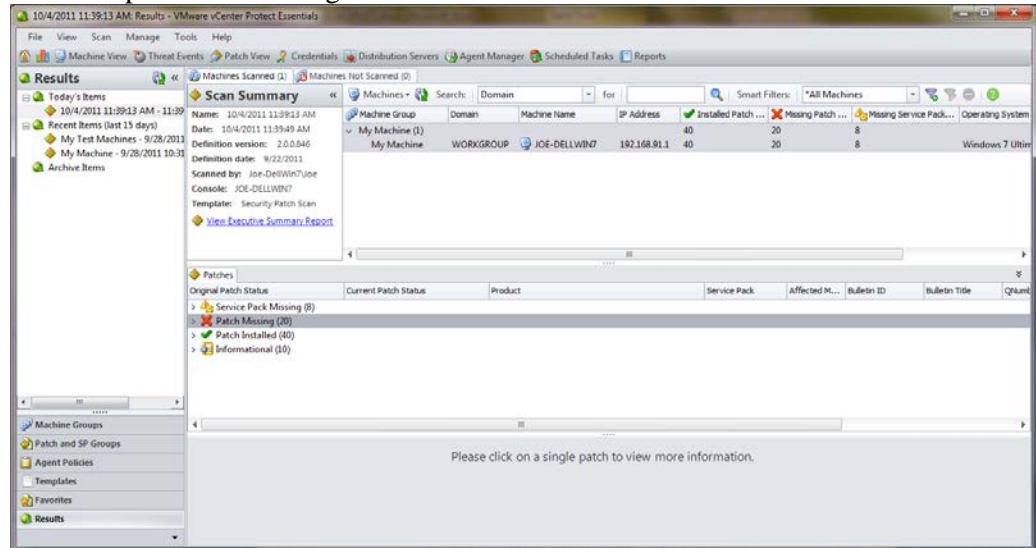
4. Review the scan results by clicking the **View complete results** link.

Note: For information on performing scheduled scans, see the tutorial available at: <http://www.shavlik.com/training-on-demand.aspx>.

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 complete results** link from within the Operations Monitor
- You can view the results for prior scans by clicking **Results** in the button tray at the bottom of the navigation bar and then selecting the desired scan in the top half of the navigation bar.



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, click the  **Machine View** icon.

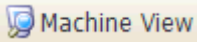
Complete information on using Machine View is available within the Help system at **Common Tasks > Using Machine View**.

Deploying Patches

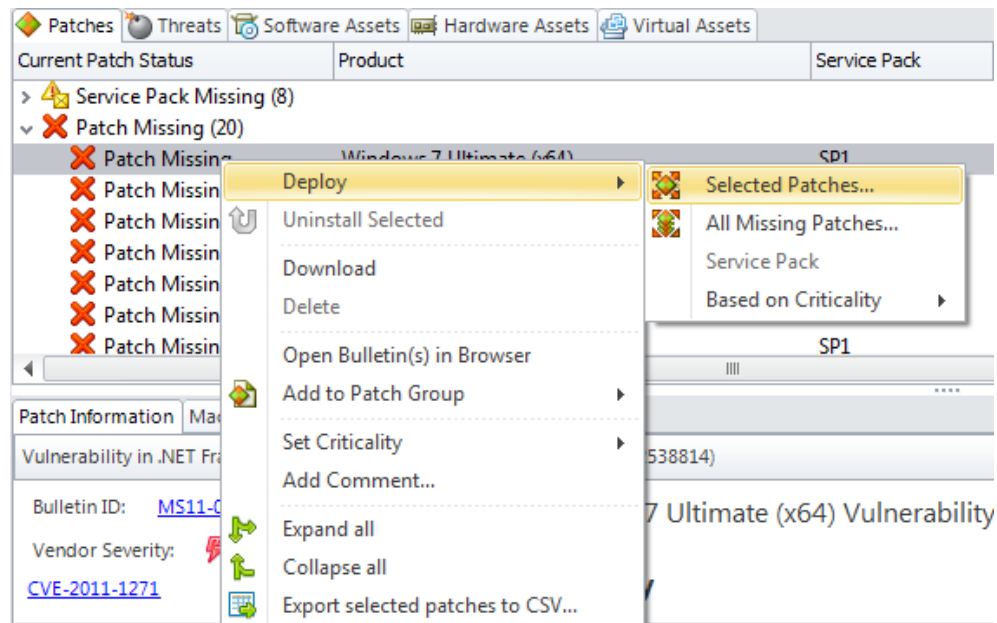
Once you've identified a missing patch that you'd like to deploy, simply right-click the patch and then deploy the patch to the selected machine. You can choose to deploy with the default deployment template, or you can create your own custom deployment template. Patches can be deployed immediately, 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, click the  icon.
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 Help system at **Installation and 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 VMware vCenter Protect again.
10. Within the navigation bar, in the **Results** list, select the deployment you just performed.

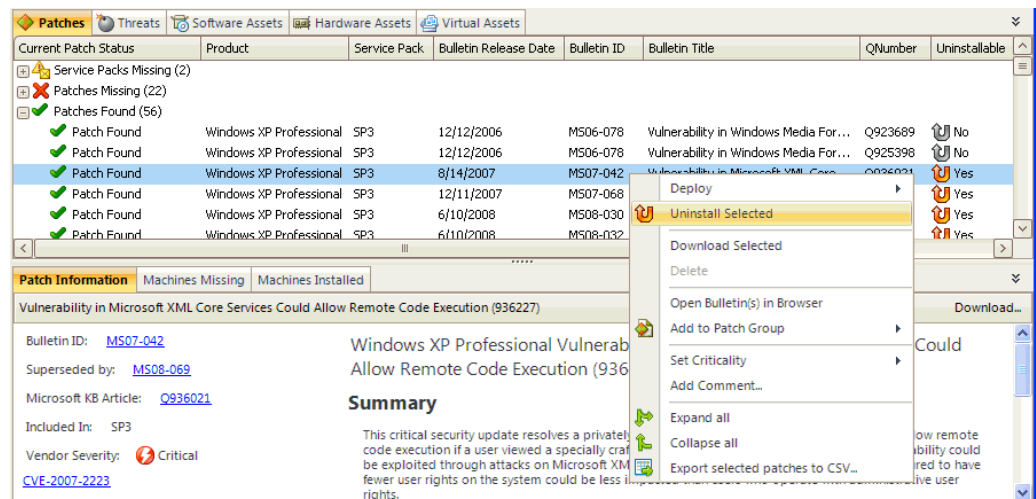
Details about the deployment are displayed on the right side of the window. The top pane displays a list machines involved in the deployment and shows how many patches each machine received. The lower pane provides information about how the patches were deployed.

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

Rolling Back Patches

VMware vCenter Protect 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:



The screenshot displays the VMware vCenter Protect interface. The top navigation bar includes tabs for Patches, Threats, Software Assets, Hardware Assets, and Virtual Assets. The main area shows a table of patches with columns for Current Patch Status, Product, Service Pack, Bulletin Release Date, Bulletin ID, Bulletin Title, QNumber, and Uninstallable. A context menu is open over a selected patch, showing options like Deploy, Uninstall Selected, Download Selected, Delete, Open Bulletin(s) in Browser, Add to Patch Group, Set Criticality, Add Comment..., Expand all, Collapse all, and Export selected patches to CSV... The selected patch is 'Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (936227)' with Bulletin ID MS07-042. The summary pane below the table provides details for this patch, including its superseded status, Microsoft KB article, included in SP3, and vendor severity (Critical).

Current Patch Status	Product	Service Pack	Bulletin Release Date	Bulletin ID	Bulletin Title	QNumber	Uninstallable
Service Packs Missing (2)							
Patches Missing (22)							
Patches Found (56)							
Patch Found	Windows XP Professional	SP3	12/12/2006	MS06-078	Vulnerability in Windows Media For...	Q923689	No
Patch Found	Windows XP Professional	SP3	12/12/2006	MS06-078	Vulnerability in Windows Media For...	Q925398	No
Patch Found	Windows XP Professional	SP3	8/14/2007	MS07-042	Vulnerability in Microsoft XML Core...	Q936021	Yes
Patch Found	Windows XP Professional	SP3	12/11/2007	MS07-068			Yes
Patch Found	Windows XP Professional	SP3	6/10/2008	MS08-030			Yes
Patch Found	Windows XP Professional	SP3	6/10/2008	MS08-032			Yes

Patch Information Machines Missing Machines Installed


Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (936227)

Bulletin ID: [MS07-042](#) Windows XP Professional Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (936227)

Superseded by: [MS08-069](#)

Microsoft KB Article: [Q936021](#)

Included In: SP3

Vendor Severity:  Critical

[CVE-2007-2223](#)

Summary

This critical security update resolves a private code execution if a user viewed a specially crafted exploit through attacks on Microsoft XML Core Services. Fewer user rights on the system could be less likely to be exploited.


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



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. VMware vCenter Protect 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** or simply click the  **Reports** icon.
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 **Common Tasks > Reports** in the Help system.

Antivirus and Antispyware Tasks

You perform antivirus and antispyware tasks using agents. Simply create an agent policy and then install the agent on a machine.

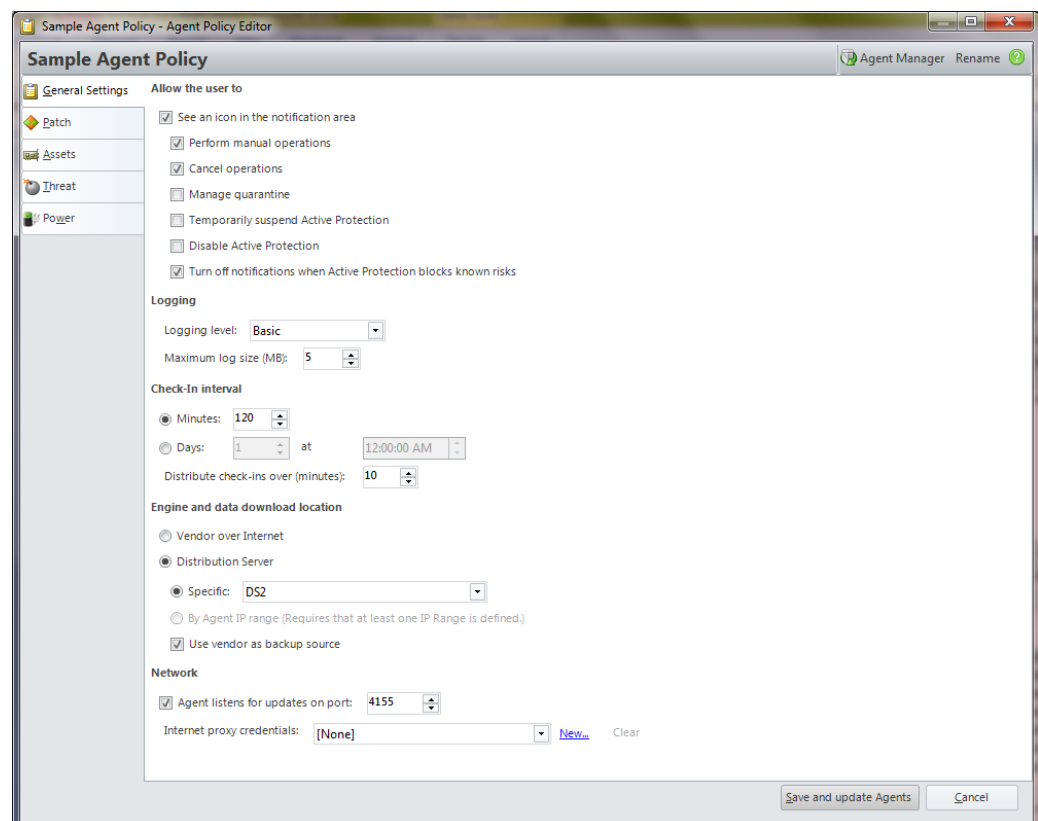
Important! Before using a threat task on agent machines, it is strongly recommended that you remove all other antivirus and antispyware programs that may be running on the agent machines. Using multiple threat programs on the same machine may cause serious performance issues.

Create an Agent Policy

To create a new VMware vCenter Protect Agent policy:

1. In the button tray at the bottom of the navigation bar, click **Agent Policies**.
2. In the **Agent Policies** pane, click **New Agent Policy**.
3. Type a name for the new agent policy and then click **OK**.

The **Agent Policy Editor** window is displayed.



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 and a very basic threat task, using the default settings in most cases. You can also configure an agent policy to perform asset and power tasks but those features are not used in this example.

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



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.

On the Threat Tab

Click **Add a Quick Scan Threat Task** and type a name for the task. For example, you might name it *Eval Threat Task*. The threat task options are displayed. Feel free to simply use the default values.

On the Exceptions Sub-Tab

Select **Always allow files**, type **winword.exe** and then click **Add**. This tells your threat task(s) and Active Protection that you always want Microsoft Word to be allowed to run. This is a very simple example of how to use the Always Allow and Never Allow lists. For more examples, click the **Examples** link.

On the Active Protection Sub-Tab

Make sure the **Enable Active Protection** check box is enabled.

Active Protection is a real-time service used to detect known and unknown threats before they infect an agent machine. It sits quietly in the background of a machine and monitors for attempts to change security configuration settings and values. If it detects an attempt to change a setting it can respond a number of different ways, depending on how it is configured. Feel free to simply use the default configuration.

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.

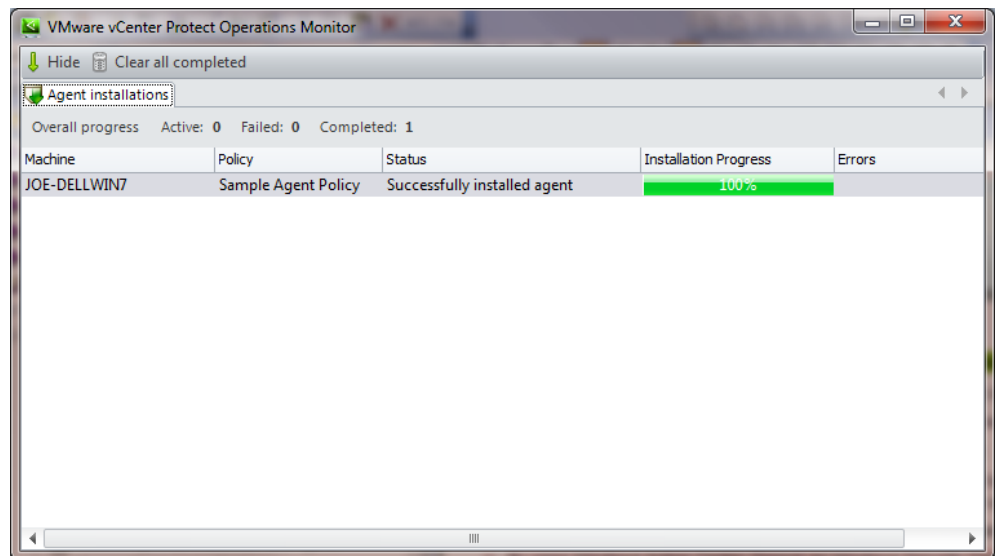


Install the Agent on the Console Machine

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 network.

1. Access the Agent Manager by clicking the  **Agent Manager** icon.
2. Select the machine you scanned previously (this should be your console machine).
3. Click **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:



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



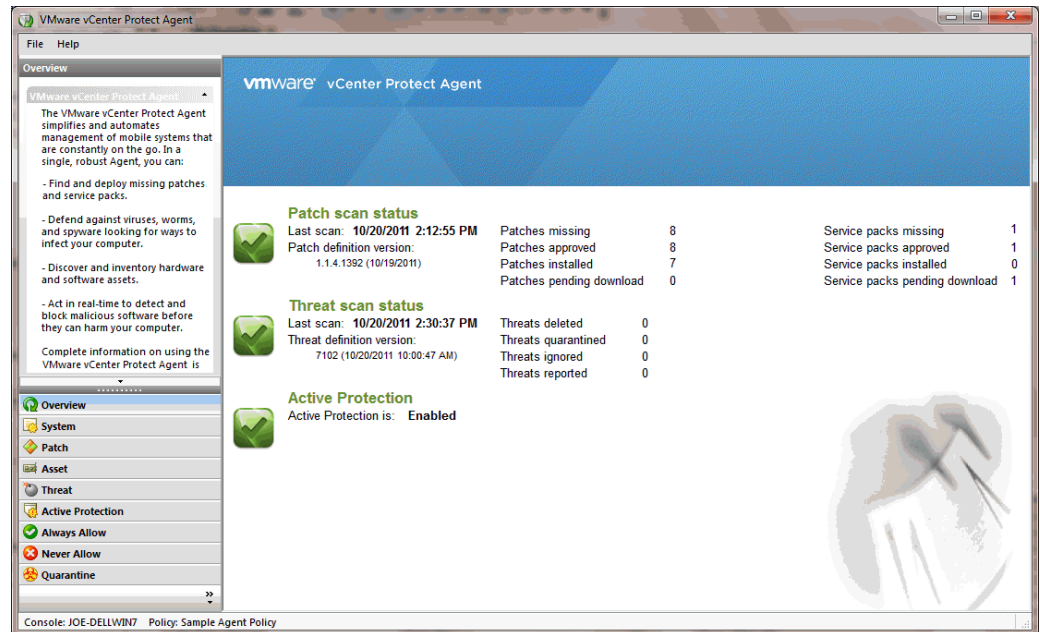
Using the Agent

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



- Select **Start > All Programs > VMware vCenter Protect > VMware vCenter Protect Agent**
- Double-click the VMware vCenter Protect Agent service icon that resides in your machine's system tray



The VMware vCenter Protect Agent client program is displayed. For example:

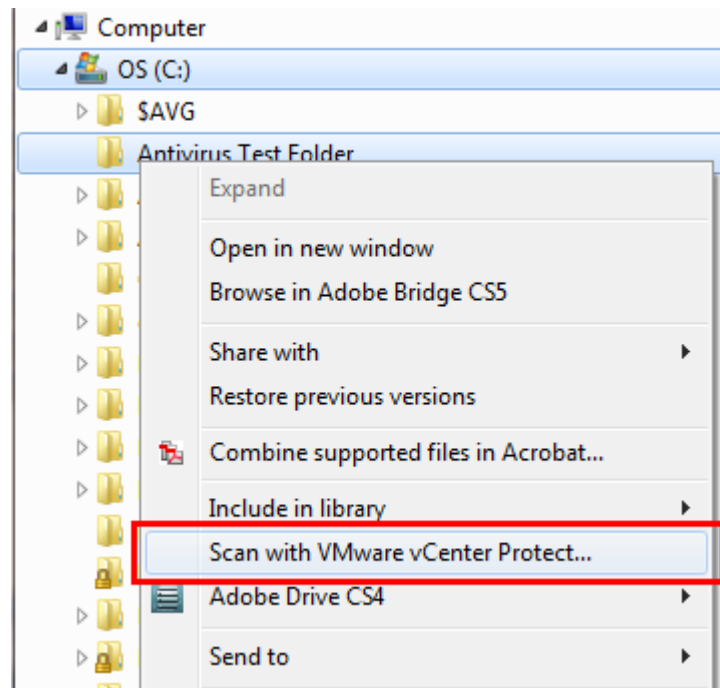


1. In the button tray located in the lower-left corner, click **Patch**.
2. In the Active Function pane located immediately above the button tray, click the patch task you created earlier (e.g. Eval Patch Task).
Wait for the patch scan to complete. You can review the results in the right-hand pane. Click **Overview** in the button tray to view the patch status of your machine.
3. In the button tray, click **Threat**.
4. In the Active Function pane located immediately above the button tray, click the threat task you created earlier (e.g. Eval Threat Task).
Wait for the threat scan to complete. You can review the results in the right-hand pane. Click **Overview** in the button tray to view the threat status of your machine.

Results from agent-based patch tasks and threat tasks are also rolled up to the console and can be viewed using either Machine View ( **Machine View**) or Threat Events View ( **Threat Events**).

Performing AV Scans on Specific Files, Folders, or Drives

If an agent is configured with a threat task or if Active Protection is enabled, the user of the machine can initiate an antivirus scan on a specific file, folder, or drive on the machine. This is done by right-clicking the desired item within Windows Explorer and then selecting **Scan with VMware vCenter Protect**. For example:



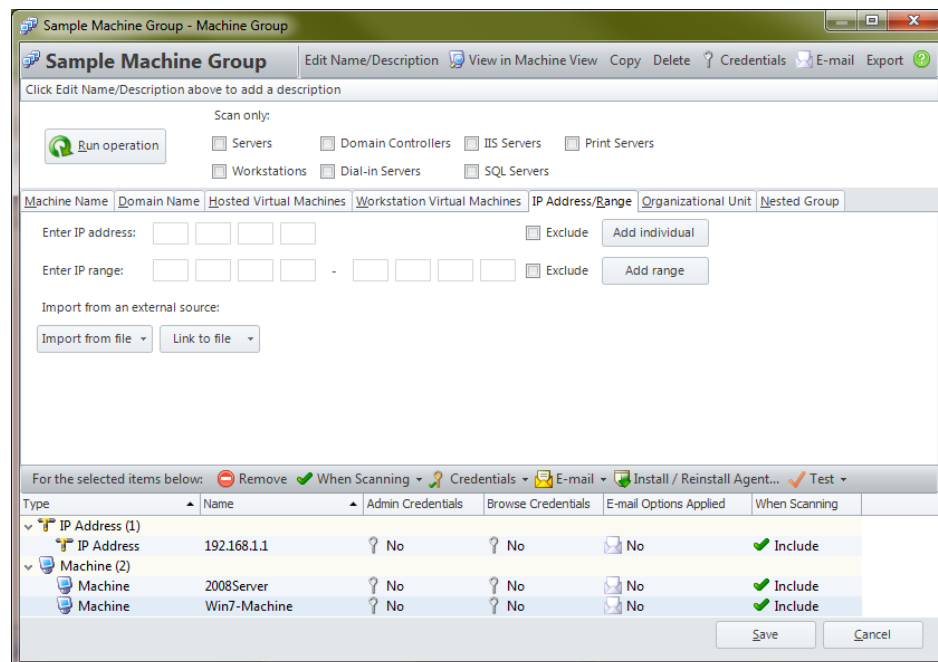
The results of the scan are displayed in the agent's threat log. The results are also reported to the console and available for viewing using either Machine View or Threat Events View.

EXPLORING THE MANY OTHER POWERFUL FEATURES OF VMWARE vCENTER PROTECT

The topics discussed up until now are designed to get you up and running quickly with VMware vCenter Protect 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.

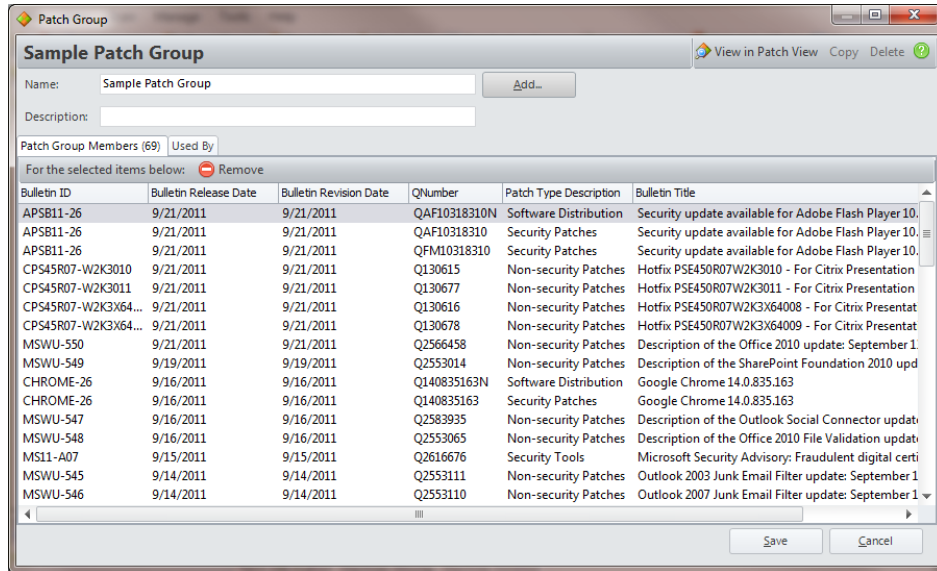
Machine Groups

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 Help system and read the **Installation and Setup > Using Machine Groups** topics.



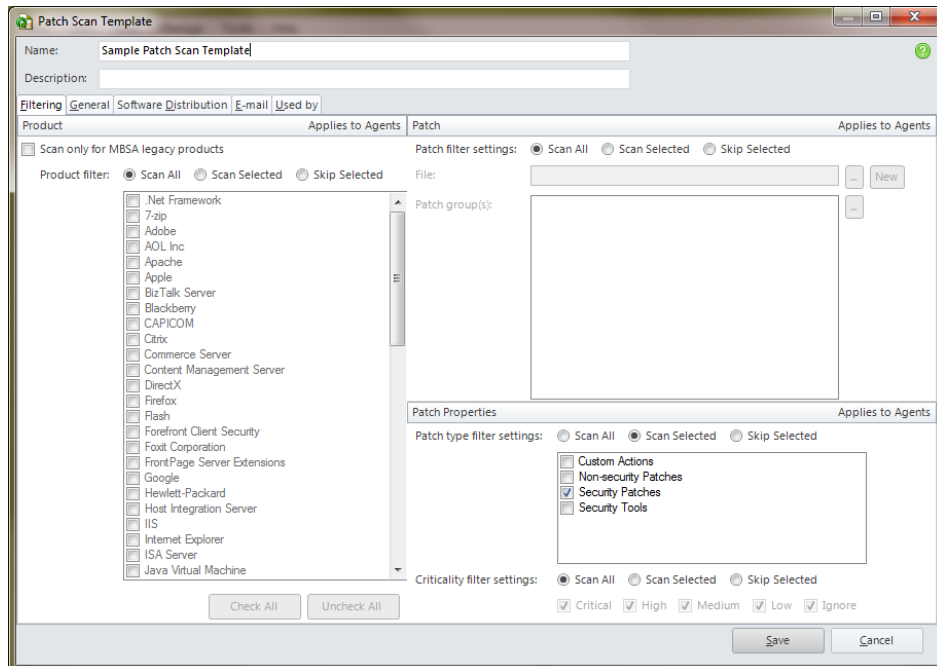
Patch Groups

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 Help system and read the **Agentless Patch Management Tasks > 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 **Agentless Patch Management Tasks > Patch Scan Templates** topics.

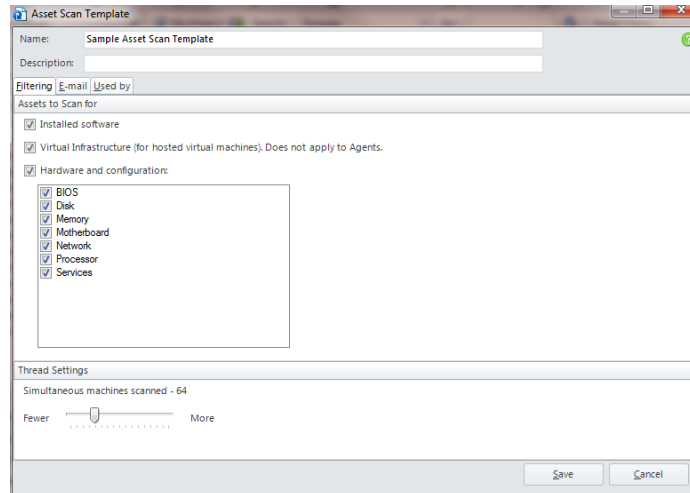


Tip: To view a video tutorial on this topic, click the video icon.



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 Help system and read the **Agentless Asset Inventory Tasks** topics.

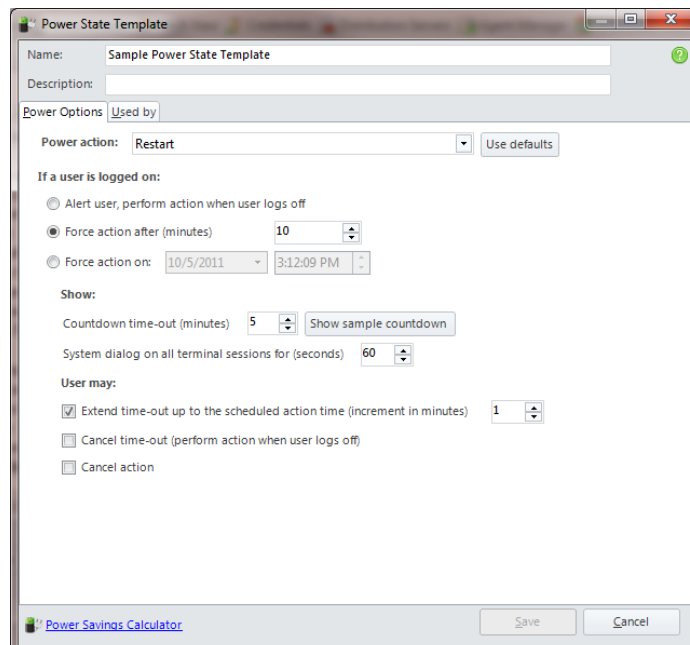


Tip: To view a video tutorial on this topic, click the video icon.



Power Management Features

Read through the **Agentless Power Management Tasks** topics in the Help system to learn how you can use VMware vCenter Protect 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.

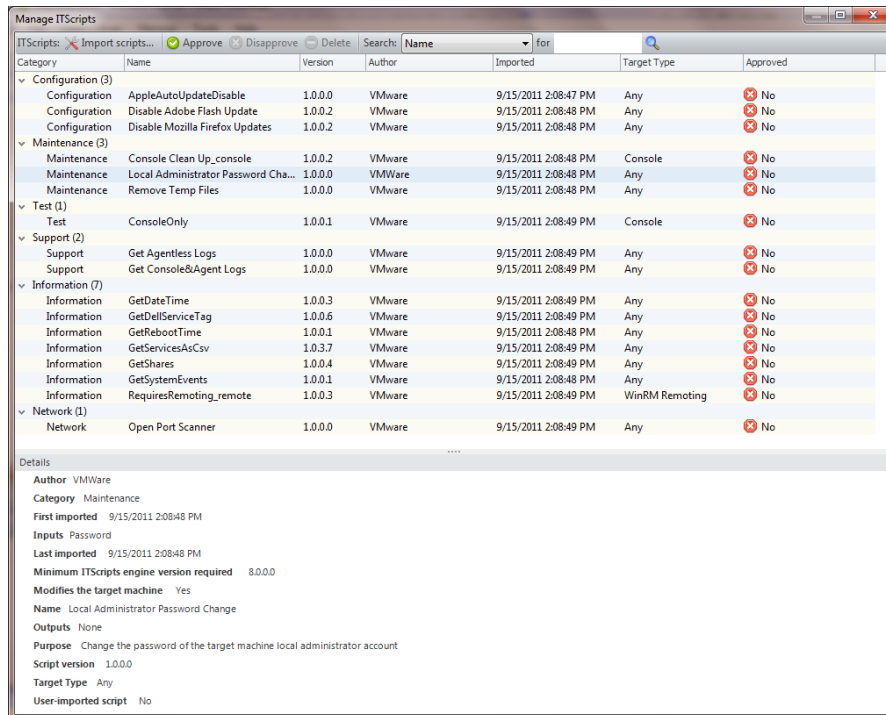


Tip: To view a video tutorial on this topic, click the video icon.



ITScripts Feature

The ITScripts feature supports the use of PowerShell 2.0 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 **IT Management Tools > ITScripts** in the Help system.



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



Remote Desktop Protocol

The Microsoft Remote Desktop Protocol (RDP) provides the ability to remotely manage Windows-based machines over a network connection. RDP capabilities are supported in VMware vCenter Protect, enabling you to use stored machine credentials to quickly connect the console to a target machine. With Remote Desktop you can access the target machine’s programs, files, and resources as if you were physically sitting in front of the machine.

