Altiris™ Patch Management Solution for Windows 7.1 from Symantec™ User Guide

Altiris™ Patch Management Solution for Windows 7.1 from Symantec™ User Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Legal Notice

Symantec, the Symantec Logo, Altiris, and any Altiris or Symantec trademarks used in the product are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our web site at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level

- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Managed Services

Managed Services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.

Consulting Services

Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.

Education Services

Education Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about enterprise services, please visit our web site at the following URL:

www.symantec.com/business/services/

Select your country or language from the site index.

Contents

Chapter 1

Introducing Patch Management Solution for Windows

This chapter includes the following topics:

About Patch Management Solution for Windows

Patch Management Solution for Windows takes inventory of managed computers to determine the operating system and software updates (patches) they require. The solution then downloads the required patches and provides wizards to help you deploy patches. The solution enables you to set up a patch update schedule to ensure that managed computers are kept up-to-date with the latest vendor security updates. Managed computers are then protected on an on-going basis.

See “Platforms supported by Patch Management Solution for Windows” on page 20.

Key features include a software repository that provides comprehensive data on software bulletins, software updates, and inventory rules, such as technical details, severity ratings, and number of executables. The process of populating the information repository from the patch management metadata files can be started after installation is complete.

To reduce labor, the software update plug-in automatically analyzes managed computers. The software update plug-in gathers patch-specific inventory on supported operating systems, applications, and the associated service pack level. The inventory data is used to determine whether a patch is required. Inventory results populate predefined filters. The software update policy wizard then automatically assigns software updates to relevant filters. The wizard also simplifies the management of distribution. Instead of creating a policy for each individual software update, you create a single policy for the relevant software bulletin. For example, if three software bulletins with seven software updates address various operating systems in various languages, you only have to manage three distribution policies. If you want to, you can modify any default settings and command-line options in a software update policy.

Integration with Notification Server 7.x includes features such as hierarchy and maintenance windows. Hierarchy lets you configure features and settings for a parent Notification Server computer, then pass the settings down to child Notification Server computers.

See “Implementing Patch Management Solution for Windows” on page 17.

How Patch Management Solution for Windows works

Patch Management Solution for Windows uses inventory information to decide which software update packages to distribute. From software update packages, you create the software update policies that send the associated packages to managed computers and install the appropriate software update programs.

After you install Patch Management Solution for Windows, you download complete software bulletin information from the Symantec Web site. Information includes the severity of each software bulletin, details on its software updates, and where they can be downloaded from Microsoft or Adobe. This information also includes rules for creating filters and rules on how to verify that a software update is installed. Then you deploy the software update plug-in to managed computers, which gathers inventory, including software vendor, software release, and service pack information. From this inventory, Patch Management Solution for Windows creates specific filters to target only the computers requiring individual software updates.

See “About the software update plug-in” on page 23.

You must stage software bulletins to download software updates and create packages. When a software bulletin is staged, each associated software update executable is downloaded from Microsoft or Adobe to the Notification Server computer. From the information in software bulletin executables, Patch Management Solution for Windows then creates a software update package for each software update. From the staged software bulletins , you must create software update policies to distribute software update packages to the appropriate computer filters (previously known as collections). When a managed computer receives a software update policy, it verifies that the update is needed, then downloads the software update package from the Notification Server computer. The managed computer then installs the update. At an interval, the software update policy is re-evaluated and software updates are reinstalled if needed. For example, if an operation removes a software update, it is reinstalled. Or if a vendor revises a software update, it is reinstalled.

After the software update plug-in distributes software updates, it sends results of patch deployment to the Notification Server computer. This information can be viewed through reports and the dashboard.

You can configure part or all of Patch Management Solution for Windows to automatically download and install future software updates. When configuring the solution, you should consider possible effects on your network environment. Symantec recommends that you distribute new updates to a test environment first.

What's new in Patch Management Solution for Windows 7.1

In the 7.1 release of Patch Management Solution, the following new features are introduced:

- The Software Management Solution Plug-in can be installed on 64-bit operating systems.
- The solution supports standard hierarchy editable properties.

  This feature lets you define which settings of replicated policies can be modified by the child Notification Server administrators.
- Hierarchy improvements.

  Improved performance of hierarchy-related reports. Policies are now using native Notification Server replication rules.

Where to get more information

Use the following documentation resources to learn about and use this product.

Table 1-1 Documentation resources

Document	Description	Location
Release Notes	Information about new features and important issues.	The **Product Support** page, which is available at the following URL: http://www.symantec.com/business/support/all_products.jsp When you open your product's support page, look for the **Documentation** link on the right side of the page.
User Guide	Information about how to use this product, including detailed technical information and instructions for performing common tasks.	■ The Documentation Library, which is available in the Symantec Management Console on the **Help** menu. ■ The **Product Support** page, which is available at the following URL: http://www.symantec.com/business/support/all_products.jsp When you open your product’s support page, look for the **Documentation** link on the right side of the page.
Help	Information about how to use this product, including detailed technical information and instructions for performing common tasks. Help is available at the solution level and at the suite level. This information is available in HTML help format.	The Documentation Library, which is available in the Symantec Management Console on the **Help** menu. Context-sensitive help is available for most screens in the Symantec Management Console. You can open context-sensitive help in the following ways: ■ The F1 key when the page is active. ■ The Context command, which is available in the Symantec Management Console on the **Help** menu.

In addition to the product documentation, you can use the following resources to learn about Symantec products.

Table 1-2 Symantec product information resources

Resource	Description	Location
SymWISE Support Knowledgebase	Articles, incidents, and issues about Symantec products.	http://www.symantec.com/business/theme.jsp?themeid=support-knowledgebase

Table 1-2 Symantec product information resources *(continued)*

Resource	Description	Location
Symantec Connect	An online resource that contains forums, articles, blogs, downloads, events, videos, groups, and ideas for users of Symantec products.	http://www.symantec.com/connect/endpoint-management

Implementing Patch Management Solution for Windows

This chapter includes the following topics:

Implementing Patch Management Solution for Windows

Patch Management Solution for Windows requires some components to be configured or enabled before others function correctly. When initially completing each task, you can also configure it for future automation. Automation is a key feature of Patch Management Solution for Windows as it reduces system administration workload and enhances overall security.

To implement Patch Management Solution for Windows

1. Install or upgrade the solution.

   See "Installing Patch Management Solution" on page 20.

   See "Upgrading Patch Management Solution" on page 20.

2. Install or upgrade the Symantec Management Agent on every computer to which you want to send patches.

   For more information, see topics about installing or upgrading the Symantec Management Agent in the *Symantec Management Platform User Guide*.

3 Install or upgrade the software update plug-in.

See "Installing the software update plug-in" on page 24.

See "Upgrading the software update plug-in" on page 24.

4 Configure the Patch Management Solution core settings.

See "Configuring patch management Core Services settings" on page 29.

5 Configure the software updates installation settings.

See "Configuring software updates installation settings " on page 31.

6 Configure the vulnerabilities check interval.

See "Configuring the inventory and vulnerabilities checking interval" on page 32.

7 Download the Adobe and Microsoft software updates catalog. Download the QChain software.

See "Downloading the software updates catalog" on page 40.

See "Downloading the QChain software" on page 41.

8 View which software updates you need to install, and then stage software bulletins.

See "Staging software bulletins" on page 47.

9 Create software update policies to distribute software updates.

See "Distributing software updates" on page 48.

10 Evaluate the results by running the **Software Update Delivery Summary** report and revisiting compliance reports.

See "Viewing the software update delivery summary report " on page 49.

See "Viewing Patch Management Solution reports" on page 56.

Chapter 3

Installing Patch Management Solution for Windows

This chapter includes the following topics:

Prerequisites for Patch Management Solution

Patch Management Solution requires the following:

- Symantec Management Platform 7.1.
  For more information, see topics about system requirements for Symantec Management Platform in the *Symantec Management Platform Installation Guide*.

When you install or upgrade Patch Management Solution through the Symantec Installation Manager, Symantec Management Platform is installed automatically.

See "Installing Patch Management Solution" on page 20.

Platforms supported by Patch Management Solution for Windows

The Patch Management Solution for Windows component of Patch Management Solution supports the following operating systems:

- Windows XP SP2 and later, 32-bit and 64-bit.
- Windows Vista SP1 and later, 32-bit and 64-bit.
- Windows 7, 32-bit and 64-bit.
- Windows Server 2003 SP2 and later, 2003 R2 SP2 and later, 32-bit and 64-bit.
- Windows Server 2008 32-bit and 64-bit, 2008 Core, 2008 R2, 2008 R2 Core.
- Windows Hyper-V Server 2008.

Installing Patch Management Solution

Starting from version 7.1, the Patch Management Solution installation includes the following components:

- Patch Management Solution for Windows
- Patch Management Solution for Linux
- Patch Management Solution for Mac

You install this product by using the Symantec Installation Manager. You can download the installation files directly to your server or you can create offline installation packages.

For details, see the ITMS 7.1 Implementation Guide at http://www.symantec.com/docs/DOC3464.

Upgrading Patch Management Solution

You upgrade this product by using the Symantec Installation Manager. You can download the installation files directly to your server or you can create offline installation packages.

For details, see the ITMS 7.1 Implementation Guide at http://www.symantec.com/docs/DOC3464.

After you upgrade the solution, you must upgrade the Symantec Management Agent, and the software update plug-in that are installed on the managed computers.

For more information about upgrading the Symantec Management Agent, see *Symantec Management Platform User Guide*.

See "Upgrading the software update plug-in" on page 24.

Uninstalling Patch Management Solution

Use the Symantec Installation Manager to uninstall this product.

Licensing Patch Management Solution

Each Symantec product comes with a seven-day trial license that is installed by default. You can register and obtain a 30-day evaluation license through the Symantec Web site at http://www.symantec.com/business/products/activating/ or purchase a full product license.

Use the Symantec Installation Manager to install licenses.

Note: Automatic upgrade protection (AUP) is required for continued use of Patch Management Solution for Windows. Without current AUP, you cannot download and use new Microsoft patch management metadata files. However, you can continue to use the Microsoft patch management metadata files that were downloaded before the expiration of AUP.

Installing the Software Update Plug-in

This chapter includes the following topics:

About the software update plug-in

The software update plug-in manages all of the Patch Management Solution for Windows functionality on a client computer. When the Inventory Rule Plug-in (distributed by default by Notification Server) reports that a certain software update is required for a managed computer, the update is sent to the software update plug-in. The software update plug-in ensures that the update is applicable and not already installed, and then installs it.

After you install the software update plug-in on a managed computer, the **Software Updates** tab appears in the Symantec Management Agent user interface. This tab displays the status software updates for that computer. To open the Symantec Management Agent user interface, click the Symantec Management Agent icon in the system tray of the managed computer.

See “Software update plug-in user interface” on page 25.

See “Installing the software update plug-in” on page 24.

Installing the software update plug-in

The software update plug-in manages all of the Patch Management Solution functionality on a client computer.

See “About the software update plug-in” on page 23.

Note: If you have a large number of computers on which to install the software update plug-in, consider deploying it during off-peak hours to minimize network traffic. Deploying the software update plug-in can take some time, depending on the number of managed computers and the Symantec Management Agent settings.

To install the software update plug-in

1. In the Symantec Management Console, on the **Settings** menu, click **Agents/Plug-ins > All Agents/Plug-ins**.
2. In the left pane, click **Software > Patch Management > Software Update Plug-in Install**.
3. (Optional) In the right pane, make any wanted changes.

   For help, press F1 or click **Help > Context**.
4. Turn on the policy.
5. Click **Save changes**.

Upgrading the software update plug-in

If you upgraded Patch Management Solution from a previous version, you must also upgrade the software update plug-ins that are installed on the target computers.

See “About the software update plug-in” on page 23.

To upgrade the software update plug-in

1. In the Symantec Management Console, on the **Settings** menu, click **Agents/Plug-ins > All Agents/Plug-ins**.
2. In the left pane, click **Software > Patch Management > Software Update Plug-in Upgrade**.
3. (Optional) In the right pane, make any wanted changes.

   For help, press F1 or click **Help > Context**.

4 Turn on the policy.

5 Click **Save changes**.

Uninstalling the software update plug-in

You can uninstall the software update plug-in if there is an extended period of time when you do not want to use the patch management features on a managed computer and you want to eliminate any overhead that is caused by the plug-in.

See “About the software update plug-in” on page 23.

Note: Ensure that the **Software Update Plug-in Install** policy is turned off before uninstalling the software update plug-in.

See “Installing the software update plug-in” on page 24.

To uninstall the software update plug-in

1 In the Symantec Management Console, on the **Settings** menu, click **Agents/Plug-ins > All Agents/Plug-ins**.

2 In the left pane, click **Software > Patch Management > Software Update Plug-in Uninstall**.

3 (Optional) In the right pane, make any wanted changes.

For help, press F1 or click **Help > Context**.

4 Turn on the policy.

5 Click **Save changes**.

Software update plug-in user interface

When the software update plug-in is installed on a managed computer, a **Software Updates** tab appears in the Symantec Management Agent. From this tab, users can view the software updates that are applicable to their computer. They can view the status of all received software updates: those that have been scheduled to be installed and those that have been recently installed.

See “About the software update plug-in” on page 23.

Table 4-1 Items in the software update plug-in user interface

Item	Description
Schedules	This pane lists all scheduled activities for the software update plug-in.
Show Updates	By checking or unchecking boxes, you can choose to show or hide software updates with the status listed next to each box. For example, uncheck **Not Currently Applicable** to hide any software updates not applicable to the managed computer.
Tasks	Click **Start Software Update Cycle** to manually start the installation of software updates rather than wait for scheduled times. This option is available only if **Allow user to run** is checked on the **Default Software Update Plug-in Policy** page.
Software updates for this computer	Displays the software updates that are applicable to this computer.
Icons in the **Status** column	■ A red error icon indicates that the maximum application retries for a failed software update have been exceeded. ■ A yellow warning icon indicates that the software update has failed to be applied at least once, but has not exceeded the maximum application retries. It is reapplied. ■ The green tick icon indicates that the Applicable rule is TRUE and the IsInstalled rule indicates that the update was installed. ■ A clock icon indicates that the Applicable rule is true and the IsInstalled rule is FALSE. The software update is scheduled for installation. ■ An information icon indicates that the Applicable rule has evaluated false. This means that the software update does not apply to this computer. You can also configure the agent not to display the software updates that do not apply by clearing the **Not Currently Applicable** check box in the **Show Updates** pane. ■ A user icon indicates that a user installed the update. ■ A download icon indicates that the plug-in is downloading or attempting to download a software update package. ■ A superseded icon indicates that the update was superseded by a later update and will not be installed.

Table 4-1 Items in the software update plug-in user interface *(continued)*

Item	Description
Text labels in the **Status** column	■ **Failed to Install** – The maximum application retries for a failed software update has been exceeded. ■ **Installation Failed – Rescheduled** – The software update has failed to be applied at least once but has not exceeded the maximum application retries. It will be reapplied. ■ **Installed** – The Applicable rule is TRUE and the IsInstalled rule indicates that it is already installed. If the Last Applied date is not empty, it means that the plug-in has installed the update. ■ **Installed by User** – The software update was applicable, but was installed before the Software Update policy has arrived to the computer. ■ **Installation Scheduled** – The Applicable rule is true and the IsInstalled rule is FALSE. The software update is scheduled for installation. ■ **Not Applicable** – The Applicable rule has evaluated false. This means that the software update does not apply to this computer. ■ **Pending** – The Applicable and IsInstalled rules have not yet been evaluated. ■ **Download required** – The rules have been evaluated and the update package needs to be downloaded to the agent. ■ **Retry** – An attempt to download the package has failed and the agent is trying to download the package again.
Bulletin Name	The name of the bulletin containing the software update.
Software Update Name	The name of the individual software update.
Last Applied	The date and time of the last applied download. The last install time is displayed only if the software update plug-in installs the software update. If the software update is already installed (another source installed the software update) when the software update plug-in goes to install it the first time, this field will display “Never”.
Schedule	Time of schedule means that this software update has been scheduled to be installed. Not scheduled means that this software update has not been scheduled to be installed.

Chapter 5

Configuring Patch Management Solution for Windows

This chapter includes the following topics:

Configuring patch management Core Services settings

On the **Core Services** page you can configure to which location the software updates should be downloaded. You can also create custom severity levels to apply to software updates.

The settings that you configure on the **Core Services** page apply to Windows and Linux components of Patch Management Solution.

To configure patch management Core Services settings

1. In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
2. In the left pane, click **Software > Patch Management > Core Services**.
3. In the right pane, make any wanted changes.

   See "Core Services page" on page 33.
4. Click **Save Changes**.

Creating and assigning custom severity levels

A software update deemed critical may not necessarily be critical in your environment. You can create your own custom severity levels and assign them to software bulletins.

You first create custom severity levels, and then assign them to bulletins. You cannot alter the vendor-specified severity levels, only custom severity levels.

See "About software updates and software bulletins" on page 45.

To create a custom severity level

1. In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
2. In the left pane, click **Software > Patch Management > Core Services**.
3. In the right pane, click the **Custom Severity** tab.
4. In the **Severity Level** box, type the name that you want to give the custom severity level. For example, "Install right away!"
5. Click **Add**.
6. Click **Move Up** or **Move Down** to position custom severity levels in the list.
7. Click **Save Changes**.

To assign a custom severity level to a software bulletin

1. In the Symantec Management Console, on the **Actions** menu, click **Software > Patch Remediation Center**.
2. On the **Patch Remediation Center** page, in the software bulletin list, right-click on a software bulletin, and then click **Custom Severity**.
3. Click a severity level.
4. Click **Refresh** to view the new data in the **Custom Severity** column.

Configuring vendor settings

You can set up how you want Microsoft or Adobe software updates distributed.

You can exclude Microsoft software updates that you do not use in your organization. Excluding software releases ensures that unnecessary files are not downloaded.

See “About software updates and software bulletins” on page 45.

To configure vendor settings

1. In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
2. In the left pane, click **Software > Patch Management**.
3. Do one of the following:
   - Click **Microsoft Settings > Microsoft**.
   - Click **Adobe Settings > Adobe**.
4. In the right pane, make any wanted changes.

   See “Vendor settings page” on page 33.
5. Click **Save changes**.

Configuring software updates installation settings

The **Default Software Update Plug-in Policy** page lets you configure when the software update plug-in can install software updates and restart the target computer.

See “About the software update plug-in” on page 23.

To configure the software updates installation settings

1. In the Symantec Management Console, on the **Settings** menu, click **Agents/Plug-ins > All Agents/Plug-ins**.
2. In the left pane, click **Software > Patch Management > Windows > Default Software Update Plug-in Policy**.
3. In the right pane, configure when and how do you want to install updates.

   See “Default Software Update Plug-in Policy page” on page 36.
4. Click **Save changes**.

Configuring the inventory and vulnerabilities checking interval

Vulnerability analysis let you periodically inventory operating systems, applications, and installed patches on managed computers with the software update plug-in installed. For example, the **Microsoft Vulnerability Analysis** policy detects vulnerabilities to known Microsoft security problems. Vulnerability information is then used to determine which software updates the managed computer requires. Based on this information, filters are automatically created to assist with the targeting of software update policies.

The **Microsoft Vulnerability Analysis** policy now incorporates four policies that were included in Patch Management Solution for Windows 6.2.

The policies are as follows:

- Default Windows OS Inventory Policy
- Default Windows Software Release Inventory Policy
- Default Microsoft Inventory Policy
- Default Microsoft Vulnerability Analysis Policy

You can configure how often you want to check for vulnerabilities.

To configure the vulnerabilities checking interval

1. In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
2. In the left pane, click **Software > Patch Management**
3. Click **Microsoft Settings > Microsoft Vulnerability Analysis** or **Adobe Settings > Adobe Vulnerability Analysis**.
4. In the right pane, in the **Scan interval** box, specify how often to report back inventory on the vulnerability of managed computers.
5. Click **Only if Changed** (set by default) if you want to report inventory only if it has changed, or click **Always**.
6. If you want to send a log of the results back to Notification Server, check **Send inventory summary**.
7. Do not change the targeted filter from **All Windows Computers with Software Update Plug-in Installed Target** unless you have a specific reason to do so.
8. Click **Save changes**.

Core Services page

The **Core Services** page lets you configure to which location the software updates should be downloaded. You can also create custom severity levels to apply to software updates.

(Patch Management Solution for Windows only) You can select any additional languages that you want to download with the **Patch Management Import** task.

The settings that are defined on this page apply to Windows and Linux components of Patch Management Solution.

See "About software updates and software bulletins" on page 45.

See "Configuring patch management Core Services settings" on page 29.

See "Creating and assigning custom severity levels" on page 30.

Table 5-1 Options on the **Core Services** page

Option	Description
Managed Languages	(Patch Management Solution for Windows only) Specifies the languages that you want to download.
To Location	Specifies the location to which you want to download the software update packages. The default location is C:\Program Files\Altiris\Patch Management\Packages\Updates. If you change the location and you want to relocate existing software update packages, use the **Check Software Update Package Integrity** task. See "Checking the integrity of software update packages " on page 41.
Download from staging location	(Patch Management Solution for Windows only) Specifies the location to download packages from if you want to download them from a cache in a different location. For this functionality to work, the file structure in that location must be exactly the same as the folder structure under C:\Program Files\Altiris\Patch Management\Packages\Updates.

Vendor settings page

This page lets you set up how you want vendor software updates distributed.

See “Configuring vendor settings” on page 31.

Some of these settings are used as default values on the **Software Update Policy Wizard** page. All new vendor software updates that are downloaded have these settings by default.

If you change the settings, existing software update policies and packages are not updated with these defaults. If you want to update existing packages, check **Update new package settings for already downloaded packages** on the **Policy and Package Settings** tab.

See “Distributing software updates” on page 48.

See “Patch Remediation Center page ” on page 49.

Table 5-2 Options on the **Software Update Options** tab of the vendor settings page

Option	Description
Patch Filter Update Interval	Specifies when to update the target filters for all software updates. By default, the filter update is performed every 30 minutes.
Resource Exclusions	(Microsoft vendor policy only) Lets you select the software releases to exclude from download. For example, you can exclude the software releases that are not used in your organization. Excluding software releases ensures that unnecessary files are not downloaded.
Software Update Distribution Options	The table shows the filter that the policy targets. The default target is **All Windows Computers with Software Update Plug-in Installed Target**.

Table 5-3 Options on the **Policy and Package Settings** tab of the vendor settings page

Option	Description
Delete packages after	Lets you specify when to delete the software update packages that are no longer needed. Default: 1 week.

Table 5-3 Options on the **Policy and Package Settings** tab of the vendor settings page *(continued)*

Option	Description
Use multicast when the Symantec Management Agent's multicast option is enabled	Check if you want to use multicast when distributing software update packages. For more information on multicasting, see the *Symantec Management Platform User Guide*.
Allow Package Server distribution	This option is checked by default to ensure that package servers process software update packages. For more information on package servers, see the *Symantec Management Platform User Guide*.
Assign package to	Lets you select the package distribution method. For more information on assigning packages to package servers, see the *Symantec Management Platform User Guide*.
Use alternate download location on Package Server	Lets you specify a different location on a package server to which to download packages. If you are using Linux Package Servers in your envirionment, the Windows path that you specify is converted to UNIX paths automatically. You must use the trailing slash for the conversion to work correctly. For example, C:\path\ is converted to /path/ on Linux Package Servers.
Use alternate download location on client	Lets you specify a different location on the managed computers to which to download packages.
Update new package settings for already downloaded packages	By default, the changes that you make on this page are not applied to the packages that have already been downloaded. Check this option if you want to update the existing package settings after you click **Save Changes**. Only the packages from the current vendor will be updated.

Table 5-4 Options on the **Programs** tab of the vendor settings page

Option	Description
Terminate after	Lets you specify a time after which to terminate a running software update program.
Run with rights	Lets you specify which account to use to run the program. If you select the Specified User, you must specify user domain information.
Program can run	Lets you specify the conditions in which the program can run.
Agent Events	Sends relevant events from managed computers to Notification Server.

Default Software Update Plug-in Policy page

This page lets you specify settings (including install and restart options) the software update plug-in uses when you install software updates on managed computers.

The default resource target for the policy is designed to find any agents that do not have another software update plug-in configuration policy applied to them. For this reason, the default resource target cannot be changed. If you want to change the default resource target, you must clone the policy and alter the resource target on the clone.

By default, the settings that you specify on this page apply to all Windows computers that have the software update plug-in installed.

See "About the software update plug-in" on page 23.

See "Configuring software updates installation settings " on page 31.

Table 5-5 Options on the **Installation Schedules** tab of the **Default Software Update Plug-in Policy** page

Option	Description
Schedule	Lets you configure a schedule when software updates get installed on the managed computer. This schedule appears on the **Software Updates** tab of the Symantec Management Agent on the target computer.
Reinstallation attempts after task failure	Lets you set the number of times Patch Management Solution for Windows should attempt to reinstall a software update if the initial install attempt fails. Default: 3 times.

Table 5-5 Options on the **Installation Schedules** tab of the **Default Software Update Plug-in Policy** page *(continued)*

Option	Description
Allow user to run	Lets a user initiate a software update installation from the Symantec Management Agent by clicking **Start Software Update** in the Symantec Management Agent user interface.
Allow restart after installation	Lets you specify when to restart the managed computer after software updates are installed.
Never	Do not automatically restart the target computer after a software update installation.
Scheduled	Restart the computer on a specific schedule. For example, use this option to create an after hours restart schedule if you do not want to affect user productivity with repeated restarts during work hours. Symantec recommends that you do not set your restart schedule too soon after the software update installation schedule. This schedule appears on the **Software Updates**tab of the Symantec Management Agent on the target computer.
At end of software update cycle	Select this option to restart after all updates in a single update cycle have been installed.
Override maintenance windows settings	Check if you want to use the install and the restart options that you specified in this policy. Uncheck to abide by the maintenance windows that are specified in Notification Server configuration policies.

Table 5-6 Options on the **Notification** tab of the **Default Software Update Plug-in Policy** page

Options	Description
Notify user	Check if you want to send a message to the users of the computer where a patch management task is about to run. Specify for how long the message should be displayed before a task is run. You can type a custom message: for example, “Software updates will install on your computer in 10 minutes. Please ensure that all work is saved”. When the message appears, the user can choose to install the updates immediately or close the dialog box.
Show progress message	Lets you choose to show users a dialog box indicating the progress of software update installations.
Show pending message	Lets you choose to warn users of a pending restart. The time you select represents how soon before the pending restart the user is warned. The user can choose to restart immediately.
Show reminder message	Lets you choose to notify a user that a restart is required. You can specify a schedule on which to display the notification. The user can choose to restart later, or restart immediately. If the user does not manually restart, the restart occurs according to your settings on the **Installation Schedules** tab.
Allow user to defer	Lets you choose to warn a user of a pending restart. Specify for how long the user can defer the restart. The user can choose to restart immediately, or defer the restart.

Chapter 6

Configuring Patch Management server tasks

This chapter includes the following topics:

About Patch Management Solution server tasks

You must configure server tasks (previously known as background actions) to run automatically at regular intervals. Examples of server tasks include **Import Patch Data for Microsoft**, **Import Patch Data for Adobe**, and **Download QChain**. Automated server tasks ensure that you have the latest, most accurate data, and your software update tasks are kept up to date. To configure a task to run automatically, set a schedule for it.

The **Import Patch Data for Microsoft** task downloads Microsoft software updates catalog files and imports all software management resources from these files into the CMDB. The **Import Patch Data for Adobe** task does the same for Adobe software updates. The **Microsoft QChain** task chains the Microsoft software updates together before they are distributed to managed computers. Other server tasks ensure data integrity or assist in automating software update distribution processes.

The **Import Patch Data for Microsoft**, **Import Patch Data for Adobe**, and **Download QChain** tasks must successfully run before you can stage or distribute any software updates.

See "Implementing Patch Management Solution for Windows" on page 17.

See "Downloading the software updates catalog" on page 40.

See "Downloading the QChain software" on page 41.

Downloading the software updates catalog

You must download the Microsoft and Adobe software updates catalog files (patch management metadata, or patch management import files) before you can stage software updates or create software update policies.

See "Implementing Patch Management Solution for Windows" on page 17.

Note: If the Altiris Log Viewer is open, close it before you perform this task. By closing the viewer, you can improve the task's performance by as much as 50 percent.

You may want to create a schedule for this task as well. This procedure ensures that you have the latest, most accurate data, and your software update tasks are kept up to date. Symantec recommends that you configure the task to run daily.

To download the software updates catalog immediately

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, expand **Jobs and Tasks > System Jobs and Tasks > Software > Patch Management**.
3. Click one of the following:
   - **Import Patch Data for Microsoft**
   - **Import Patch Data for Adobe**
4. (Optional) In the right pane, make any wanted changes and then click **Save changes**.

   See "Import Patch Data for Microsoft and Import Patch Data for Adobe pages" on page 42.
5. Under **Task Status**, click **New Schedule**.
6. In the **New Schedule** dialog box, click **Now**, and then click **Schedule**.

To configure a schedule for downloading the software updates catalog

1. On the **Import Patch Data for Microsoft** or **Import Patch Data for Adobe** page, under **Task Status**, click **New Schedule**.
2. In the **New Schedule** dialog box, click **Schedule**, and then configure a schedule on which to run this task.

   Symantec recommends that you configure the task to run daily.
3. Click **Schedule**.

Downloading the QChain software

QChain is an executable that groups software updates together before you distribute them to managed computers. QChain removes the need of a computer restart after an individual update is installed.

Patch Management Solution for Windows downloads QChain from the Microsoft Web site automatically after you install the solution through the Symantec Installation Manager.

If you want, you can download QChain manually. For example, you may want to do this if you see that the task has failed to run the first time.

See “Implementing Patch Management Solution for Windows” on page 17.

To download QChain

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, expand **Jobs and Tasks > System Jobs and Tasks > Software > Patch Management**, and then click **Download QChain**.
3. (Optional) In the right pane, make any wanted changes and then click **Save changes**.

   See “Download QChain page” on page 43.
4. Under **Task Status**, click **New Schedule**.
5. In the **New Schedule** dialog box, click **Now**, and then click **Schedule**.

Checking the integrity of software update packages

You can verify that software update packages in software update tasks have the correct global server settings applied. If you changed settings in a vendor policy, run the **Check Software Update Package Integrity** task to check that all software update packages have the correct new settings and values.

See “Configuring vendor settings” on page 31.

The task also relocates the software update packages in case you changed the default software update package location on the **Core Services** page.

See “Configuring patch management Core Services settings” on page 29.

To check the integrity of software update packages

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, expand **Jobs and Tasks > System Jobs and Tasks > Software > Patch Management**, and then click **Check Software Update Package Integrity**.
3. If you want to delete the downloaded updates that are not part of any software update policy or belong to a superseded bulletin, check **Delete updates from file system that are no longer in use**.
4. If you want to relocate downloaded updates if the **Software Update Package Location** has changed, check **Relocate existing packages if default Software Update Package location on Core Service page has changed**.

   See “Configuring patch management Core Services settings” on page 29.
5. Under **Task Status**, click **New Schedule** and specify a schedule on which to run the task.

Import Patch Data for Microsoft and Import Patch Data for Adobe pages

This background action downloads the software update catalog files and imports all software management resources from these files into the CMDB. These resources are necessary for populating the **Patch Remediation Center** and updating patches to managed computers. When you download the software update catalog files, you automatically import all software management resources.

See “Downloading the software updates catalog” on page 40.

Table 6-1 Options on the **Import Patch Data** page

Option	Description
Default Location	The default location from which the patch management metadata files are downloaded.
Alternative Location	Lets you specify a custom location from which to download the patch management metadata files.

Table 6-1 Options on the **Import Patch Data** page *(continued)*

Option	Description
Only download if modified	Ensures that only updated files are downloaded, thus avoiding unnecessary downloads.
Automatically revise software update policies after Patch Management Import	Automatically updates software update policies with the latest Microsoft patch management metadata. Each download of the patch management metadata files may contain data and fixes for existing software updates. By checking this option, you can use the new data to resolve any known issues with software updates.
Enable distribution of newly added software updates	Enables the distribution of the software update packages that were added to the software bulletin.
Disable all Superseded Software Updates	This option disables the rollout of any software update tasks containing superseded software updates.

Download QChain page

The QChain is an executable that groups software updates together before you distribute them to managed computers. You must download QChain after you run the **Import Patch Data for Microsoft** task and before you distribute software updates.

See "Downloading the QChain software" on page 41.

Table 6-2 Options on the Download QChain page

Option	Description
Location	The location from which the QChain files are downloaded.
Only download if modified	Ensures that only updated files are downloaded, thus avoiding unnecessary downloads.
Retry failed downloads	The number of times to retry downloading the QChain files before the task fails.

Chapter 7

Staging and distributing software bulletins and software updates

This chapter includes the following topics:

About software updates and software bulletins

A software update or patch is any update or hotfix that is used to improve or fix a software product. A software bulletin is a bundle of software updates that are released together.

Patch Management Solution for Windows uses targeted deployments. Updates are not deployed to a computer unless that computer specifically needs that software update. If a managed computer meets the prerequisites of a software update, it falls into a targeted filter. The prerequisites are matched against the data that is sent to Notification Server by the software update plug-in: for example, the Internet Explorer and operating system versions. Software updates are then installed according to Microsoft specifications. For example, if Microsoft requires a restart, then the computer is restarted after the update is installed. Restarts on managed computers are minimized because the updates that do not require a restart are installed before the software updates that do.

When a software update has been superseded and rendered obsolete by another update or updates, the later update is installed.

Microsoft assigns severity levels to software updates, but you can also create a custom severity level.

See "Creating and assigning custom severity levels" on page 30.

Warning: Microsoft provides the software updates that Patch Management Solution for Windows distributes for Microsoft products. You must ensure that each software update works correctly in your environment before deploying it. Symantec recommends that you first distribute any required software update in a test environment before deploying it to your production environment.

About staging and distributing software bulletins

You stage software bulletins from the **Patch Remediation Center** page, where all available software updates are listed.

When you stage a software bulletin, all associated updates are downloaded to the Notification Server computer.

When the number in the **Updates** column equals the number in the **Downloaded** column, all updates for the software bulletin have been downloaded. Also, the value in the **Staged** column changes to **True**.

See "Staging software bulletins" on page 47.

After the bulletin is staged, you can create software update policies to distribute the software update to managed computers.

Sometimes not all software updates can be downloaded for a software bulletin because Microsoft may stop hosting the bulletin or relocate it. You cannot create a software update policy unless all updates for a particular software bulletin or update have been downloaded.

See "Distributing software updates" on page 48.

Staging software bulletins

You can stage a software bulletin to download associated updates.

See "About staging and distributing software bulletins" on page 46.

You can stage all software bulletins. However, Symantec recommends that you stage only the bulletins that the target computers require. On the **Patch Remediation Center** page, in the compliance reports, you can view how many computers require an update.

After the updates are downloaded, you must create a software update policy to distribute the updates to managed computers.

See "Distributing software updates" on page 48.

When you stage a software bulletin, a task is created that downloads the software updates. You can view the status of this task to troubleshoot downloading of software updates.

To stage a software bulletin

1. In the Symantec Management Console, on the **Actions** menu, click **Software > Patch Remediation Center**.
2. In the right pane, in the **Show** drop-down box, click **Microsoft Compliance by Bulletin** or **Adobe Compliance by Bulletin**, and then click the **Refresh** symbol.

   These reports let you see which updates the target computers require.
3. Click the bulletins that you want to stage.

   For example, click the bulletins that have a high number in the **Vulnerable** column.
4. Right-click the selected bulletins, and then click **Stage**.

   If the **Stage** option is not available, the bulletin is being staged. If there is a **Software Update Policy Wizard** option available in the menu, the bulletin is staged and ready to be distributed.

   See "Distributing software updates" on page 48.

To view the status of a software bulletin download

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, click **Jobs and Tasks > System Jobs and Tasks > Software > Patch Management > Download Software Update Package**.
3. In the right pane, view the status of download tasks.

Distributing software updates

After you stage software bulletins and download the associated software updates, you must create software update policies that deploy software updates to the appropriate computers.

See "Staging software bulletins" on page 47.

The **Software Update Policy Wizard** page lets you create software update policies.

The policies that you create are stored in the **Manage > Policies > Software > Patch Management > Software Update Policies** folder. You can view the details of the policy and change settings if necessary.

To distribute software updates

1. In the Symantec Management Console, on the **Actions** menu, click **Software > Patch Remediation Center**.
2. In the right pane, in the **Show** drop-down box, click **Microsoft Compliance by Bulletin** or **Adobe Compliance by Bulletin**, and then click the **Refresh** symbol.

   These reports let you see which updates the target computers require.
3. Click the bulletins that you want to distribute.

   For example, click the bulletins that have a high number in the **Vulnerable** column.
4. Right-click the selected bulletins, and then click **Software Update Policy Wizard**.

   If the **Software Update Policy Wizard** option is not available, the bulletin is not staged. You must first stage the bulletin.

   See "Staging software bulletins" on page 47.
5. (Optional) Configure the settings as needed.

   See "Software Update Policy Wizard pages " on page 51.
6. Click **Next**.
7. (Optional) On the second page of the wizard, check the updates that you want to distribute.
8. If you want to activate the new software update policy, turn on the policy. To turn on the policy, click on the colored circle and then click **On**.

   You can also turn on the policy later.
9. Click **Distribute software updates**.

Viewing the software update delivery summary report

The **Windows Software Update Delivery Summary** report summarizes the results of all scheduled Microsoft software update policies. It tells you which computers the software update tasks target, and if the updates have been successfully installed. The report also tells you if any software update tasks failed, or if they have not yet completed.

Patch Management Solution for Windows also provides other reports that you can view.

See "About Patch Management Solution reports" on page 53.

To view the software update delivery summary report

1. In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
2. In the left pane, click **Software > Patch Management > Remediation Status > Windows Software Update Delivery Summary**.
3. In the right pane, leave the default settings, and then click **Refresh**.

About software update policies and maintenance windows

Maintenance windows are time periods in which maintenance tasks, including the installation of software updates, are performed. To ensure that software update policies abide by maintenance windows, leave the **Override Maintenance Window Settings** check box unchecked in the first page of the **Software Update Policy Wizard**. If the box is checked, the software update plug-in ignores maintenance windows and installs the updates as instructed otherwise by the software update policy.

See "Software Update Policy Wizard pages " on page 51.

Installing a software update may take longer than a specified maintenance window. In this case, the installation of the updates completes, but any required restarts are deferred until the next maintenance window.

Patch Remediation Center page

This page lets you view, stage, and distribute all software updates that are provided by software update catalog files.

See "About staging and distributing software bulletins" on page 46.

See “About software updates and software bulletins” on page 45.

Table 7-1 Items on the **Patch Remediation Center** page

Item	Description
Bulletin	The bulletin's number, as supplied by the vendor.
Severity	The bulletin's vendor-specified severity level.
Custom Severity	The bulletin's user-defined severity level.
Staged	Indicates if the bulletin has been set to download included software updates. If all updates have been downloaded, the result is **True**. Otherwise it is **False**.
Policies	The number of software update policies that have been created from the bulletin.
Updates	The number of software updates that are included in the bulletin.
Downloaded	The number of software updates currently downloaded.
Released	The date the bulletin was released.
Revised	The date the bulletin was revised.
Description	A description of the vulnerabilities that the software bulletin addresses.

Table 7-2 Right-click actions on the **Patch Remediation Center** page

Item	Description
View Targeted Computers	Displays the computers that the software update policy containing this bulletin is targeting. You must create a software update policy to view targeted computers.
View Applicable Computers	Displays the computers to which the selected bulletin applies.
View Installed Computers	Displays the computers on which the selected bulletin is installed.
View Vulnerable Computers	Displays the computers that do not have the selected bulletin installed.

Software Update Policy Wizard pages

The software update policy wizard creates the software update policies that distribute software updates to managed computers. A software update policy that is created from a software bulletin includes every software update that is in the bulletin.

See "Distributing software updates" on page 48.

Table 7-3 Options on the first page of the **Software Update Policy Wizard**

Option	Description
Software Updates	The names of each software update that is included in the bulletin.
Software Bulletins	The name of the bulletin or bulletins you have chosen to make policies for. You cannot edit the software bulletins through the software update policy wizard. You can click a software bulletin to open the Resource Manager to view detailed information on the software bulletin. You can only select a software bulletin that has been previously staged.
Name	The name of the policies you have chosen from the policies window. This field is populated automatically if only one policy is listed in the Tasks field.
Description	The vendor description of the bulletin.
Use Multicast when the Symantec Management Agent's multicast option is enabled	(Patch Management Solution for Windows only) Enables multicast features.
Run (other than agent default)	Runs the software updates installation at a different time than the time that is specified in the software update plug-in settings. See "Configuring software updates installation settings " on page 31.
As soon as possible	Runs the software updates installation as soon as the software update policy arrives to the target computer.
Power on computer (Wake on LAN)	(Patch Management Solution for Windows only) Attempts to turn on the computer before installing software updates.

Table 7-3 Options on the first page of the **Software Update Policy Wizard** *(continued)*

Option	Description
On schedule	Runs the software updates installation on a schedule.
Override Maintenance Windows settings	Overrides the specified maintenance windows settings. See "About software update policies and maintenance windows" on page 49.
Apply to computers	Lets you specify the target collection or collections to which the software update policy applies. If you use the software update policy wizard, the correct resource target for the selected software bulletin is automatically applied.

Table 7-4 Options on second page of the Software Update Policy Wizard

Options	Description
On/Off	Lets you enable or disable the software update policy for the software bulletin and included software updates. Click **On** if you want the policy to become active after you complete the wizard. You can also turn on the policy later. The policies that you create are located at **Manage > Policies > Software > Patch Management > Software Update Policies**.
Software Bulletin	The name of the software bulletin.
Update Name	The name of each software update executable. If Enable is selected, all of the executables are enabled. Click the hyperlink to open the **Resource Manager** page for the software update.
Culture	The language and culture of the software update.
Package	The software package that is associated with the update. Click the hyperlink to open the package's Resource Manager.
Command Line	The command line to be run against the package. Click the hyperlink to open the command-line options dialog box to change the recommended options.

Chapter 8

Using Patch Management reports

This chapter includes the following topics:

About Patch Management Solution reports

You can view and manage your patch management data through reports. These reports give you information specific to Patch Management Solution. For example, you can use compliance reports to determine how many urgent software updates your managed computers require.

See "About compliance reports" on page 54.

Reports let you view information in various ways. You can see your information in tables or graphically in charts. You can also drill down on specific items in a report to obtain additional information.

You can stage or distribute software updates directly from reports by right-clicking on the update name in the report.

Patch Management Solution provides the following reports:

- Compliance reports
  See "About compliance reports" on page 54.
- Diagnostic reports
  See "About diagnostic reports" on page 55.
- Remediation status reports
  See "About remediation status reports" on page 55.
- Software bulletin reports
  See "About software bulletin reports " on page 55.

See "Viewing Patch Management Solution reports" on page 56.

Patch Management Solution also has a patch management home page. This page is a portal page that is comprised of a number of Web parts displaying results from commonly used reports.

See "About the Patch Management Solution for Windows home page" on page 55.

About compliance reports

Compliance reports are the key to quickly determining what software updates your managed computers require. Compliance reports are used to determine if computers are up-to-date with the latest software updates. These reports are also used to check if a particular software bulletin or update is installed on your managed computers. This is useful if a specific security issue affects your network environment and a certain update addresses the problem.

You can start distributing software updates directly from report results. For example, if you want to quickly distribute all critical updates, sort the report results by **Severity**. Then, right-click all critical updates and click **Stage**. Then you can distribute the updates.

See "About staging and distributing software bulletins" on page 46.

You can find the compliance reports in the Symantec Management Console under **Reports > All Reports > Software > Patch Management > Compliance**.

Compliance reports are also featured on the Patch Management Solution home page for easy access.

See "About the Patch Management Solution for Windows home page" on page 55.

See "About Patch Management Solution reports" on page 53.

About diagnostic reports

The diagnostics reports display vulnerability summary and software update plug-in installation information.

You can find the diagnostics reports in the Symantec Management Console under **Reports > All Reports > Software > Patch Management > Diagnostics**.

See "About Patch Management Solution reports" on page 53.

About remediation status reports

The remediation status reports summarize and detail software update associations and activities.

You can find the remediation status reports in the Symantec Management Console under **Reports > All Reports > Software > Patch Management > Remediation Status**.

See "About Patch Management Solution reports" on page 53.

About software bulletin reports

The software bulletins reports summarize and detail software bulletin activity and status.

You can find the remediation status reports in the Symantec Management Console under **Reports > All Reports > Software > Patch Management > Software Bulletins**.

See "About Patch Management Solution reports" on page 53.

About the Patch Management Solution for Windows home page

The home page is a portal page providing patch management summary information at a glance. The page is comprised of a number of Web parts displaying results from commonly used reports.

See "About Patch Management Solution reports" on page 53.

You cannot customize the portal page directly. If you want, you can add patch management Web parts to other configurable portal pages. For example, the **My Portal** page.

You can access the home page by clicking **Home > Patch Management**, and then, under **Microsoft**, click **Updates**.

Only the **Windows Compliance** home page is available. A home page for Adobe is not available.

Table 8-1 Web parts on the **Windows Compliance** page

Web part	Description
Microsoft License Status	Reports on the amount of Patch Management Solution for Windows licenses in use, their status, and expiration date.
Microsoft Vulnerabilities	Reports on the number of Microsoft vulnerabilities that need to be addressed. This Web part is also available in a graph form.
Microsoft Software Update Delivery Summary	Reports on the number of patches that were executed in the past 30 days and how many succeeded or did not complete. This Web part is also available in a graph form.
Microsoft Software Bulletin Summary	Reports on the number of software bulletins available, staged, tasks created, and new bulletins in the last 30 days. This Web part is also available in a graph form.
Microsoft Configuration Summary	An overall configuration summary, which includes computers with the software update plug-in, computers not reporting vulnerability analysis, Microsoft patch management metadata and QChain versions, and so on.

Viewing Patch Management Solution reports

Patch Management Solution for Windows provides reports that let you view detailed information about the updates.

See "About Patch Management Solution reports" on page 53.

To view Patch Management reports

1 In the Symantec Management Console, on the **Reports** menu, click **All Reports**.

2 In the left pane, expand **Software > Patch Management**.

3 Click the report that you want to view.

For example, click **Compliance > Windows Compliance by Bulletin**.

4 In the right pane, leave the default settings, and click **Refresh**.

5 If you want to view more information about an update, right-click on any update, and click **Resource Manager**.

Each type of compliance report opens a different Resource Manager , depending on the type of results. For example, the **Windows Compliance by Computer** report opens a computer-type Resource Manager. At the bottom of the **Summaries** tab, under **Additional Information**, click the hyperlink to the Microsoft Technet article on the bulletin.

Replicating Patch Management data in hierarchy

This chapter includes the following topics:

About replicating Patch Management Solution for Windows data

Downloading Microsoft and Adobe software update catalog files (patch management metadata, or patch management import files) to multiple Notification Servers can consume considerable network resources and time. Notification Server hierarchy features remove the need to download patch management metadata files individually. You can download the files once to a single parent Notification Server. Then you can use Patch Management Solution replication rules to send the relevant data to any number of child Notification Servers. The replicated data on the child Notification Servers is identical to the data on the parent.

See "About hierarchy and data replication direction" on page 65.

Before you can replicate data, you must run the **Patch Management Language Alerting** rule.

See "About the Patch Management Language Alerting rule" on page 60.

See "Replicating patch management language alerts" on page 60.

See "About software update catalog replication" on page 61.

See "Replicating the software updates catalog" on page 61.

See "About software update policy replication" on page 62.

See "Replicating a software update policy manually " on page 62.

About the Patch Management Language Alerting rule

Different Notification Servers within a hierarchy may manage different patch management language resources. The **Patch Management Language Alerting** replication rule ensures that child Notification Servers only receive data and software update policies for their managed languages. This rule replicates information about the managed languages of the child Notification Server up to the parent. You must run this rule on a child before any attempt is made to replicate patch management data or software update policies. A parent Notification Server must manage all of the languages that its children require.

The rule is preconfigured to run daily at 20:00.

See "Replicating patch management language alerts" on page 60.

Replicating patch management language alerts

You must run the **Patch Management Language Alerting** rule on a child before any attempt is made to replicate the software update catalog or software update policies.

See "About the Patch Management Language Alerting rule" on page 60.

To replicate patch management language alerts

1. In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Hierarchy**.
2. In the left pane, click **Hierarchy > Hierarchy Management**.
3. In the right pane, click the **Replication** tab.
4. Expand the **Resources** section.

5 Click **Patch Management Language Alerting**.

6 Click the **Edit** symbol.

7 Set a schedule to run before running other patch management replication functions.

About software update catalog replication

Downloading Microsoft or Adobe patch management software update catalog files to multiple Notification Servers can consume considerable network resources. Notification Server hierarchy features remove the need to download patch management software update catalog files individually. You can download the files once to a single parent Notification Server. Then you can use the **Patch Management Import Data Replication for Microsoft** and **Patch Management Import Data Replication for Adobe** rules to send the relevant data to any number of child Notification Servers. The replicated data on the child Notification Servers is identical to the data on the parent, depending on managed languages.

The rules are preconfigured to run daily at 23:00.

See "Replicating the software updates catalog" on page 61.

Replicating the software updates catalog

After downloading Microsoft or Adobe software updates catalog files and importing data to a parent Notification Server, you can replicate the data to any number of child Notification Servers.

See "About software update catalog replication" on page 61.

Warning: You must configure the **Patch Management Language Alerting** rule to run before the software catalog data replication.

See "About the Patch Management Language Alerting rule" on page 60.

To replicate the software updates catalog

1 In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Hierarchy**.

2 In the left pane, select **Hierarchy > Hierarchy Management**.

3 In the right pane, click the **Replication** tab.

4 Expand the **Resources** section.

5. Click **Patch Management Import Data Replication for Microsoft** or **Patch Management Import Data Replication for Adobe**.
6. Click the **Edit** symbol.
7. Under **Replicate**, select **Differential** if you want to only replicate changed or new data. Select **Complete** to send all Microsoft patch management software update catalog files to child Notification Servers each time the task runs.
8. Under **Schedule**, create a custom schedule or select the standard replication schedule.
9. Under **Data Verification**, specify a percentage of data to be verified during each replication, and check **Verify data integrity** if wanted.
10. Turn on the rule.
11. Click **Save changes**.

About software update policy replication

Software update policies distribute software updates to the target computers.

See "Distributing software updates" on page 48.

In Patch Management Solution 7.1, the software update policies are always replicated to child Notification Servers. Replication occurs on the default Notification Server replication schedule.

You can also replicate a software update policy manually.

See "Replicating a software update policy manually " on page 62.

Replicating software update policies does not replicate the actual software update files. Child Notification Servers download the needed software update files from the vendor.

Replicating a software update policy manually

You can save time and resources by replicating existing software update policies to child Notification Servers.

See "About software update policy replication" on page 62.

All software update policies are replicated to child Notification Servers on the default replication schedule. If you want, you can also manually replicate a policy immediately.

Warning: Before you replicate software update policies, ensure that the **Patch Management Language Alerting** rule and the **Patch Management Import Data Replication** rule have run.

See "About the Patch Management Language Alerting rule" on page 60.

See "About software update catalog replication" on page 61.

To replicate a software update policy manually

1. In the Symantec Management Console, on the **Manage** menu, click **Policies**.
2. In the left pane, expand **Software > Patch Management > Software Update Policies**.
3. Right-click a policy, and then click **Hierarchy > Replicate Now**.

Technical reference

This appendix includes the following topics:

- About hierarchy and data replication direction
- About Patch Management Solution security roles

About hierarchy and data replication direction

Patch Management Solution for Windows and Patch Management Solution for Linux support the hierarchy and the replication features of the Symantec Management Platform. These features let you create settings, schedules, and other data at the top-level Notification Server computer and replicate them to child-level Notification Server computers.

Patch Management Solution for Mac does not support replication.

See "About replicating Patch Management Solution for Windows data" on page 59.

Table A-1 Items that are replicated by the default Notification Server replication schedule with no custom replication rules

Item	Replication direction
All the server tasks settings and schedules: ■ **Download QChain** ■ **Check Software Update Package Integrity** ■ **Import Patch Data for Microsoft/Adobe/Red Hat/Novell**	Down
Microsoft/Adobe/Linux Vulnerability Analysis policy settings	Down
Microsoft/Adobe/Red Hat/Novell vendor settings	Down
Default Software Update Plug-in Policy settings	Down

Table A-1 Items that are replicated by the default Notification Server replication schedule with no custom replication rules *(continued)*

Item	Replication direction
Software update plug-in install, upgrade, and uninstall policy settings	Down
Software update policies	Down

Table A-2 Items that are replicated with custom replication rules

Item	Replication direction	Description
Language support information (Patch for Windows only)	Up	This information is replicated when the **Patch Management Language Alerting** rule is enabled.
OS inventory data (Patch for Linux only)	Up	This information is replicated when the **Patch Linux OS Channel Resource Replication** rule is enabled.
Patch management metadata	Down	This information is replicated when the **Patch Management Import Data Replication for Adobe/Microsoft/Red Hat/Novell** rules are enabled. For Windows, only the updates and bulletins that are associated with the child computer's supported languages are replicated. For Linux, only the metadata for the channels that are relevant to the child Notification Server's client computers is replicated.
Compliance summary	Up	This information is replicated when the **Patch compliance summary replication** rule is enabled. The vulnerability analysis is replicated up as a summary.

About Patch Management Solution security roles

You can assign the following security roles to Symantec Management Console users:

- **Patch Management Administrators**
- **Patch Management Rollout**

Users with **Patch Management Administrators** role have full access to Patch Management Solution functionality, but no access to the rest of the Symantec Management Console.

Users with **Patch Management Rollout** role have limited access to the following Patch Management Solution functionality:

- Software update policies
- Reports
- Patch Remediation Center page

Users with the **Patch Management Rollout** role can perform the following actions:

- Enable, disable, and change settings in the software update policies .
- View reports.

Index