Altiris™ Patch Management Solution for Windows® 7.1 SP2 from Symantec™ User Guide

Altiris™ Patch Management Solution for Windows® 7.1 SP2 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

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

See "*Altiris™ Patch Management Solution for Windows 7.1 SP2 from Symantec™ Third-Party Legal Notices*" on page 75.

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 lets you inventory managed computers to determine the software updates (patches) that they require. The solution then lets you download the required software updates from the software vendor and provides you with the tools to install the software updates. Software updates include but are not limited to security updates, hot fixes, and service packs. Software from vendors such as Microsoft, Adobe, Mozilla, Google, Sun Microsystems, and many others can be patched.

See “Software that Patch Management Solution for Windows supports” on page 13.

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 you complete the installation of the solution.

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.

What's new in Patch Management Solution for Windows 7.1 SP2

The 7.1 SP2 release of Patch Management Solution for Windows includes enhancements to refine product quality.

See “About Patch Management Solution for Windows” on page 11.

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 bulletins, 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 the vendors. 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. Inventory includes 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 25.

You use the **Distribute Software Updates** wizard to automate the downloading and distribution of software updates. Instead of creating a policy for each individual software update, you use this wizard to create a single policy for the relevant software bulletins. You can add multiple software bulletins to a policy. If you want to, you can modify any default settings and command-line options in a software update policy.

When you download a software bulletin, each associated software update executable is downloaded from the vendor 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 downloaded software bulletins, you then create software update policies to distribute software update packages to the appropriate computer filters. 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 or a package server. 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.

Software that Patch Management Solution for Windows supports

Patch Management Solution for Windows lets you install software updates for software from the following vendors:

- 7-Zip
- Adobe Systems
- AOL Inc
- Apple
- Citrix Systems
- Foxit Corporation
- Google
- Hewlett-Packard
- Microsoft
- Mozilla
- Nullsoft
- Opera Software
- Oracle
- RealNetworks

- RealVNC
- Research In Motion
- Skype Technologies S.A.
- Sun Microsystems
- WinZip

See "About Patch Management Solution for Windows" on page 11.

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 **Supported Products A-Z** page, which is available at the following URL: http://www.symantec.com/business/support/index?page=products Open your product's support page, and then under **Common Topics**, click **Release Notes**.
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 **Supported Products A-Z** page, which is available at the following URL: http://www.symantec.com/business/support/index?page=products Open your product's support page, and then under **Common Topics**, click **Documentation**.

Table 1-1 Documentation resources *(continued)*

Document	Description	Location
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
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

Chapter 2

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 can function correctly. When you complete each task for the first time, 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.

See "About Patch Management Solution for Windows" on page 11.

Table 2-1 Process for implementing Patch Management Solution for Windows

Step	Action	Description
Step 1	Install or upgrade the solution.	Use Symantec Installation Manager to install the solution. See "About installing Patch Management Solution" on page 22. See "About upgrading Patch Management Solution for Windows" on page 23.

Table 2-1 Process for implementing Patch Management Solution for Windows *(continued)*

Step	Action	Description
Step 2	Install or upgrade the Symantec Management Agent.	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*. See "Where to get more information" on page 14.
Step 3	Install or upgrade the software update plug-in.	Install the plug-in that manages all of the Patch Management Solution for Windows functionality on a client computer. See "Installing the software update plug-in" on page 26. See "Upgrading the software update plug-in" on page 26.
Step 4	Configure the Patch Management Solution core settings.	(Optional) Configure the software update files storage location settings. See "Configuring patch management Core Services settings" on page 31.
Step 5	Configure the software updates installation settings.	Configure when do you want to perform software update installation and computer restarts. See "Configuring software updates installation settings" on page 33.
Step 6	Configure the system assessment scan interval.	Configure when to run the system assessment scan, which inventories managed computers for the software updates that they require. See "Configuring the system assessment scan interval" on page 34.
Step 7	Download the Windows software updates metadata.	Download the Windows software updates metadata and configure metadata update schedule. See "Downloading the Windows software updates catalog" on page 42.

Table 2-2 Process for installing software updates

Step	Action	Description
Step 1	Review and distribute available software updates.	View which software bulletins you need to install, then download updates and create software update policies. See "Downloading software updates" on page 49. See "Downloading and distributing software updates" on page 50.

Table 2-2 Process for installing software updates *(continued)*

Step	Action	Description
Step 2	Evaluate the results.	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 51. See “Viewing Patch Management Solution reports” on page 62.

Installing Patch Management Solution for Windows

This chapter includes the following topics:

System requirements for Patch Management Solution

Patch Management Solution requires the following:

- Symantec Management Platform 7.1 SP2

For details on Symantec Management Platform implementation, see the *IT Management Suite 7.1 SP2 Planning and Implementation Guide* at the following URL:

http://www.symantec.com/docs/DOC4827

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

See "About installing Patch Management Solution" on page 22.

See “About Patch Management Solution for Windows” on page 11.

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, including SP1, 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, including SP1
- Windows Hyper-V Server 2008
- Windows XP Embedded SP3

  For the Software Update Plug-in to work properly on Windows XP Embedded SP3, the following software must be installed on the client computer:

  - Windows Installer Service
  - TCP/IP Networking with File Sharing and Client for MS Networks
  - TCP/IP Networking
  - Secondary Logon Component

    This component is required to use the "Run with right as" setting on Notification Server side.
  - Copy and Compare Tools

    Some custom action updates require the xcopy.exe tool to be installed.

See “About Patch Management Solution for Windows” on page 11.

About 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 on Symantec Management Platform implementation, see the *IT Management Suite 7.1 SP2 Planning and Implementation Guide* at the following URL:

http://www.symantec.com/docs/DOC4827

See "About Patch Management Solution for Windows" on page 11.

About upgrading Patch Management Solution for Windows

For general information about migrating from Symantec Management Platform and Patch Management Solution for Windows versions 6.x and 7.0, see the following documentation resources:

- *IT Management Suite Migration Guide version 6.x to 7.1 SP2* at:
  http://www.symantec.com/docs/DOC4742
- *IT Management Suite Migration Guide version 7.0 to 7.1 SP2* at:
  http://www.symantec.com/docs/DOC4743

You upgrade this product from version 7.1 or later to 7.1 SP2 by using the Symantec Installation Manager. You can download the installation files directly to your server or you can create offline installation packages.

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

Software update packages, software update policies, and downloaded software updates metadata from Patch Management Solution for Windows version 7.1 and earlier are not compatible with 7.1 SP2. After you upgrade or migrate to 7.1 SP2, you must run the clean-up task that removes incompatible data. A link to the clean-up task is available on the **Import Patch Data for Windows** page.

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

See "Upgrading the software update plug-in" on page 26.

See "About Patch Management Solution for Windows" on page 11.

About uninstalling Patch Management Solution

Use the Symantec Installation Manager to uninstall this product.

See "About Patch Management Solution for Windows" on page 11.

About 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.

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

See "About Patch Management Solution for Windows" on page 11.

Chapter 4

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 system assessment scan tool reports to Notification Server that a certain software update is required for a managed computer, the update is then 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 27.

See "Installing the software update plug-in" on page 26.

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 25.

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.

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

To install the software update plug-in

1. In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Rollout 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 Symantec Management Agent and the software update plug-ins that are installed on the target computers.

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

See "About the software update plug-in" on page 25.

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

To upgrade the software update plug-in

1. In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Rollout 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 25.

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 26.

To uninstall the software update plug-in

1 In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Rollout 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 25.

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	■ **Installation is in Progress** – The update is currently being installed. ■ **Verification** – The update is installed, but assessment scan has not been run yet to verify this. ■ **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. ■ **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 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 displays “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 that you can later apply to software updates.

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

See “About Patch Management Solution for Windows” on page 11.

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

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 34.
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 can alter custom severity levels. You cannot alter the vendor-specified severity levels.

See “About software updates and software bulletins” on page 48.

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 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 Windows remediation settings

You can set up how you want Windows software updates distributed. You can configure package distribution and program settings.

You can add the software update languages that you use in your organization. By default, only English is selected. Other languages are excluded to ensure that unnecessary files are not downloaded.

See "About software updates and software bulletins" on page 48.

To configure Windows remediation settings

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

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

3 Click **Windows Settings > Windows Patch Remediation Settings**.

4 In the right pane, make any wanted changes, or leave the default values.

  See "Windows Patch Remediation Settings page" on page 35.

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 25.

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

To configure the software updates installation settings

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

2 In the left pane, click **Agents/Plug-ins > Software > Patch Management > Windows > Default Software Update Plug-in Policy**.

3 In the right pane, configure when and how you want to install updates, or leave the default values.

See “Default Software Update Plug-in Policy page” on page 38.

4 Click **Save changes**.

Configuring the system assessment scan interval

The system assessment scan lets you periodically inventory operating systems, applications, and installed patches on managed computers with the software update plug-in installed. System assessment 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.

You can configure how often you want to run the system assessment scan.

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

To configure the system assessment scan interval

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

2 In the left pane, click **Software > Patch Management > Windows System Assessment Scan**.

3 In the right pane, under **Schedule**, configure how often you want the software update plug-in to perform the system assessment scan on the managed computers and report it back to Notification Server.

4 If you want to report inventory only if it has changed, check **Send Inventory Results Only if Changed** .

This option is checked by default.

5 Do not change the targeted filter from **Windows Computers with Software Update Plug-in Installed Target** unless you have a specific reason to do so.

6 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 the custom severity levels that you later apply to software updates.

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

Only users with the **Patch Management Administrators** role can modify the settings on this page.

See "About software updates and software bulletins" on page 48.

See "Configuring patch management Core Services settings" on page 31.

See "Creating and assigning custom severity levels" on page 32.

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

Option	Description
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 "Relocating or checking the integrity of software update packages" on page 43.
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.
Severity Level	Lets you create a custom severity level that you can then assign to a bulletin.

Windows Patch Remediation Settings page

This page lets you set up how you want Windows software updates distributed. The settings include package server settings, program execution options, and language settings.

See "Configuring Windows remediation settings" on page 33.

Some of these settings are used as default values in the **Distribute Software Updates** wizard.

All new Windows software updates that are downloaded have these package settings and program settings by default. After you click **Save changes**, in a dialog box that appears, you can choose to update existing software update policies and packages. Note that updating existing packages can be time-consuming. If you do not want to update existing packages at this time, you can click **Save only**.

See "Downloading and distributing software updates" on page 50.

See "Patch Remediation Center page" on page 52.

Table 5-2 Options on the **Software Update Options** tab of the **Windows Patch Remediation 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.
The default Resource Target used by the Software Update Policy Wizard	Specifies the filter that is used by default when you create a new software update policy using the **Distribute Software Updates** wizard. The default target is **Windows Computers with Software Update Plug-in Installed Target**.

Table 5-3 Options on the **Policy and Package Settings** tab of the **Windows Patch Remediation Settings** page

Option	Description
Delete packages after	Lets you specify when to delete the software update packages that are no longer needed. Default: one week.
Use multicast when the Symantec Management Agent's multicast option is enabled	Lets you specify if you want to use multicast when distributing software update packages. For more information on multicasting, 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*.

Table 5-3 Options on the **Policy and Package Settings** tab of the **Windows Patch Remediation Settings** page *(continued)*

Option	Description
Use alternate download location on Package Server	Lets you specify a different location on a package server to which to download packages. This setting accepts the following values: ■ C:\myfolder\ ■ \\myserver\myshare\ ■ \\%computername%\myshare\ In this case, %computername% is a token that will be substituted with a package server computer name. The share must exist on the package server and be accessible with the Agent Connectivity Credentials (ACC). If these conditions are not met, the packages will be marked as invalid. If you are using Linux package servers in your environment, 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 clients	Lets you specify a different location on the managed computers to which to download packages.

Table 5-4 Options on the **Programs** tab of the **Windows Patch Remediation Settings** page

Option	Description
Terminate after	Lets you specify a time after which to terminate a running software update program. Default: four hours.
Run with rights	Lets you specify which account to use to run the program. If you select **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 the settings (including install and restart options) that 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 25.

See “Configuring software updates installation settings” on page 33.

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

Option	Description
Schedule	Lets you configure the schedule for installing software updates on the managed computer. This schedule appears on the **Software Updates** tab of the Symantec Management Agent on the target computer. If maintenance windows are specified in Notification Server configuration policies, this schedule is ignored unless you check **Override maintenance windows settings**.
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: three times.
Allow user to run	Lets a user initiate a software update installation from the Symantec Management Agent by clicking **Start Software Update Cycle** 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	Lets you specify to never automatically restart the managed computer after software updates are installed.

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

Option	Description
Scheduled	Lets you specify to 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	Lets you specify to restart the managed computer after all updates in a single update cycle have been installed.
Override maintenance windows settings	When maintenance windows are set up, the schedule is ignored and software updates are installed as soon as the first available maintenance window opens. Check this option to override this behavior and use the install and the restart options that you specified in this policy. Uncheck to abide by the maintenance windows. Software Update Plug-in tries to restart the computer as defined in the **Restart Defaults**. If the maintenance window is closed at the scheduled time, the restart is postponed until the next window.

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

Options	Description
Notify user	Lets you choose to send a message to the users of the computer on which 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.

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

Options	Description
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.

Run System Assessment Scan on Windows Computers task

This task lets you run a system assessment scan on the target computers outside of the normal system assessment schedule that is defined on the **System Assessment Scan Settings** page.

See “Configuring the system assessment scan interval” on page 34.

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. 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.

For example, the **Import Patch Data for Windows** task downloads Windows software updates metadata and imports all software management resources from these files into the CMDB. Other server tasks ensure data integrity or assist in automating software update distribution processes.

You must run the **Import Patch Data for Windows** task before you can download or distribute any software updates.

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

See “Downloading the Windows software updates catalog” on page 42.

Downloading the Windows software updates catalog

You must download the Windows software updates catalog (patch management metadata, or patch management import files) before you can download 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 this task to run daily.

To download the Windows 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 > Import Patch Data for Windows**.

3 In the right pane, click **Update**.

4 When the available products list import is complete, under **Vendors and Software**, check the software for which you want to download the patch management metadata.

5 (Optional) Make any other wanted changes.

See "Import Patch Data for Windows page" on page 43.

6 Click **Save changes**.

7 Under **Task Status**, click **New Schedule**.

8 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 Windows** 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 this task to run daily.

3 Click **Schedule**.

Relocating or checking the integrity of software update packages

When you change package or program settings in the **Patch Remediation Settings** policies, you can choose to run the **Check Software Update Package Integrity** task. This task checks that all software update packages have the correct new settings and values.

See "Configuring Windows remediation settings" on page 33.

You can also run this task manually to verify that software update packages in software update tasks have the correct global server settings applied.

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 31.

To relocate or 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 **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 the updates that are no longer in use from the file system**.
4. If you changed the **Software Update Package Location** value on the **Core Services** page and want to relocate downloaded updates, check **Relocate existing packages if default Software Update package location on Core Services page has changed**.

   See "Configuring patch management Core Services settings" on page 31.
5. Under **Task Status**, click **New Schedule** and specify a schedule on which to run the task.

Import Patch Data for Windows page

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.

This task downloads the information about the updates that are available for download. It does not download the actual software update files.

See "Downloading the Windows software updates catalog" on page 42.

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

Option	Description
Incremental import	Ensures that only updated files are downloaded, thus avoiding unnecessary downloads.
Delete previously downloaded data for vendors, software and languages that are now excluded	Deletes the data that is associated with excluded software releases. By default, this option is unchecked so that this data is not deleted on the next patch metadata import. If you leave this option unchecked, you can perform partial metadata refresh and save time and bandwidth.
Default Location	Lets you choose to use the default location for downloading the patch management metadata files.
Alternative Location	Lets you specify a custom location from which to download the patch management metadata files.
Automatically revise Software Update policies after importing patch data	Updates existing software update policies with the latest Windows patch management metadata automatically. Each download of the patch management metadata files may contain data and fixes for the software bulletins that were published earlier. By checking this option, you can use the new data to resolve any known issues with existing software bulletins.
Enable distribution of newly added software updates	Enables the distribution of the software updates that were added to existing software bulletins by the software vendor. If you check this option, the software updates that are added to existing software update policies will be enabled for distribution. If you do not check this option, the software updates will be added to the policy, but not enabled.
Disable all superseded Software Updates	Disables the rollout of any software update tasks containing superseded software updates.

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

Option	Description
Vendors and Software	Lets you choose the software for which you want to import the software updates metadata. When you run this task for the first time, you must click **Update** to download the list of available vendors, software, and languages for which you can download software updates.

Chapter 7

Downloading and distributing software updates and software bulletins

This chapter includes the following topics:

About software updates and software bulletins

A software update or patch is any update or hot fix 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 the software vendor specifications. For example, if the update requires a restart, then the computer is restarted after the update is installed. Service Packs are installed before other software updates.

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

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

See “Creating and assigning custom severity levels” on page 32.

Warning: 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.

See “About downloading and distributing software updates” on page 48.

About downloading and distributing software updates

You can stage software bulletins and download software update packages on the **Patch Remediation Center** page, where all available software updates are listed. You can also do this from any Patch Management Solution report.

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**.

You can choose to download the software update packages and distribute them at a later time. You also have an option to download and then, once the download has finished, distribute the software update to managed computers.

See “Downloading software updates” on page 49.

See “Downloading and distributing software updates” on page 50.

Sometimes not all software updates can be downloaded for a software bulletin. For example, 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.

When distributing updates, you should consider possible effects on your network environment. Symantec recommends that you distribute new updates to a test environment first.

Downloading software updates

You can download a software bulletin and its associated updates to the Notification Server computer.

See “About downloading and distributing software updates” on page 48.

You can download all software bulletins. However, Symantec recommends that you download 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 can create a software update policy to distribute the updates to managed computers.

See “Downloading and distributing software updates” on page 50.

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

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

To download 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 **Windows 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 download.

For example, click the bulletins that have a high number in the **Not Installed** column. You can select multiple items while holding down the Shift or Control key.

4 Right-click the selected bulletins, and then click **Download Packages**.

You can close the status dialog box; the download continues in the background.

To view the status of a software updates download

1 In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.

2 In the left pane, click **System Jobs and Tasks > Software > Patch Management > Download Software Update Package**.

3 In the right pane, view the status of download tasks.

Downloading and distributing software updates

To deliver and install the software updates to the appropriate computers, you must create software update policies.

The **Distribute Software Updates** wizard lets you create software update policies. If the associated software updates are not yet downloaded, Patch Management Solution creates a download task. When download is completed, the software update policy is distributed to the target computers.

If you want to install a Service Pack, Symantec recommends that you create a software update policy for this service pack only, without any other bulletins included in it. Also, in the wizard, check the **Allow immediate restart if required** box.

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.

You can view the software update policies distribution results in reports.

See “Viewing the software update delivery summary report” on page 51.

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

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 **Windows 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 **Not Installed** column. You can select multiple items while holding down the Shift or Control key.
4. Right-click the selected bulletins, and then click **Distribute Packages**.
5. (Optional) Configure the settings as needed.

   See "Distribute Software Updates wizard pages" on page 55.
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 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 - Details** report summarizes the results of all scheduled Microsoft software update policies. It shows you which computers the software update tasks target, and if the updates have been successfully installed. The report also shows 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 59.

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

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, expand **Software > Patch Management > Remediation Status**, and then click **Windows Software Update Delivery - Details**.
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 installation of software updates and other maintenance tasks are performed. To ensure that software update policies abide by maintenance windows, leave the **Override Maintenance Window Settings** check box unchecked on the first page of the **Distribute Software Updates** wizard.

If maintenance windows are defined, software updates are installed as soon as the first available maintenance window opens. The software update installation schedule is ignored.

If you check the box, the software update plug-in ignores maintenance windows and installs the updates as instructed by the software update policy.

See “Distribute Software Updates wizard pages” on page 55.

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, download, and distribute the software updates that the software update metadata files provide.

See “About downloading and distributing software updates” on page 48.

See “About software updates and software bulletins” on page 48.

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

Item	Description
Bulletin	The bulletin's number, as supplied by the vendor.

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

Item	Description
Severity	The bulletin's vendor-specified severity level.
Custom Severity	The bulletin's user-defined severity level.
Staged	The download status of the software updates for this bulletin. 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 in the **All Software Bulletins** report

Item	Description
Resource Manager	Opens the **Resource Manager** for the selected bulletin. For more information, see the *Symantec Management Platform User Guide*.
Export	Lets you export the bulletin information to an XML file.
Properties	Displays the item's properties and audit information.
CMDB Functions	This option is displayed when Altiris CMDB Solution is installed. For more information, see the *CMDB Solution User Guide*.
Custom Severity	Lets you assign a custom severity level. See "Creating and assigning custom severity levels" on page 32.
Add To Filter	This option is displayed when Altiris CMDB Solution is installed. For more information, see the *CMDB Solution User Guide*.

Table 7-2 Right-click actions in the **All Software Bulletins** report *(continued)*

Item	Description
Add to organizational group	Lets you add a resource to an organizational group.
Disable	Lets you disable the distribution of the bulletin. If the bulletin is already included in a software update policy, it will not be installed. To enable the bulletin, use the **Download Packages** or **Recreate Packages** commands.
Distribute Packages	Launches the **Distribute Software Updates** wizard. See "Downloading and distributing software updates" on page 50.
Download Packages	Initiates the download of software update packages. See "Downloading software updates" on page 49. This option is not available if the packages are already downloaded.
Recreate Packages	Lets you check the integrity of downloaded packages and re-download if necessary. This option is not available if the packages are not yet downloaded.
View Policies	Lets you view the software update policies that contain this particular bulletin. This option is available only if a policy has been created for this bulletin.
View Targeted Computers	Displays the computers that the software update policy containing this bulletin is targeting. You must create a software update policy before you can view targeted computers. The bulletin must not be disabled.
List Software Updates	Displays the list of software updates that are included into the software bulletin.

Table 7-3 Right-click actions in the **Windows Compliance by Bulletin** report

Item	Description
View Software Bulletin Information	Displays the software bulletin information such as description, release date, applicable operating systems, and so on.

Table 7-3 Right-click actions in the **Windows Compliance by Bulletin** report *(continued)*

Item	Description
View Targeted Computers by Bulletin	Displays the computers that the software update policy containing this bulletin is targeting. You must create a software update policy before you can view targeted computers. The bulletin must not be disabled.
View Applicable Computers by Bulletin	Displays the computers to which the selected bulletin applies.
View Installed Computers by Bulletin	Displays the computers on which the selected bulletin is installed.
View Not Installed Computers by Bulletin	Displays the computers that do not have the selected bulletin installed.

Distribute Software Updates wizard pages

The **Distribute Software Updates** 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. If needed, a download task is created that downloads software update packages from the vendor.

See "Downloading and distributing software updates" on page 50.

Table 7-4 Options on the first page of the **Distribute Software Updates** wizard

Option	Description
Name	The name of the software update policy that you want to create. This field is populated automatically with the bulletin names.
Description	The description of the software update policy that you want to create. This field is populated with the vendor description of the selected bulletins.

Table 7-4 Options on the first page of the **Distribute Software Updates** wizard *(continued)*

Option	Description
Software Bulletins	The names of the bulletins for which you have chosen to make policies. You can click a software bulletin to open the Resource Manager to view detailed information on the software bulletin. You cannot edit the software bulletins through the **Distribute Software Updates** wizard.
Software Updates	The names of each software update that is included in the bulletin.
Use Multicast when the Symantec Management Agent's multicast option is enabled	Enables multicast features. For more information, see the *Symantec Management Platform User Guide*.
Allow immediate restart if required	Restarts the target computer automatically after installing an update that requires a restart.
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 33.
As soon as possible	Runs the software updates installation as soon as the software update policy arrives at the target computer.
Power on computer (Wake on LAN)	Attempts to turn on the computer before installing software updates.
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 52.
Apply to computers	Lets you specify the target collection or collections to which the software update policy applies. If you use the **Distribute Software Updates** wizard, the correct resource target for the selected software bulletin is automatically applied.

Table 7-5 Options on second page of the **Distribute Software Updates** 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**.
Immediately replicate that policy down the hierarchy	This option is available only on the parent Notification Server computer in a hierarchy. Lets you replicate the software update policy immediately down the hierarchy bypassing the default replication schedules. Use this option to replicate an emergency software update. Note that software update installation is not performed immediately after you create and replicate a software update policy. Software update installation time depends on the software update policy, solution, and the Symantec Management Agent settings.
Software Bulletin	Displays the name of the software bulletin.
Update Name	Displays the name of each software update executable. If you enable this advertisement, all of the executables are enabled. Click the hyperlink to open the **Resource Manager** page for the software update. The language and culture of the software update is displayed in the section's title bar.
Package	This option is available only if software update packages for this bulletin are downloaded. Displays the name of the software update package.
Command Line	This option is available only if software update packages for this bulletin are downloaded. Displays the name of the command line that is used to install this package.

Update download and policy creation status dialog

This dialog box displays the package download or software update policy creation status.

You can close this dialog box. The action will continue to run in background.

See "About downloading and distributing software updates" on page 48.

Distribute Software Updates task

Patch Management Solution uses this task to distribute software updates. This task uses the Symantec Management Agent's built-in software management framework functionality to distribute and install updates.

See "About downloading and distributing software updates" on page 48.

This task is read-only.

Download Software Update Package task

Patch Management Solution uses this task to download software updates from the vendor to a local repository.

See "About downloading and distributing software updates" on page 48.

This task is read-only.

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. Reports give you the information that is 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 60.

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 download or distribute software updates directly from reports by right-clicking the update name in the report.

Patch Management Solution provides the following reports:

- Compliance reports
  See "About compliance reports" on page 60.
- Diagnostic reports
  See "About diagnostics reports" on page 61.
- Remediation status reports
  See "About remediation status reports" on page 61.
- Software bulletin reports
  See "About software bulletins reports" on page 61.

See "Viewing Patch Management Solution reports" on page 62.

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

See "About the Windows compliance dashboard" on page 61.

About compliance reports

Compliance reports let you quickly determine which 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 capability 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 **Download Packages** or **Distribute Packages**.

See "About downloading and distributing software updates" on page 48.

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 compliance dashboard for easy access.

See "About the Windows compliance dashboard" on page 61.

See "About Patch Management Solution reports" on page 59.

About diagnostics 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 59.

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 59.

About software bulletins reports

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

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

See "About Patch Management Solution reports" on page 59.

About the Windows compliance dashboard

The **Windows Compliance** page provides 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 59.

You cannot customize this 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 portal page by clicking **Home > Patch Management**, and then, in the left pane, under **Windows**, click **Compliance Dashboard**.

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

Web part	Description
Patch Management License Status	Reports on the amount of Patch Management Solution licenses in use, their status, and expiration date.
Windows Patch Configuration Summary	Provides an overall configuration summary, which includes computers with the software update plug-in, computers not reporting vulnerability analysis, Windows patch management metadata versions, and so on.
Windows Missing Updates	Reports on the number of Windows updates that can be installed.
Windows Software Update Delivery by Execution	Reports on the number of software updates installations that were executed in the past 30 days and how many succeeded or did not complete.
Windows Software Bulletin Summary	Reports on the number of software bulletins available, staged, tasks created, and new bulletins in the last 30 days.

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 59.

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 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. When you open a Resource Manager for a software update, you can click **Summaries > Software Bulletin Details**, and under **Additional Information** you can find a hyperlink to the Microsoft Technet article on the bulletin.

Chapter 9

Replicating Patch Management data in hierarchy

This chapter includes the following topics:

About replicating Patch Management Solution for Windows data in hierarchy

Downloading software update catalog files (patch management metadata, or patch management import files) to multiple Notification Server computers 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 Server computers. The replicated data on the child Notification Server computers is identical to the data on the parent.

Patch Management Solution supports only two-level hierarchy. A child Notification Server computer cannot be a parent to another child.

See "About hierarchy and data replication direction" on page 71.

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

See "About the Patch Management Language Alerting rule" on page 66.

See "Replicating patch management language alerts" on page 66.

See "About software update catalog replication" on page 67.

See "Replicating the software updates catalog" on page 67.

See "About software update policy replication" on page 68.

See "Replicating a software update policy manually" on page 69.

About the Patch Management Language Alerting rule

Different Notification Server computers within a hierarchy may manage different patch management language resources. The **Patch Management Language Alerting** replication rule ensures that child Notification Server computers only receive data and software update policies for their managed languages. This rule replicates information about the managed languages of the child Notification Server computer 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 computer 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 66.

See "About replicating Patch Management Solution for Windows data in hierarchy" on page 65.

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 66.

See "About replicating Patch Management Solution for Windows data in hierarchy" on page 65.

To replicate patch management language alerts on a schedule

1. On the child Notification Server computer, 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 Windows patch management software update catalog files to multiple Notification Server computers 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 computer. Then you can use the **Patch Management Import Data Replication for Windows** rule to send the relevant data to any number of child Notification Server computers. The replicated data on the child Notification Server computers 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 67.

See "About replicating Patch Management Solution for Windows data in hierarchy" on page 65.

Replicating the software updates catalog

After downloading Windows software updates catalog files and importing data to the parent Notification Server computer, you can replicate the data to any number of child Notification Server computers.

See "About software update catalog replication" on page 67.

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

See "About the Patch Management Language Alerting rule" on page 66.

See "About replicating Patch Management Solution for Windows data in hierarchy" on page 65.

To replicate the software updates catalog on a schedule

1. On the parent Notification Server computer, 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 Windows**.
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 Windows patch management software update catalog files to child Notification Server computers each time the task runs.
8. Under **Schedule**, set the schedule a few hours after the **Patch Management Language Alerting** rule schedule.
9. Under **Data Verification**, specify a percentage of data to be verified during each replication, and check **Verify data integrity** if you want.
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 "Downloading and distributing software updates" on page 50.

In Patch Management Solution 7.1 and later, the software update policies are always replicated to child Notification Server computers. 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 69.

Another option is to replicate a policy immediately after you create it. To do this, check the **Immediately replicate that policy down the hierarchy** option in the **Distribute Software Updates** wizard.

See "Downloading and distributing software updates" on page 50.

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

See "About replicating Patch Management Solution for Windows data in hierarchy" on page 65.

Replicating a software update policy manually

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

See "About software update policy replication" on page 68.

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

You can replicate a single policy or a collection of policies. If you want to manually replicate a collection of policies, you must create a new folder and move policies under this folder. Then you can right-click the folder and launch replication.

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 66.

See "About software update catalog replication" on page 67.

See "About replicating Patch Management Solution for Windows data in hierarchy" on page 65.

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 or a folder, 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 in hierarchy" on page 65.

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: ■ **Check Software Update Package Integrity** ■ **Import Patch Data for Windows/Red Hat/Novell**	Down
Run System Assessment Scan on Windows/Linux Computers task settings and schedules	Down
Windows/Linux System Assessment Scan policy settings	Down
Windows/Red Hat/Novell Patch Remediation Settings policy	Down

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

Item	Replication direction
Default Software Update Plug-in Policy settings	Down
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 Windows/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 system assessment scan result 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 the **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 the **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.

See “About Patch Management Solution for Windows” on page 11.

Altiris™ Patch Management Solution for Windows 7.1 SP2 from Symantec™ Third-Party Legal Notices

This appendix includes the following topics:

- Third-Party Legal Attributions
- CabDotNet

Third-Party Legal Attributions

This Symantec product may contain third party software for which Symantec is required to provide attribution ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. This appendix contains proprietary notices for the Third Party Programs and the licenses for the Third Party Programs, where applicable.

CabDotNet

MIT License

This code is licensed under the license terms below, granted by the copyright holder listed above. The term copyright holder” in the license below means the copyright holder listed above.

Copyright (c) <year> <copyright holders>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Index