Symantec™ Patch Management Solution for Windows® 8.1 powered by Altiris™ technology User Guide
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 website at the following URL:

support.symantec.com

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:

support.symantec.com

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, DVDs, 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_apj@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com
Contents

Technical Support ............................................................................................................. 4

Chapter 1 Introducing Patch Management Solution for Windows ........................................... 9
  About Patch Management Solution for Windows ............................................................. 9
  How Patch Management Solution for Windows works ....................................................... 11
  Components of Patch Management Solution for Windows ............................................. 12
  Where to get more information ......................................................................................... 12

Chapter 2 Implementing Patch Management Solution for Windows ....................................... 15
  Preparing your environment for Patch Management ............................................................. 15
  Installing the software update plug-in ................................................................................. 17
  Configuring Windows software updates distribution ............................................................ 18
  Downloading the Windows software updates catalog ......................................................... 18
  Distributing Software Updates ........................................................................................... 19
  Running compliance and vulnerability reports ................................................................. 20
  Downloading and distributing software updates ................................................................. 22
  Viewing software update delivery results ............................................................................ 23

Chapter 3 Performing Advanced Configuration ...................................................................... 25
  Upgrading the software update plug-in .............................................................................. 25
  Uninstalling the software update plug-in ........................................................................... 26
  Configuring software updates download location ............................................................... 26
  Creating and assigning custom severity levels .................................................................... 27
  Configuring software updates installation settings ............................................................. 28
  Configuring Windows System Assessment Scan policy ...................................................... 28
  Relocating or checking the integrity of software update packages ...................................... 29
  Staging software bulletins .................................................................................................. 31
<table>
<thead>
<tr>
<th>Chapter 4</th>
<th>Replicating Patch Management Solution for Windows data in hierarchy</th>
<th>33</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>About replicating Patch Management Solution for Windows data in hierarchy</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>Replicating patch management language alerts</td>
<td>34</td>
</tr>
<tr>
<td></td>
<td>Replicating the software updates catalog</td>
<td>35</td>
</tr>
<tr>
<td></td>
<td>Replicating a software update policy</td>
<td>36</td>
</tr>
<tr>
<td>Appendix A</td>
<td>Technical reference</td>
<td>38</td>
</tr>
<tr>
<td></td>
<td>About hierarchy and data replication direction</td>
<td>38</td>
</tr>
<tr>
<td></td>
<td>About Patch Management Solution security roles</td>
<td>39</td>
</tr>
<tr>
<td>Index</td>
<td></td>
<td>41</td>
</tr>
<tr>
<td>Patch Management Solution Glossary</td>
<td></td>
<td>43</td>
</tr>
</tbody>
</table>
Introducing Patch Management Solution for Windows

This chapter includes the following topics:

- About Patch Management Solution for Windows
- How Patch Management Solution for Windows works
- Components of Patch Management Solution for Windows
- Where to get more information

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. Patch Management provides all security updates, critical updates and hotfixes, but does not provide all optional updates.

Integration with Notification Server 7.x and higher 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 “Preparing your environment for Patch Management” on page 15.

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
- EMC
- Foxit Corporation
- Google
- Hewlett-Packard
- LibreOffice
- Lightning UK
- Microsoft
- Mozilla
- Nullsoft
- Opera Software
- Oracle
- Rarlab
- Real
- RealVNC
- Research In Motion
- Skype Technologies S.A.
- Sourceforge.Net
- Sun Microsystems
- UltraVNC
- WinZip
- Wireshark Foundation
- Yahoo!
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 website. 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.

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.
Components of Patch Management Solution for Windows

The process of populating the information repository from the patch management metadata files can be started after you complete the installation of the solution.

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 27.

**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.

Where to get more information

Use the following documentation resources to learn about and use this product.
### Table 1-1 Documentation resources

<table>
<thead>
<tr>
<th>Document</th>
<th>Description</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Notes</td>
<td>Information about new features and important issues.</td>
<td>The <strong>Supported Products A-Z</strong> page, which is available at the following URL: <a href="https://www.symantec.com/products/products-az">https://www.symantec.com/products/products-az</a>. Open your product's support page, and then under <strong>Common Topics</strong>, click <strong>Release Notes</strong>.</td>
</tr>
</tbody>
</table>
| 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: https://www.symantec.com/products/products-az. Open your product's support page, and then under **Common Topics**, click **Documentation**. |
| 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:  
■ Click the page and then press the F1 key.  
■ Use 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

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>SymWISE Support Knowledgebase</td>
<td>Articles, incidents, and issues about Symantec products.</td>
<td>Knowledge Base</td>
</tr>
</tbody>
</table>
### Table 1-2  Symantec product information resources (continued)

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Unified Help System</td>
<td>All available IT Management Suite and solution guides are accessible from this Symantec Unified Help System that is launched on cloud.</td>
<td>Unified Help System</td>
</tr>
<tr>
<td>Symantec Connect</td>
<td>An online resource that contains forums, articles, blogs, downloads, events, videos, groups, and ideas for users of Symantec products.</td>
<td>The links to various groups on Connect are as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Deployment and Imaging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Discovery and Inventory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- ITMS Administrator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Mac Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Monitor Solution and Server Health</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Patch Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Reporting</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- ServiceDesk and Workflow</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Software Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Server Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Workspace Virtualization and Streaming</td>
</tr>
</tbody>
</table>
Implementing Patch Management Solution for Windows

This chapter includes the following topics:

- Preparing your environment for Patch Management
- Distributing Software Updates

Preparing your environment for Patch Management

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.


<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Install or upgrade the solution.</td>
<td>Use Symantec Installation Manager to install the solution.</td>
</tr>
<tr>
<td>Step</td>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Step 2</td>
<td>Install or upgrade the Symantec Management Agent.</td>
<td>Install or upgrade the Symantec Management Agent on every computer to which you want to send patches. For more information, see the topics about installing or upgrading the Symantec Management Agent in the <em>IT Management Suite Administration Guide</em>. See “Where to get more information” on page 12.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Install or upgrade the software update plug-in.</td>
<td>Install the plug-in that manages all of the Patch Management Solution for Windows functionality on a client computer. See &quot;Installing the software update plug-in&quot; on page 17. See &quot;Upgrading the software update plug-in&quot; on page 25.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Enable the <strong>Windows Update</strong> service.</td>
<td>On client computers, enable and configure the <strong>Windows Update</strong> service to make available the installation of software updates. You can configure the <strong>Windows Update</strong> service to start manually or automatically. Symantec recommends that you configure the <strong>Windows Update</strong> service to start manually. When you enable the Manual startup type setting, the service starts and remains started until a computer restart. <strong>Warning:</strong> When you enable the Automatic startup type setting, client computers may be restarted after the software update cycle is completed. For more information, see the following knowledge base article: <a href="http://www.symantec.com/docs/TECH41678">http://www.symantec.com/docs/TECH41678</a></td>
</tr>
<tr>
<td>Step 6</td>
<td>Configure the software update files location settings.</td>
<td>(Optional) Configure the software update files storage location settings. See “Configuring software updates download location” on page 26.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Configure the software updates installation settings.</td>
<td>(Optional) Configure the time when you want to perform software update installation and computer restarts. See “Configuring software updates installation settings” on page 28.</td>
</tr>
</tbody>
</table>
Table 2-1  Process for implementing Patch Management Solution for Windows (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 8</td>
<td>Configure the system assessment scan interval.</td>
<td>(Optional) Configure when to run the system assessment scan, which inventories managed computers for the software updates that they require. See “Configuring Windows System Assessment Scan policy” on page 28.</td>
</tr>
<tr>
<td>Step 9</td>
<td>Download the Windows software updates metadata.</td>
<td>Download the Windows software updates metadata and configure the metadata update schedule. See “Downloading the Windows software updates catalog” on page 18.</td>
</tr>
</tbody>
</table>

**Installing 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 of software updates for that computer. If the tab is not visible, in the Symantec Management Agent, click **View > Software Updates**. To open the Symantec Management Agent user interface, click the Symantec Management Agent icon in the system tray of the managed computer.

See “Installing the software update plug-in” on page 17.

**Note:** If you have a large number of computers where you want 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 “Preparing your environment for Patch Management” on page 15.
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, expand Software > Patch Management > Software Update Plug-in Install.

3. (Optional) In the right pane, make any necessary changes.
   For help, press F1 or, on the Help menu, click Context.

4. In the upper right corner of the page, click the colored circle, and then click On.

5. Click Save changes.

The next step is to configure software update package distribution and program settings.

See “Configuring Windows software updates distribution” on page 18.

Configuring Windows software updates distribution

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

To configure Windows remediation settings

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

2. In the left pane, expand Software > Patch Management > Windows Settings, and then click Windows Patch Remediation Settings.

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

4. Click Save changes.

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 “Preparing your environment for Patch Management” on page 15.

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.
Before you perform this step, ensure that you have installed or upgraded the software update plug-in.

See “Installing the software update plug-in” on page 17.

See “Upgrading the software update plug-in” on page 25.

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, under Vendors and Software, 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 necessary changes.
6. Click Save changes.
8. In the New Schedule dialog box, click Now, and then click Schedule.

To configure a schedule for downloading the software updates catalog

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.

Distributing Software Updates

After you configure Patch Management Solution to work in your environment, you can gather information about the needs and priorities for patching in your environment. Use this information to set up software update policies, and then evaluate the results with software update delivery reports.

See “Preparing your environment for Patch Management” on page 15.
### Table 2-2  Process for installing software updates

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Run compliance and vulnerability reports</td>
<td>Check your environment for vulnerabilities and evaluate which software updates you need to distribute.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Running compliance and vulnerability reports” on page 20.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Review and distribute available software updates</td>
<td>View which software bulletins you need to install, then download updates and create software update policies.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Downloading and distributing software updates” on page 22.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Staging software bulletins” on page 31.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Evaluate the results.</td>
<td>Evaluate the results by running the <strong>Software Update Delivery Summary</strong> report and revisiting compliance reports.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Viewing software update delivery results” on page 23.</td>
</tr>
</tbody>
</table>

For an example on how to manage the updates with Patch Management Solution, please see the following videos:

<table>
<thead>
<tr>
<th>Youtube link</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.youtube.com/watch?v=LfjiZ8peXhs">http://www.youtube.com/watch?v=LfjiZ8peXhs</a></td>
<td>Run compliance and vulnerability reports</td>
</tr>
<tr>
<td><a href="http://www.youtube.com/watch?v=iY25PztN7Kc">http://www.youtube.com/watch?v=iY25PztN7Kc</a></td>
<td>Run compliance and vulnerability reports</td>
</tr>
</tbody>
</table>

### Running compliance and vulnerability 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.

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.
Table 2-3  Patch Management Solution reports

<table>
<thead>
<tr>
<th>Report type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance reports</td>
<td>Compliance reports let you quickly determine which software updates your managed computers require. Compliance reports are used to determine if the 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.</td>
</tr>
<tr>
<td>Diagnostics reports</td>
<td>The diagnostics reports display vulnerability summary and software update plug-in installation information.</td>
</tr>
<tr>
<td>Remediation status reports</td>
<td>The remediation status reports summarize and detail software update associations and activities.</td>
</tr>
<tr>
<td>Software bulletins reports</td>
<td>The software bulletins reports summarize and detail software bulletins activity and status.</td>
</tr>
</tbody>
</table>

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. If you want to view more information about an update, right-click any update, and then 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.

The next step is to review and distribute available software updates.

See “Downloading and distributing software updates” on page 22.
See “Staging software bulletins” on page 31.
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 to the client computers at a later time. You can also distribute the software updates once the download is complete.

See “Staging software bulletins” on page 31.

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 the effects it can possibly have on your network environment. Symantec recommends that you distribute new updates to a test environment first.

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 software update delivery results” on page 23.

See “Preparing your environment for Patch Management” on page 15.

Before you perform this step, ensure that you have run the compliance and vulnerability reports.
See “Running compliance and vulnerability reports” on page 20.

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.

6. Click Next.

7. (Optional) On the second page of the wizard, check the updates that you want to distribute.

8. At the upper right of the page, click the colored circle, and then click On.

   You can also turn on the policy later.

9. Click Distribute software updates.

   The next step is to view the results.

Viewing software update delivery results

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 been completed.

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

See “Preparing your environment for Patch Management” on page 15.
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.
Performing Advanced Configuration

This chapter includes the following topics:

- Upgrading the software update plug-in
- Uninstalling the software update plug-in
- Configuring software updates download location
- Creating and assigning custom severity levels
- Configuring software updates installation settings
- Configuring Windows System Assessment Scan policy
- Relocating or checking the integrity of software update packages
- Staging software bulletins

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 *IT Management Suite Administration Guide*.

See "Preparing your environment for Patch Management" on page 15.
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.

The next step is to configure the Patch Management Solution core settings.

See “Configuring software updates download location” on page 26.

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.

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 17.

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.

Configuring software updates download location

You can configure to which location on Notification Server the software updates should be downloaded.
The settings that you configure apply to Windows and Linux components of Patch Management Solution.

See “Preparing your environment for Patch Management” on page 15.

To configure software updates download location

1. In the Symantec Management Console, on the Settings menu, click All Settings.
2. In the left pane, expand Software > Patch Management > Core Services.
3. In the right pane, on the Locations tab, specify the software updates download location.
4. Click Save Changes.

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 29.

The next step is to configure the software updates installation settings.

Creating and assigning custom severity levels

A software update marked 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.

The settings that you configure apply to Windows and Linux components of Patch Management Solution.

To create a custom severity level

1. In the Symantec Management Console, on the Settings menu, click All Settings.
2. In the left pane, expand Software > Patch Management > Core Services.
3. In the right pane, click the Custom Severity tab.
4. On the Custom Severity tab, 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 the 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 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 “Preparing your environment for Patch Management” on page 15.

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, expand 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 the updates, or leave the default values.
4. Click Save changes.

Configuring Windows System Assessment Scan policy

Windows system assessment scan detects applicable and installed updates on client computers with the software update plug-in installed. System assessment information is then used to determine which software updates are required. Based on this information, filters targeting the software update policies are created automatically.

System assessment scan runs automatically in the following cases:

- When the client computer receives a new or changed Windows Assessment Scan Policy
- When the client computer receives a new or changed Software Update policies
- According to the custom schedule defined by the user
- During the maintenance window
Before an update is deployed

After an update is deployed

When Symantec Management Agent starts after a reboot that was initiated by an update deployment

To change the default scan settings, configure the Windows System Assessment Scan policy.

See “Preparing your environment for Patch Management” on page 15.

To configure Windows System Assessment Scan policy

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

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

3. In the right pane, under Schedule, configure how often you want the system assessment scan to run on client computers.

   If you want the plug-in to report inventory only if it has changed, check Send Inventory Results Only if Changed.

4. This option is checked by default.

5. (Optional) Under Applied To, choose on which client computers you want the scan to run.

   Symantec recommends that you do not change the default filter from Windows Computers with Software Update Plug-in Installed Target unless you have a specific reason to do so.

6. Turn the policy on.

7. Click Save changes.

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.

See “Configuring Windows software updates distribution” on page 18.

This task checks that all software update packages have the correct new settings and values.
If some physical files are missing on the file system in the software update package location, this task uses the URL from the latest imported patch metadata to re-download the required files.

You can 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 software updates download location” on page 26.

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 Check Delete the downloaded packages that are no longer in use (Windows only) if you want to delete the following downloaded Windows software update packages:
   - The packages that have no association with any software update.
   - The packages that are not part of any software update policy and belong to a disabled bulletin.

4 If you changed the Software Update Package Location value on the Core Services page and want to relocate downloaded updates to the new location, check Relocate existing packages if default Software Update package location on Core Services page has changed.

   When you enable this option, the Check Software Update Package Integrity task works as follows:
   - If some physical files are missing on the file system in the old location, the task re-downloads the required files to the old location but fails to relocate the files to the new location. The overall task result is Failed. You need to re-run the task with this option checked to successfully relocate the files to the new location.
   - The task successfully relocates the downloaded updates to the new location only when the new location is accessible.
   - The task fails if the old or new location is inaccessible. No physical files are relocated.

5 Under Task Status, click New Schedule and specify a schedule on which to run the task.
Staging software bulletins

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

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 22.

When you choose to download a software bulletin, a task is created that downloads the associated software updates. Note that only one instance of a download task may run at the same time for software update packages. A queue of download tasks may appear on Notification Server or a package server, and the software update packages may be downloaded with a delay. You can view the status of this task to troubleshoot the download of software updates.

See “Preparing your environment for Patch Management” on page 15.

Before you perform this step, ensure that you have run the compliance and vulnerability reports.

See “Running compliance and vulnerability reports” on page 20.

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 client computers require.

3. Select the bulletins that you want to download.

   For example, select 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 or leave it open in a new window; 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, expand **System Jobs and Tasks > Software > Patch Management > Download Software Update Package**.

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

The next step is to view the results.

See “**Viewing software update delivery results**” on page 23.
Replicating Patch Management Solution for Windows data in hierarchy

This chapter includes the following topics:

- About replicating Patch Management Solution for Windows data in hierarchy
- Replicating patch management language alerts
- Replicating the software updates catalog
- Replicating a software update policy

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.

A Package Distribution Hierarchy Editable Property (HEP) allows you to control on the parent Notification Server, if the Package Distribution section on the
**Windows Patch Remediation Settings** page is editable on the child Notification Server.

If you enable this feature on the parent Notification Server, and then replicate it down to the child Notification Servers, the **Windows Patch Remediation Settings** page becomes editable on these child Notification Servers. This means that these settings can then be managed on the child Notification Servers independently from the parent Notification Server.

If you disable this feature on the parent Notification Server, and the replicate this change down the hierarchy, the **Windows Patch Remediation Settings** page becomes read-only on the child Notification Servers and the corresponding settings then become inherited from the parent Notification Server.

See “About hierarchy and data replication direction” on page 38.

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

See “Replicating patch management language alerts” on page 34.

See “Replicating the software updates catalog” on page 35.

See “Replicating a software update policy” on page 36.

### Replicating patch management language alerts

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 “About replicating Patch Management Solution for Windows data in hierarchy” on page 33.

**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.

Replicating the software updates catalog

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.

---

**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 “Replicating patch management language alerts” on page 34.
See “About replicating Patch Management Solution for Windows data in hierarchy” on page 33.

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.
Replicating a software update policy

Software update policies distribute software updates to the target computers.

See “Downloading and distributing software updates” on page 22.

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.

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.

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.

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.

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 “Replicating patch management language alerts” on page 34.

See “Replicating the software updates catalog” on page 35.
See “About replicating Patch Management Solution for Windows data in hierarchy” on page 33.

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 33.

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

<table>
<thead>
<tr>
<th>Item</th>
<th>Replication direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the server tasks settings and schedules:</td>
<td>Down</td>
</tr>
<tr>
<td>■ Check Software Update Package Integrity</td>
<td></td>
</tr>
<tr>
<td>■ Import Patch Data for Windows/Red Hat/SUSE</td>
<td></td>
</tr>
<tr>
<td>Run System Assessment Scan on Windows/Linux Computers task settings and schedules</td>
<td>Down</td>
</tr>
<tr>
<td>Windows/Linux System Assessment Scan policy settings</td>
<td>Down</td>
</tr>
<tr>
<td>Windows/Red Hat/SUSE Patch Remediation Settings policy</td>
<td>Down</td>
</tr>
</tbody>
</table>
**Table A-1**  
Items that are replicated by the default Notification Server replication schedule with no custom replication rules (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Replication direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Software Update Plug-in Policy settings</td>
<td>Down</td>
</tr>
<tr>
<td>Software update plug-in install, upgrade, and uninstall policy settings</td>
<td>Down</td>
</tr>
<tr>
<td>Software update policies</td>
<td>Down</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Item</th>
<th>Replication direction</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Language support information (Patch for Windows only)</td>
<td>Up</td>
<td>This information is replicated when the Patch Management Language Alerting rule is enabled.</td>
</tr>
<tr>
<td>OS inventory data (Patch for Linux only)</td>
<td>Up</td>
<td>This information is replicated when the Patch Linux OS Channel Resource Replication Rule is enabled.</td>
</tr>
<tr>
<td>Patch management metadata</td>
<td>Down</td>
<td>This information is replicated when the Patch Management Import Data Replication for Windows/Red Hat/SUSE rules are enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For Windows, only the updates and bulletins that are associated with the child computer's supported languages are replicated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For Linux, only the metadata for the channels that are relevant to the child Notification Server's client computers is replicated.</td>
</tr>
<tr>
<td>Compliance summary</td>
<td>Up</td>
<td>This information is replicated when the Patch Compliance Summary Replication rule is enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The system assessment scan result is replicated up as a summary.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>A</th>
<th>analyzing vulnerabilities. See assessing systems assessing systems 28 assigning severity levels 27</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>Check Software Update Package Integrity task about 29 checking package integrity 29 compliance analysis. See system assessment scan configuring Patch Management Solution core settings 26 severity levels 27 updates installation settings 28 Windows remediation settings 18 context-sensitive help 12 Core Services settings configuring 26</td>
</tr>
<tr>
<td>D</td>
<td>Distribute Software Updates wizard 22 distributing software bulletins viewing update summary reports 23 distributing software updates 22 documentation 12 download location 26 downloading patch management metadata 18 software updates catalog 18 downloading and distributing software updates 22 downloading software updates 31</td>
</tr>
<tr>
<td>H</td>
<td>help context-sensitive 12 hierarchy replicating data 33–34, 36 replicating patch management metadata 35 replicating software updates catalog 35</td>
</tr>
<tr>
<td>I</td>
<td>Import Patch Data for Windows task about 18 installing software update plug-in 17 inventory collecting. See system assessment scan</td>
</tr>
<tr>
<td>P</td>
<td>patch management import data. See patch management metadata Patch Management Import Data Replication rule configuring 35 Patch Management Language Alerting rule configuring 34 patch management metadata downloading 18 replicating 35 Patch Management Solution for Windows about 9 distributing software updates 19 implementing 15 overview 11 recommended workflow 15 patching recommended workflow 15 PMImport. See patch management metadata</td>
</tr>
<tr>
<td>R</td>
<td>Release Notes 12 relocating packages 29 replicating data in hierarchy 33–34, 36 replicating software update policies 36 replication direction 38 reports compliance 20 diagnostic 20 remediation status 20 software bulletin 20 viewing 20</td>
</tr>
</tbody>
</table>
restarts
configuring 28

S
security roles 39
severity levels
assigning 27
configuring 27
software bulletins
configuring installation settings 28
viewing update summary reports 23
software update plug-in
about 17
installing 17
uninstalling 26
upgrading 25
software update policy
replicate now 36
replicating 36
software updates
computer restart time 28
distributing 22
downloading 31
downloading and distributing 22
installation settings 28
installation time 28
software updates catalog
downloading 18
replicating 35
staging software updates. See downloading
system assessment scan
configuring 28

U
uninstalling
software update plug-in 26
upgrading
software update plug-in 25

V
vulnerability analysis. See windows system
assessment scan policy

W
Windows Patch Remediation Settings page 18
Windows remediation settings
configuring 18
<table>
<thead>
<tr>
<th>Glossary Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Software Update Package Integrity task</td>
<td>A task that checks that all software update packages have the correct new settings and values. This task runs when the package or program settings in the Patch Remediation Settings policies have been changed.</td>
</tr>
<tr>
<td>custom severity level</td>
<td>A user-defined level of importance that is applied to software updates.</td>
</tr>
<tr>
<td>data replication</td>
<td>A one-way transfer of data between Notification Server and a client computer or another Notification Server.</td>
</tr>
<tr>
<td>Distribute Software Updates wizard</td>
<td>A wizard that is used to create software update policies.</td>
</tr>
<tr>
<td>patch</td>
<td>An update or a hot fix that is used to improve or fix a software product.</td>
</tr>
<tr>
<td>Patch Management Import Data Replication for Windows rule</td>
<td>A component of Patch Management Solution that is used to send the patch management software update catalog files to any number of child Notification Server computers after these files are downloaded to a parent Notification Server computer.</td>
</tr>
<tr>
<td>patch management metadata</td>
<td>The information about the available updates.</td>
</tr>
<tr>
<td>Patch Remediation Center page</td>
<td>A page in the Symantec Management Console that lists all available software updates. From this page, users download (stage) the files and create Software Update policies.</td>
</tr>
<tr>
<td>remediation status report</td>
<td>An account that summarizes and details software associations and activities.</td>
</tr>
<tr>
<td>software bulletin</td>
<td>A collection of software update patches that are released in a bundle.</td>
</tr>
<tr>
<td>software update plug-in</td>
<td>A component of Patch Management Solution that handles the patch management functionality on a client computer. When a client computer requires a certain software update, the update is sent from the Notification Server computer 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.</td>
</tr>
<tr>
<td>software update policy</td>
<td>An element of Patch management that distributes software updates to the client computers.</td>
</tr>
<tr>
<td>Software Update Policy Wizard</td>
<td>A wizard that is used to create the executables that deliver software updates to managed computers.</td>
</tr>
<tr>
<td>stage</td>
<td>To prepare a software bulletin or update for distribution. When a user stages a software bulletin, all included software updates are downloaded from the vendor.</td>
</tr>
<tr>
<td><strong>system assessment scan</strong></td>
<td>A process that is used to periodically inventory operating systems, applications, and installed patches on the client computers that have the software update plug-in installed.</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>targeted deployment</strong></td>
<td>A process of deploying a software update to a client computer that specifically needs that particular update.</td>
</tr>
<tr>
<td><strong>Windows remediation settings</strong></td>
<td>The configuration of the way the Windows software updates are to be distributed. The settings include package server settings, program execution options, and language settings.</td>
</tr>
</tbody>
</table>