

Altiris™ Patch Management Solution from Symantec for Linux User's Guide

Version 7.0



Altiris™ Patch Management Solution for Linux 7.0 from Symantec

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.

Documentation version 7.0

Legal Notice

Copyright © 2009 Symantec Corporation. All rights reserved.

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

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.

XML-RPC.NET Charles Cook Copyright (c) 2006 Charles Cook The MIT License Copyright (c) 2006 Charles Cook 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 product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

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

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in

Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014

<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 maintenance 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 Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week
- Advanced features, including Account Management Services

For information about Symantec's Maintenance Programs, you can visit our Web site at the following URL:

www.symantec.com/techsupp/

Contacting Technical Support

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

www.symantec.com/techsupp/

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/techsupp/

Customer service

Customer service information is available at the following URL:

www.symantec.com/techsupp/

Customer Service is available to assist with 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 maintenance 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

Maintenance agreement resources

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

Asia-Pacific and Japan	contractsadmin@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportolutions@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:

Symantec Early Warning Solutions	These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.
Managed Security Services	These 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.
Educational Services	Educational 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

Select your country or language from the site index.

Contents

Technical Support	4	
Chapter 1	Introducing Patch Management Solution for Linux	9
	About Patch Management Solution for Linux	9
	Where to get more information	9
Chapter 2	Implementing Patch Management Solution for Linux	13
	Implementing Patch Management Solution for Linux	13
Chapter 3	Distributing Errata and Software Updates	15
	About errata and patches	15
	Downloading Novell updates	16
	Novell Updates Import Task	16
	Downloading Red Hat errata	17
	Red Hat Errata Import Task page	18
	Patch Management Remediation Center page	19
	About Software Update policies	20
	About staging errata and patches	20
	Staging errata and patches	21
	About Software Update policies and maintenance windows	21
	About the Software Update policy wizard	21
	Creating Software Update policies	23
Chapter 4	Using the Software Update Agent	25
	About the Software Update Agent	25
	About the Software Update Agent Rollout Job	26
	About the Software Update Agent Rollout Task	26
	Installing the Software Update Agent	26
	Upgrading the Software Update Agent	27
	Software Update Agent Upgrade page	27
	Configuring the Software Update Agent	28

	Default Software Update Agent Policy page	28
	Configuring the Update Agent Discovery Task	31
	Update Agent Discovery Task page	32
	Uninstalling the Software Update Agent	33
Chapter 5	Using Patch Management Solution for Linux	35
	Inventorying Linux servers	35
	Default Linux OS Inventory Policy page	36
	Gathering Novell inventory	36
	Default Novell Inventory Policy page	37
	Gathering Red Hat inventory	37
	Default Red Hat Inventory Policy page	38
	Configuring Novell settings	38
	Novell settings page	39
	Configuring Red Hat settings	40
	Red Hat settings page	41
Chapter 6	Using Patch Management Solution for Linux reports	43
	About Patch Management Solution for Linux reports	43
	About compliance reports	44
	Viewing compliance reports	44
	Viewing the Red Hat Software Update Compliance Portal	45
	Red Hat Software Update Compliance Portal page	45
	Viewing the Novell Software Update Compliance Portal	45
	Novell Software Update Compliance Portal page	46
	About Red Hat reports	46
	About SUSE reports	46
Index	47

Introducing Patch Management Solution for Linux

This chapter includes the following topics:

- [About Patch Management Solution for Linux](#)
- [Where to get more information](#)

About Patch Management Solution for Linux

Patch Management Solution for Linux lets you scan Red Hat and Novell Linux computers for security vulnerabilities. The solution then reports on the findings and lets you automate the downloading and distribution of needed errata, or software updates. Only SUSE updates are supported for Novell. This solution downloads the required patches and provides wizards to help you deploy them. During configuration, you can set up an automatic patch update schedule to ensure that managed computers are up-to-date and protected on an on-going basis.

Where to get more information

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

Table 1-1 Documentation resources

Document	Description	Location
Release Notes	<p>Information about new features and important issues.</p> <p>This information is available as an article in the Altiris Knowledge Base.</p>	<p>http://kb.altiris.com/</p> <p>You can search for the product name under Release Notes.</p>
Implementation Guide	<p>Information about how to install, configure, and implement this product.</p> <p>This information is available in PDF format.</p>	<p>The Product Support page, which is available at the following URL:</p> <p>http://www.symantec.com/business/support/all_products.jsp</p> <p>When you open your product's support page, look for the Documentation link on the right side of the page.</p>
User's Guide	<p>Information about how to use this product, including detailed technical information and instructions for performing common tasks.</p> <p>This information is available in PDF format.</p>	<ul style="list-style-type: none"> ■ The Documentation Library, which is available in the Symantec Management Console on the Help menu. ■ The Product Support page, which is available at the following URL: http://www.symantec.com/business/support/all_products.jsp <p>When you open your product's support page, look for the Documentation link on the right side of the page.</p>
Help	<p>Information about how to use this product, including detailed technical information and instructions for performing common tasks.</p> <p>Help is available at the solution level and at the suite level.</p> <p>This information is available in HTML help format.</p>	<p>The Documentation Library, which is available in the Symantec Management Console on the Help menu.</p> <p>Context-sensitive help is available for most screens in the Symantec Management Console.</p> <p>You can open context-sensitive help in the following ways:</p> <ul style="list-style-type: none"> ■ The F1 key ■ 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 Altiris products.

Table 1-2 Altiris information resources

Resource	Description	Location
Altiris Knowledge Base	Articles, incidents, and issues about Altiris products.	http://kb.altiris.com/
Altiris Juice	An online magazine that contains best practices, tips, tricks, and articles for users of Altiris products.	http://www.altiris.com/juice
Online forums	Forums for users of Altiris products.	http://forums.altiris.com/

Implementing Patch Management Solution for Linux

This chapter includes the following topics:

- [Implementing Patch Management Solution for Linux](#)

Implementing Patch Management Solution for Linux

Patch Management Solution for Linux requires some components to be configured or enabled before others function correctly. The recommended workflow is as follows:

To implement Patch Management Solution for Linux

- 1 Provide your credentials in the **Red Hat Network** tab of the Red Hat vendor policy to access the Red Hat Network (RHN).
See [“Configuring Red Hat settings”](#) on page 40.
- 2 Provide your credentials in the **Novell Customer Center** tab to access SLES 9 updates in the Novell Customer Center (NCC).
See [“Configuring Novell settings”](#) on page 38.
- 3 If required, change the default option values in the Patch Management Core Solution policy. See Patch Management Solution 7.0 User's Guide .
- 4 Configure the Update Agent Discovery Task to automatically subscribe discovered RedHat and Novell computers to each vendor's update service.
See [“Update Agent Discovery Task page”](#) on page 32.

- 5 Prepare client computers for patching by running the Software Update Agent Rollout Job.
See [“Installing the Software Update Agent”](#) on page 26.
- 6 Import information about Novell Updates and Red Hat Errata.
See [“Downloading Novell updates”](#) on page 16.
See [“Downloading Red Hat errata”](#) on page 17.
- 7 Stage errata from the Patch Remediation Center.
See [“Staging errata and patches”](#) on page 21.
- 8 Create Software Update Policies.
See [“Creating Software Update policies”](#) on page 23.
- 9 Run reports.
See [“About Patch Management Solution for Linux reports”](#) on page 43.

Distributing Errata and Software Updates

This chapter includes the following topics:

- [About errata and patches](#)
- [Downloading Novell updates](#)
- [Novell Updates Import Task](#)
- [Downloading Red Hat errata](#)
- [Red Hat Errata Import Task page](#)
- [Patch Management Remediation Center page](#)
- [About Software Update policies](#)
- [About staging errata and patches](#)
- [Staging errata and patches](#)
- [About Software Update policies and maintenance windows](#)
- [About the Software Update policy wizard](#)
- [Creating Software Update policies](#)

About errata and patches

Software bulletins that contain security updates for Red Hat Linux servers are called errata. Periodically, Redhat issues the Redhat Security Advisories (RHSA), Redhat Bug Advisories (RHBA), and Redhat Enhancement Advisories (RHEA), which are the equivalent of Microsoft Software Bulletins. The advisories are either

security or bug fixes or enhancements. Each advisory contains one or more patches (rpm packages). All the RHSAs, RHBAs, and RHEAs are available at <https://rhn.redhat.com/errata>.

Software bulletins that contain SUSE security updates for Novell Linux servers are called patches. Novell patches for different products may be released several times in a month.

Patch Management Solution for Linux does not support the rollout of kernel updates because the automatic restart functionality is not available. Updates that require a restart after installation should be deployed using Software Management Solution.

Downloading Novell updates

You can download required information about Novell software updates from the Novell Customer Center.

See [“About errata and patches”](#) on page 15.

To download Novell updates

- 1 In the Symantec Management Console, on the Manage menu, click **Jobs and Tasks**.
- 2 In the left pane, click **Jobs and Tasks > System Jobs and Tasks > Software > Patch Management > Novell Updates Import Task**.
- 3 In the right pane, make any wanted changes.
See [“Novell Updates Import Task”](#) on page 16.
- 4 Click **Save changes**.

Novell Updates Import Task

This page lets you specify settings for downloading and importing all the required information for managing Novell patches. These resources are necessary for populating the Patch Remediation Center and updating patches to managed computers.

Table 3-1 Options on the Novell Updates Import Task page

Option	Description
Import Options	Provides a history of changes that have been made to the page options.

Table 3-1 Options on the Novell Updates Import Task page (*continued*)

Option	Description
Incremental Import	Prevents the task from importing the updates that have already been imported.
Import patch rpms	Imports SUSE “*.patch.rpm” packages that may be smaller in size than full rpm packages.
Associate patch information with Novell patch rpms	This option is available only when Import patch rpms is selected.
Select software channels for import	Lets you choose the operating systems that you want to download updates for. You may have to double-click the heading for the operating system list to appear. You should select only the operating systems that are installed on existing managed computers.
Revise Software Update Tasks	Lets you choose to run the Revise Software Updates task after the Novell Update Import Task runs. The Revise Software Updates task checks software update tasks for data integrity issues and resolves them.
Disable the Superseded Software Update Advertisement when the Patch Management Import task has been completed	Disables the rollout of any software update tasks that contain superseded software updates.
Schedule	Lets you specify a schedule for running the task.

Downloading Red Hat errata

You can download required Red Hat errata information from the Red Hat Network.

See “[About errata and patches](#)” on page 15.

To download Red Hat errata

- 1 In the Symantec Management Console, on the Manage menu, click **Jobs and Tasks**.
- 2 In the left pane, click **Jobs and Tasks > System Jobs and Tasks > Software > Patch Management > Red Hat Errata Import Task**.

- 3 In the right pane, make any wanted changes.
See [“Red Hat Errata Import Task page”](#) on page 18.
- 4 Click **Save changes**.

Red Hat Errata Import Task page

This page lets you specify settings for downloading and importing all the required information for managing Red Hat errata. These resources are necessary for populating the Patch Remediation Center and updating patches to managed computers. Importing errata for all available operating systems may take several days. The duration is due to the number of packages that must be downloaded from the Red Hat Network.

See [“Downloading Red Hat errata”](#) on page 17.

Table 3-2 Options on the Red Hat Errata Import Task page

Options	Description
Import Options	Lets you view a history of any changes that were made to the page options.
Incremental Import	Prevents the task from importing any patches that have already been imported.
Select software channels for import	Lets you select the operating systems that you want to download updates for. You may have to double-click the heading for the operating system list to appear.
Revise Software Update Tasks	Lets you choose to run the Revise Software Updates task after the Novell Update Import Task runs. The Revise Software Updates task checks software update tasks for data integrity issues and resolves them.
Disable the Superseded Software Update Advertisement when the Patch Management Import task has been completed	Lets you disable the rollout of any software update tasks that contain superseded software updates.
Schedule	Lets you specify a schedule for running the task.

Patch Management Remediation Center page

This page lets you view, stage, and distribute all Red Hat errata and Novell software updates. When you stage a software bulletin, all associated updates are downloaded to the Notification Server computer from the Red Hat Network or Novell Customer Center. After a bulletin is staged you can create Software Update Policies to distribute the software bulletin to managed computers. You can then create Software Update Policies to distribute the software updates to managed computers.

See [“Creating Software Update policies”](#) on page 23.

Table 3-3 Options on the Patch Remediation Center page

Option	Description
Actions	Lets you perform an action on selected software bulletins.
Save As	Lets you save the current listing.
View	Lets you select a value to filter the table entries with. For example, Latest or Last Month.
Group by	Lets you select a value to filter table entries with. This function is the same as clicking a column header.
Search	Lets you enter keywords or a software bulletin number to search for specific bulletins.
Parameters	Lets you choose which vendor's software updates to display. For example, Novell.

Table 3-3 Options on the Patch Remediation Center page (*continued*)

Option	Description
Table items	<p>Bulletin – The bulletin's number, as supplied by the vendor.</p> <p>Severity – The bulletin's vendor-specified severity level.</p> <p>Custom Severity – The bulletin's user-defined severity level.</p> <p>Staged – Displays if the bulletin has been set to download the included software updates.</p> <p>Policies – The number of Software Update Policies that have been created from the bulletin.</p> <p>Updates – The number of software updates that are included in the bulletin.</p> <p>Downloaded – The number of software updates that are currently downloaded.</p> <p>Released – The date the bulletin was released.</p> <p>Revised – The date the bulletin was revised.</p> <p>Description – A description of the vulnerabilities that the software bulletin fixes.</p>

About Software Update policies

These user-created policies distribute software updates to managed computers. After you stage errata and download the associated software updates, you must create Software Update policies. Software Update policies deploy software updates to the appropriate computers. They are stored in the Red Hat and Novell folders under Policies > Software > Patch Management > Software Update Policies.

See [“About errata and patches”](#) on page 15.

About staging errata and patches

You stage errata and patches from the Patch Remediation Center, where all available updates are listed. When you stage patches or errata, all associated software updates are downloaded to the Notification Server computer from the RHN or NCC. After a patch or erratum is staged you can create Software Update Policies to distribute software updates to managed computers.

See “[Patch Management Remediation Center page](#)” on page 19.

See “[Staging errata and patches](#)” on page 21.

Staging errata and patches

You can stage errata or patches so you can then create a Software Update policy to distribute the updates to managed computers.

See “[About staging errata and patches](#)” on page 20.

To stage errata or patches

- 1 In the Symantec Management Console, on the Actions menu, click **Software > Patch Remediation**.
- 2 In the right pane, select the all of the patches and errata you want to stage.
- 3 Right-click the selected items and select **Stage**.

About Software Update policies and maintenance windows

Maintenance windows are defined time periods in which maintenance tasks, including Software Update Policies, are performed. To ensure Software Update Policies abide by maintenance windows, leave the Override Maintenance Window check box unchecked in the first page of the Software Update Policy Wizard. Also leave the check box unchecked in the schedule dialog for any task. If the box is not checked, the Software Update Agent ignores maintenance windows. The Software Update Agent then installs the updates as instructed otherwise by the Software Update Policy.

About the Software Update policy wizard

You use the Software Update policy wizard to create Software Update policies that distribute errata and software updates to managed computers. You can create a software task from an individual software update, but that is not the most efficient way to distribute updates. The wizard includes two pages.

Table 3-4 Options on the first page of the Software Update Policy Wizard

Option	Description
Software Update(s)	The names of each software update or updates that are included in the task.

Table 3-4 Options on the first page of the Software Update Policy Wizard
(continued)

Option	Description
Software Bulletin(s)	The name of the bulletin or bulletins you have chosen to make tasks for. You cannot edit the software bulletins through the Software Update policy wizard.
Name	The name of the tasks you have chosen from the tasks window. This field is populated automatically if only one task is listed in the Tasks field.
Description	The vendor's description of the bulletin.
Package Options	<p>Use Multicast when the Altiris Agent's multicast option is enabled – Lets you choose to use multicast features.</p> <p>Initiate execution (other than agent default) – You can choose to run the Software Update Policy at a different time to the time that is specified in the Software Update Agent settings.</p> <p>On schedule – You can choose to specify a schedule.</p> <p>Override Maintenance Window Settings – You can choose to override specified maintenance windows settings.</p>
Apply to computers	<p>Specifies the target collection or collections to which the Software Update policy applies.</p> <p>If you use the Software Update policy wizard, the correct target collection for the selected software bulletin is automatically applied.</p> <p>You can change the collection with the Collection Selector hyperlink.</p>

Table 3-5 Options on the second page of the Software Update Policy Wizard

Option	Description
Enable Software Update Task	<p>You can click On or Off to enable the Software Update Policy for the software bulletin and included software updates. The name of the executable file for each software update in a software bulletin is displayed.</p> <p>Update Name – The name of each software update executable. If Enable is selected, all of the executables is enabled. Click the hyperlink to open the resource manager page for the software update.</p> <p>Dependencies – The dependencies that the policy requires.</p>
Distribute software updates	Lets you complete the wizard.

Creating Software Update policies

The Software Update policy wizard lets you easily create and set up Software Update policies to distribute errata and patches to managed computers. Software Update policies must be created before you can distribute any software updates to managed computers.

See [“About errata and patches”](#) on page 15.

See [“About the Software Update policy wizard”](#) on page 21.

To create a Software Update policy

- 1 In the Symantec Management Console, on the Actions menu, click **Software > Patch Remediation**.
- 2 In the content pane, select the staged software updates that you want to distribute.
- 3 Right-click the updates and select **Software Update Policy Wizard**.
- 4 Complete the Software Update policy wizard, making any wanted changes.

See [“About the Software Update policy wizard”](#) on page 21.

Using the Software Update Agent

This chapter includes the following topics:

- [About the Software Update Agent](#)
- [About the Software Update Agent Rollout Job](#)
- [About the Software Update Agent Rollout Task](#)
- [Installing the Software Update Agent](#)
- [Upgrading the Software Update Agent](#)
- [Software Update Agent Upgrade page](#)
- [Configuring the Software Update Agent](#)
- [Default Software Update Agent Policy page](#)
- [Configuring the Update Agent Discovery Task](#)
- [Update Agent Discovery Task page](#)
- [Uninstalling the Software Update Agent](#)

About the Software Update Agent

The Software Update Agent manages patch management functionality on a managed computer. When a managed computer requires a certain software update, the update is sent to the Software Update Agent. The Software Update Agent ensures that the update is applicable and not already installed, then installs it.

See [“Configuring the Software Update Agent”](#) on page 28.

See [“Installing the Software Update Agent”](#) on page 26.

About the Software Update Agent Rollout Job

This job consists of the following tasks:

- **The Update Agent Discovery Task**
Detects the managed computers that are ready to receive updates. The task also sends back information on which managed computers need to be configured to access the Red Hat Network and the Novell Customer Center.
- **The Software Update Agent Rollout Task**
Installs the Software Update Agent on any managed computer that does not yet have it.

See [“Installing the Software Update Agent”](#) on page 26.

See [“About the Software Update Agent”](#) on page 25.

About the Software Update Agent Rollout Task

The Software Update Agent Rollout Job uses this task to distribute the Software Update Agent to managed computers. The Software Update Agent Rollout Task is read only.

See [“About the Software Update Agent Rollout Job”](#) on page 26.

Installing the Software Update Agent

The Software Update Agent manages all of the Patch Management Solution functionality on a managed computer.

See [“About the Software Update Agent”](#) on page 25.

See [“About the Software Update Agent Rollout Job”](#) on page 26.

To install the Software Update Agent

- 1 In the Symantec Management Console, on the Settings menu, click **Solution Settings > Patch Management Configuration**.
- 2 In the left pane, click **Patch Management > Linux > Software Update Agent Rollout > Software Update Agent Rollout Job**.
- 3 In the right pane, either click **Quick Run** and select a workgroup, or click **Schedule**, and specify a schedule.
- 4 Click **Save changes**.

Upgrading the Software Update Agent

Managed computers already using an older version of software update agent must upgrade to version 7.0 to work with Patch Management Solution 7.0.

See [“Software Update Agent Upgrade page”](#) on page 27.

To upgrade the Software Update Agent

- 1 In the Symantec Management Console, on the Settings menu, click **Settings > All Settings**.
- 2 In the left pane, click **Settings > Software > Software Update Agent for Linux > Rollout > Software update Agent Upgrade**.
- 3 In the right pane, make any wanted changes.
See [“Software Update Agent Upgrade page”](#) on page 27.
- 4 Click **Save changes**.

Software Update Agent Upgrade page

This page lets you upgrade the software update agent on managed computers. Computers already using an older version of software update agent must upgrade to version 7.0.

See [“Upgrading the Software Update Agent”](#) on page 27.

Table 4-1 Options on the Software Update Agent Upgrade page

Option	Description
On/Off	Lets you enable or disable the task.
Package Name	The name of the package.
Applied to	By default, this task is applied to the resource filter All Linux Computers Requiring Software Update Agent Upgrade Target. You can change this target if wanted.
Schedule	Lets you specify a schedule for the policy to run. You can choose a time, or window of time in which to roll out the agent. You also have the option of immediately rolling out the agent.

Table 4-1 Options on the Software Update Agent Upgrade page (*continued*)

Option	Description
Extra schedule options	The options are as follows: Run once ASAP – immediately roll out the agent. User can run – allow the user to choose when the agent installs. Notify user when the task is available – notify users when the task is ready to run. Warn before running – warn users before the agent installs.
Save changes	Saves the changes you have made to the task.

Configuring the Software Update Agent

The Software Update Agent is a plug-in agent for the Altiris Agent. The Software Update Agent manages the Patch Management Solution functionality on a managed computer. This agent needs to be deployed to all managed computers that you want to distribute software updates to.

See [“Default Software Update Agent Policy page”](#) on page 28.

See [“About the Software Update Agent”](#) on page 25.

To configure the Software Update Agent

- 1 In the Symantec Management Console, in the Settings menu, click **Solution Settings > Patch Management Configuration**.
- 2 In the left pane, click **Patch Management > Linux > Software Update Agent Configuration > Default Software Update Agent Policy**.
- 3 In the right pane, make any wanted changes.
 See [“Default Software Update Agent Policy page”](#) on page 28.
- 4 Click **Apply**.

Default Software Update Agent Policy page

This policy is used to specify settings for the Software Update Agent. The settings are then used to automatically install software updates on managed computers. The filter that the policy targets is designed to find any agents that do not have

a configuration policy applied to them. Settings that are specified in this page apply to all Linux computers that have the Software Update Agent installed.

See “[Configuring the Software Update Agent](#)” on page 28.

Table 4-2 Options on the Installation Schedules tab of the Default Software Update Agent Policy

Option	Description
Software Update Installation	<p>These options determine when software updates get installed on the managed computer and when the managed computer restarts. The options allow for effective batching of software update installations.</p> <p>Add Schedule – Lets you choose to specify a schedule for applying software updates to the managed computer. On this schedule, QChain is called to chain the software updates together, and then the software updates are sent to the managed computer. QChain is only applicable to computers running Windows NT 4 or later. This schedule displays on the Software Updates tab of the Altiris Agent.</p> <p>Reinstallation attempts after task failure – Lets you set the number of times Patch Management should attempt to reinstall a software update after a task failure.</p> <p>Reinstallation attempts when task requires a reboot prior to install – Sometimes a software update requires a restart. This option sets the number of times to retry the software update installation after the restart.</p> <p>Maximum number of consecutive successful installations allowed per update – The number of times an update can be installed.</p> <p>Allow user to initiate – Allows users to initiate software update installation from the Altiris Agent by clicking the Start Software Update icon.</p>

Table 4-2 Options on the Installation Schedules tab of the Default Software Update Agent Policy (*continued*)

Option	Description
Reboot Defaults	<p>Allow reboot after installation – Lets you choose to allow reboots after installation.</p> <p>Never – Lets you choose to not automatically restart the user’s computer after a software update installation.</p> <p>Scheduled – Lets you choose if you want to specify a restart schedule for software updates that require a restart. For example, you do not want to affect user productivity with repeated restart during work hours, so you create an after hours restart schedule. This schedule displays on the Software Updates tab of the Altiris Agent.</p> <p>Warning: Do not set your restart schedule too soon after the Software Update Installation schedule. The restart schedule can cause the computer to restart before updates have finished installing.</p> <p>At end of software update cycle – Click to restart after all updates have been installed.</p>
Maintenance Windows	Lets you choose to Abide by maintenance windows to only install software updates during maintenance windows.
Apply to	Specifies the filter or filters to which this policy applies.

Table 4-3 Options on the Notification tab of the Default Software Update Agent Policy

Option	Description
Software Update Installation Notice	<p>Notify user – Lets you choose to send a message to users that a Patch Management task is about to run.</p> <p>The default dialog box message is as follows: New software updates ready to apply. The user can choose to Install Now, or Close the dialog box.</p> <p>Custom Message – Lets you choose to create a customized message of up to 128 characters. For example, Software updates installing on your computer in 10 minutes. Please ensure that all work is saved.</p>
Software Update Reboot Notifications	<p>These options let you control whether or not you want to notify users when a software update requires a restart. Each of the following notification messages appears in a separate dialog box on the user's screen.</p> <p>Show pending message – Lets you choose to warn the user of a pending restart. The time you select represents how soon before the pending restart the user is warned. The user can choose to Reboot Now.</p> <p>Show reminder message – Lets you choose to notify a user that a restart is required. If the user does not manually restart, the computer restarts according to your settings in the Default Reboot Options section. The user can choose to Reboot Later, or Reboot Now.</p> <p>Allow user to defer – Lets you choose to warn a user of a pending restart. The user can choose to Reboot now, or defer the restart and choose the deferral time from a menu.</p>

Configuring the Update Agent Discovery Task

This task discovers managed computers with registered Red Hat Network clients.

To configure the Update Agent Discovery Task

- 1 In the Symantec Management Console, on the Settings menu, click **Agents/Plug-ins > All Agents/Plug-ins**.
- 2 In the left pane, click **Agents/Plug-ins > Software > Software Update Agent for Linux > Rollout Update Agent Discovery Task**.
- 3 In the right pane, make any wanted changes.
See “[Update Agent Discovery Task page](#)” on page 32.
- 4 Click **Save changes**.

Update Agent Discovery Task page

This page is used by the Software Update Agent Rollout Job to discover managed computers with registered Red Hat Network computers and reports software channel subscription details.

See “[Configuring the Update Agent Discovery Task](#)” on page 31.

Note: SLES 9 computers can only be registered successfully by Patch Management Solution for Linux if the `suse_register` tool (from the `suseRegister` rpm package) is installed. The tool is available in SLES 9 SP4 but is not installed by default. After registering SUSE Linux managed computers, you should assign the proper activation code for the registered computers in the NCC within 15 days.

Table 4-4 Options on the Update Agent Discovery Task page

Option	Description
Try to register not registered clients	This option is selected by default to automatically subscribe discovered Red Hat and Novell computers to each vendor’s update service. Only subscribed computers receive patches. The solution updates computers to avoid breaking vendor license agreements. If this option is selected, enter an email address in the NCC account e-mail field.

Table 4-4 Options on the Update Agent Discovery Task page (*continued*)

Option	Description
Red Hat Options	<p>After installing Red Hat Enterprise Linux, an applet appears that displays the update status of the computer as defined by the Red Hat Network (RHN). This applet leverages the up2date agent to alert users when an update is available. If the applet is left in place, the user is alerted of new patches outside of the Symantec Patch Management framework and prompted to update directly with the Red Hat Satellite Server (RHSS).</p> <p>Disable Red Hat Network Notifications on clients running up2date by removing rhn-applet lets you remove the applet.</p>
Novel Account Information	<p>The email address entered here is used to register SUSE computers with a proper account in the NCC.</p>
Task Status	<p>The Quick Run icon lets you immediately run the task. The New Schedule icon lets you create a schedule for the task.</p> <p>In the schedule dialog box, the Override Maintenance Windows option lets you run the task at the scheduled time regardless of maintenance windows.</p> <p>See “About Software Update policies and maintenance windows” on page 21.</p>
Save changes	<p>Saves any changes you have made to the task.</p>

Uninstalling the Software Update Agent

You can uninstall the Software Update Agent if there is an extended period of time when you do not want to use patch management features on a managed computer.

Warning: Ensure that the Software Update Rollout Job is disabled before uninstalling the Software Update Agent.

See [“Installing the Software Update Agent”](#) on page 26.

To uninstall the Software Update Agent

- 1** In the Symantec Management Console, in the Settings menu, click **Solution Settings > Patch Management Configuration**.
- 2** In the left pane, click **Patch Management > Linux > Software Update Agent Uninstall > Software Update Agent Uninstall**.
- 3** In the right pane, click the **On** symbol.
- 4** Leave the default settings unless specifically required.
- 5** Click **Save changes**.

Using Patch Management Solution for Linux

This chapter includes the following topics:

- [Inventorying Linux servers](#)
- [Default Linux OS Inventory Policy page](#)
- [Gathering Novell inventory](#)
- [Default Novell Inventory Policy page](#)
- [Gathering Red Hat inventory](#)
- [Default Red Hat Inventory Policy page](#)
- [Configuring Novell settings](#)
- [Novell settings page](#)
- [Configuring Red Hat settings](#)
- [Red Hat settings page](#)

Inventorying Linux servers

You can gather operating system and installed update inventory from Linux servers.

To inventory Linux servers

- 1 In the Symantec Management Console, on the Settings menu, click **Solution Settings > Patch Management Configuration**.
- 2 In the left pane, click **Patch Management > Linux > Software Inventory > Global > Default Linux OS Inventory Policy**.
- 3 In the right pane, make any wanted changes to the default settings.
See “[Default Linux OS Inventory Policy page](#)” on page 36.
- 4 Click **Apply**.

Default Linux OS Inventory Policy page

This page lets you inventory operating systems and installed updates on managed Linux computers. The Software Update Agent collects the inventory. Also, from this information filters are automatically created to assist with the targeting of Software Update policies.

See “[Inventorying Linux servers](#)” on page 35.

Table 5-1 Options on the Default Linux OS Inventory Policy page

Option	Description
Interval	Lets you specify how often you want to gather inventory from Linux servers. For example, every 4 hours.
Report Inventory	The Only if changed option is selected by default to conserve network traffic. You can click Always if you have a specific need to gather full inventory from your Linux servers regularly.
Send inventory summary	Lets you choose to send inventory summary back to Notification Server .
Apply to	The target to which you want the policy to apply. The default target is All Linux Computers with Software Update Agent Installed. Only change the target if you have a specific need for doing so.

Gathering Novell inventory

You can gather Novell update inventory from Linux servers.

To gather Novell inventory from Linux servers

- 1 In the Symantec Management Console, on the Settings menu, click **Solution Settings > Patch Management Configuration**.
- 2 In the left pane, click **Patch Management > Linux > Novell > Default Novell Inventory Policy**.
- 3 In the right pane, make any wanted changes to the default settings.
See [“Default Novell Inventory Policy page”](#) on page 37.
- 4 Click **Apply**.

Default Novell Inventory Policy page

This page lets you gather Novell update information from managed Linux computers. The Software Update Agent collects the inventory. Also, from this information filters are automatically created to assist with the targeting of Software Update policies.

See [“Gathering Novell inventory”](#) on page 36.

Table 5-2 Options on the Default Novell Inventory Policy page

Option	Description
Interval	Specifies how often Novell inventory is gathered from Linux servers. For example, every 4 hours.
Report Inventory	The Only if changed option is selected by default to conserve network traffic. Click Always if you have a specific need to gather full inventory from your Linux servers regularly.
Send inventory summary	Lets you choose to send inventory summary to Notification Server .
Applies to	The target to which you want the policy to apply. The default target is All Linux Computers with Software Update Agent Installed. Only change the target if you have a specific need for doing so.

Gathering Red Hat inventory

You can gather Red Hat errata information from Linux servers.

To gather Red Hat inventory from Linux servers

- 1 In the Symantec Management Console, on the Settings menu, click **Solution Settings > Patch Management Configuration**.
- 2 In the left pane, click **Patch Management > Linux > Red Hat Default Red Hat Inventory Policy**.
- 3 In the right pane, make any wanted changes.
See “[Default Red Hat Inventory Policy page](#)” on page 38.
- 4 Click **Apply**.

Default Red Hat Inventory Policy page

This page lets you gather errata information from managed Linux computers. The Software Update Agent collects the inventory. Also from this information, filters are automatically created to assist with the targeting of Software Update policies.

See “[About errata and patches](#)” on page 15.

See “[Gathering Red Hat inventory](#)” on page 37.

Table 5-3 Options on the Default Red Hat Inventory Policy page

Option	Description
Inventory	Specifies how often Novell inventory is gathered from Linux servers. For example, every 4 hours.
Report Inventory	The Only if changed option is selected by default to conserve network traffic. Click Always if you have a specific need to gather full inventory from your Linux servers regularly.
Send inventory summary	Lets you choose to send inventory summary to Notification Server .
Applies to	The target to which you want the policy to apply. The default target is All Linux Computers with Software Update Agent Installed. Only change the target if you have a specific need for doing so.

Configuring Novell settings

You can set up how you want to distribute Novell updates.

To configure Novell settings

- 1 In the Symantec Management Console, on the Settings menu, click **Solution Settings > Patch Management Configuration**.
- 2 In the left pane, click **Patch Management > Server Settings > Novell > Novell**.
- 3 In the right pane, make any wanted changes.
See “[Novell settings page](#)” on page 39.
- 4 Click **Apply**.

Novell settings page

This page lets you configure how you want Novell updates distributed. It lets you define which collections to send updates to, where to store updates, when to delete old updates, and more. Some of these settings are used as default values in the Software Update policy wizard. All Novell updates have these settings by default. If you change these settings, existing Software Update policies and packages are not updated with these defaults. You can force them to update by re-creating packages from the Patch Remediation Center.

See “[Configuring Novell settings](#)” on page 38.

Table 5-4 Options on the General tab of the Novell page

Option	Description
Verify authenticity of downloaded Software Updates	Enabled by default, this checks that updates are Novell certified.
Software Update Distribution Options	<p>Patch Collection Update Interval – Specifies a maintenance window during which managed computers receive software updates from Software Update policies. For example, Start at 12AM and End at 3AM.</p> <p>The table shows the filter that the policy targets. The default filter is as follows: All Linux Computers with Software Update Agent Installed Target. If you need to change the filter, click Apply to and select a new target or individual computers. Use the Search field to search for a computer or target by name.</p>

Table 5-5 Options on the Advanced tab of the Novell page

Option	Description
Package Defaults	Specifies how often to delete software update packages.
Package Distribution	<p>Allow Package Server distribution - This field is checked by default to ensure that a package server processes software update packages (recommended).</p> <p>For more information, see topics on package servers in the Symantec Management Platform Help.</p> <p>Use alternate download location on Package Server - Specifies a different Location to download packages onto a package server.</p> <p>Use alternate download location on client - Specifies a different Location to download packages on managed computers. This option is grayed out because the solution requires that all packages are downloaded to same directory on a managed computer.</p>

Table 5-6 Options on the Programs tab of the Novell page

Options	Description
Program Defaults	The Terminate after option specifies a time after which software update tasks are terminated.
Agent Events	Specifies whether or not to send the relevant events from managed computers to the Notification Server computer.

The Novell Customer Center tab of the Novell page is where you enter your Novell customer center access credentials.

Note: All managed computers on the same Notification Server must use the same Novell account.

Configuring Red Hat settings

You can set up how you want Red Hat errata distributed.

To configure Red Hat settings

- 1 In Symantec Management Console, on the Settings menu, click **Solutions Settings > Patch Management Configuration**.
- 2 In the left pane, click **Patch Management > Server Settings > Red Hat > Red Hat**.
- 3 In the right pane, make any wanted changes.
See [“Red Hat settings page”](#) on page 41.
- 4 Click **Apply**.

Red Hat settings page

This page lets you configure how you want Linux errata distributed. You can configure which collections to send errata to, where to store errata, when to delete old errata, and more. Some of these settings are used as default values in the Software Update Policy Wizard. All Linux errata have these settings by default. If you change these settings, existing Software Update Tasks and packages are not updated with these defaults. You can force them to update by re-creating packages from the Patch Remediation Center.

See [“Configuring Red Hat settings”](#) on page 40.

Table 5-7 Options on the General tab of the Red Hat page

Option	Description
Verify authenticity of downloaded Software Updates	Enabled by default, this checks that erratum are Red Hat certified.
Software Update Distribution Options	<p>Patch Collection Update Interval – Specifies a maintenance window during which managed computers receive software updates from Software Update Policies. For example, Start at 12AM and End at 3AM.</p> <p>The table shows the filter that the policy targets. By default, it is the All Linux Computers with Software Update Agent Installed Target. If you need to change the filter, click Apply to and select a new target or individual computers. Use the Search field to search for a computer or target by name.</p>

Table 5-8 Options on the Advanced tab of the Red Hat page

Option	Description
Package Defaults	Specifies how often software update packages are deleted.
Package Distribution	<p>Allow Package Server distribution – This field is checked by default to ensure that a package server processes software update packages (recommended). For further information, see Notification Server documentation.</p> <p>Use alternate download location on Package Server – Check if you want to specify a different Location to download packages onto a package server.</p> <p>Use alternate download location on client – Check if you want to specify a different Location to download packages on managed computers. This option is grayed out because the solution requires that all packages are downloaded to same directory on a managed computer.</p>

Table 5-9 Options on the Programs tab of the Red Hat page

Option	Description
Program Defaults	The Terminate after option specifies a time after which to terminate software update tasks.
Agent Events	Specifies whether or not to send the relevant events from managed computers to the Notification Server computer .

The Red Hat Network tab of the Red Hat page is where you enter your Red Hat Network access credentials.

Note: All managed computers on the same Notification Server must use the same Red Hat Network account.

Using Patch Management Solution for Linux reports

This chapter includes the following topics:

- [About Patch Management Solution for Linux reports](#)
- [About compliance reports](#)
- [Viewing compliance reports](#)
- [Viewing the Red Hat Software Update Compliance Portal](#)
- [Red Hat Software Update Compliance Portal page](#)
- [Viewing the Novell Software Update Compliance Portal](#)
- [Novell Software Update Compliance Portal page](#)
- [About Red Hat reports](#)
- [About SUSE reports](#)

About Patch Management Solution for Linux reports

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

See “[About compliance reports](#)” on page 44.

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. The Red Hat Software Update Compliance

Portal is a portal page comprised of a number of Web parts displaying results from commonly used reports.

See [“Red Hat Software Update Compliance Portal page”](#) on page 45.

About compliance reports

Compliance reports are the key to quickly determining what software updates and errata your managed computers require. The reports are used to determine if computers are up to date with the latest errata and software updates.

See [“About errata and patches”](#) on page 15.

Compliance reports also check if a particular update is installed on your managed computers. Compliance reports are useful if a specific security issue affects your network environment and a certain update fixes the problem. These reports are featured on the Red Hat Software Update Compliance Portal and Novell Software Update Compliance Portal pages for easy access.

See [“Red Hat Software Update Compliance Portal page”](#) on page 45.

See [“Novell Software Update Compliance Portal page”](#) on page 46.

Another important feature of compliance reports is the ability to start distributing software updates directly from report results. For example, if you want to quickly distribute all critical Red Hat updates, you can sort the report results by severity. Then you can right-click all critical updates and select Stage. From this point you can create Software Update Policies to distribute the updates.

Patch Management for Linux compliance reports are as follows:

- Red Hat Compliance by Computer
- Red Hat Compliance by Errata
- Red Hat Compliance by Update
- SUSE Compliance by Computer
- SUSE Compliance by Errata
- SUSE Compliance by Update

See [“Viewing compliance reports”](#) on page 44.

Viewing compliance reports

Compliance reports tell you which software bulletins or updates need to be installed on which computers to address known vulnerabilities.

To view Red Hat Compliance reports

- 1 In the Symantec Management Console, on the Reports menu, click **All Reports**.
- 2 In the left pane, click **Reports > Software > Patch Management > Compliance**.
- 3 Choose one of the Red Hat or SUSE compliance reports.
- 4 In the right pane, modify any settings you want, and click **Refresh**.

Viewing the Red Hat Software Update Compliance Portal

You can view Red Hat errata`compliance information at a glance.

See “[Red Hat Software Update Compliance Portal page](#)” on page 45.

To view the Red Hat Software Update Compliance Portal

- 1 In the Symantec Management Console, on the Home menu, click **Patch Management > Patch Management RedHat**.
- 2 In the right pane, you can see the portal page.

Red Hat Software Update Compliance Portal page

This page displays results from Patch Management Solution for Linux reports. For example, the Red Hat Vulnerabilities Web part tells you which of your Linux servers are vulnerable to known Red Hat security problems.

See “[Viewing the Red Hat Software Update Compliance Portal](#)” on page 45.

Viewing the Novell Software Update Compliance Portal

You can view Novell Software Update`compliance information at a glance.

See “[Novell Software Update Compliance Portal page](#)” on page 46.

To view the Novell Software Update Compliance Portal

- 1 In the Symantec Management Console, on the Home menu, click **Patch Management > Patch Management Novell**.
- 2 In the right pane, you can see the portal page.

Novell Software Update Compliance Portal page

This page displays results from Patch Management Solution for Linux reports. For example, the Novell Vulnerabilities Web part tells you which of your Linux servers are vulnerable to known Novell security problems.

See [“Viewing the Novell Software Update Compliance Portal”](#) on page 45.

About Red Hat reports

The Red Hat folder contains the following reports:

- Red Hat Entitlement Status
This report lists managed Red Hat Linux computers and shows that they have proper Red Hat entitlements.
- Red Hat Software Channels Subscription
This report shows a list of managed computers that is based on Red Hat Channel Subscription.

The folder is located under the path Reports > Software > Patch Management.

About SUSE reports

The SUSE folder contains the SUSE Entitlement Status report, which lists managed SUSE computers and shows that they have proper Novell entitlements.

The folder is located under the path Reports > Software > Patch Management.

Index

C

- compliance reports
 - about 44
 - viewing 44
- context-sensitive help 9

D

- Default Linux OS Inventory Policy
 - about 36
 - configuration 35
- Default Novell Inventory Policy
 - about 37
 - configuration 36
- Default Red Hat Inventory Policy
 - about 38
 - configuration 37
- Default Software Update Agent Policy page
 - about 28
- documentation 9

E

- errata and patches
 - about 15
 - staging 21

H

- help
 - context-sensitive 9

M

- maintenance windows
 - about 21

N

- Novell patches
 - managing 16
- Novell settings page
 - about 39
 - configuration 38

- Novell Software Update Compliance Portal
 - about 46
 - viewing 45
- Novell Updates Import Task
 - about 16
 - configuration 16

P

- Patch Management for Linux reports
 - about 43
- Patch Management Remediation Center
 - about 19
- Patch Management Solution for Linux
 - about 9
 - implementation 13

R

- Red Hat Errata Import Task
 - about 18
 - configuration 17
- Red Hat reports
 - about 46
- Red Hat settings page
 - about 41
 - configuration 40
- Red Hat Software Update Compliance Portal
 - about 45
 - viewing 45
- Release Notes 9

S

- Software Update Agent
 - uninstall 33
- software update agent
 - about 25
 - configuration 28
 - installation 26
 - upgrading 27
- software update agent rollout job
 - about 26

- Software Update Agent Rollout Task
 - about 26
- Software Update Agent Upgrade page
 - about 27
- Software Update policies
 - about 20
 - creating 23
- Software Update policy wizard
 - about 21
- staging errata and patches
 - about 20
- SUSE reports
 - about 46

U

- Update Agent Discovery Task
 - about 32
 - configuration 31