Altiris™ Software Management Solution from Symantec Users Guide

Version 7.0 SP2

✸ symantec.™

Altiris™ Software Management Solution from Symantec Users Guide

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

Documentation version 7.0 SP2

Legal Notice

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

Additional enterprise services

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

Enterprise services that are available include the following:

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

Introducing Software Management Solution

This chapter includes the following topics:

- About Software Management Solution
- Components of Software Management Solution
- What you can do with Software Management Solution
- How 6.x features compare to Software Management Solution 7.0
- Where to get more information

About Software Management Solution

Software Management Solution provides intelligent and bandwidth-sensitive distribution and management of software from a central Web console. It significantly reduces desktop visits and lets you easily support your mobile work force.

Software Management Solution also lets users directly download and install approved software or request other software.

Software Management Solution integrates with the Software Catalog and the Software Library that are part of the Symantec Management Platform. By leveraging this information, Software Management Solution ensures that the correct software gets installed, remains installed, and runs without interference from other software. This integration lets your administrators focus on delivering the correct software instead of redefining the packages, command lines, and so on for each delivery.

For more information, see the topics about the Software Catalog and the Software Library in the *Symantec Management Platform Help*.

Software Management Solution combines the functionality of earlier versions of Software Delivery Solution and Application Management Solution. It also supports the software virtualization technology that was available in Altiris Software Virtualization Solution.

See "How 6.x features compare to Software Management Solution 7.0" on page 17.

Software Management Solution supports packages for the Windows, UNIX, Linux, and Mac operating systems. With few exceptions, all the functions in Software Management Solution work the same for all platforms. For example, you use the same method to create a delivery task for a Windows, UNIX, Linux, or Mac OS package.

For a complete list of the platforms that Software Management Solution supports, see the *Software Management Solution Release Notes*.

See "How Software Management Solution integrates with the Software Catalog and Software Library" on page 93.

See "Components of Software Management Solution" on page 14.

See "What you can do with Software Management Solution" on page 15.

Components of Software Management Solution

The components of Software Management Solution let you deliver and manage software on client computers.

Table 1-1   Components of Software Management Solution

Component	Description
Software delivery tasks and policies	You can use any of several methods to deliver software to client computers. The method that you use to create the task or policy depends on your delivery requirements. See "Methods for delivering software" on page 88.
Software Portal	The **Software Portal** is a Web-based interface that is installed on the client computers. With the **Software Portal**, users can request and install software with little or no administrator involvement. See "About the Software Portal" on page 161.

Table 1-1   Components of Software Management Solution *(continued)*

Component	Description
Tasks and policies for managing Windows Installer applications	You can manage Windows Installer applications as follows: ■ Repair broken Windows Installer applications. ■ Update the source paths for Windows Installer applications. See "About managing Windows Installer applications" on page 192.
Tasks for managing virtual applications	You can use software virtualization to facilitate the management of most Windows-based software on managed computers. Software virtualization lets you avoid conflicts between applications. It also lets you quickly restore a broken application to its original installed state. See "Managing virtual applications" on page 217.
Reports	Predefined reports let you easily view and analyze your software management data. You can also create your own custom reports. See "About Software Management Solution reports" on page 82.
Wise Toolkit	Wise Toolkit provides the tools that let administrators create, customize, and manage installations. Wise Toolkit consists of the following tools: ■ Wise InstallTailor ■ WiseScript for NS See "About Wise Toolkit" on page 49.

See "What you can do with Software Management Solution" on page 15.

What you can do with Software Management Solution

Software Management Solution lets you distribute and manage the software that is used in your organization.

See "About Software Management Solution" on page 13.

Table 1-2   What you can do with Software Management Solution

Task	Description
Configure the default settings for Managed Software Delivery policies.	Configuration settings control the behavior of Managed Software Delivery policies. Rather than configuring these settings individually for each policy, you can configure the default settings that apply to all new Managed Software Delivery policies. Then you can change the settings for a specific policy only when needed. See "About Software Management Solution settings" on page 54. See "Configuring the default settings for Managed Software Delivery" on page 54.
Perform an advanced software delivery.	Managed Software Delivery simplifies your advanced software deliveries by letting you deliver software as a unit, which can include multiple software resources and their dependencies. For example, you can create a single Managed Software Delivery policy that installs an application and its associated patches and service packs. Managed Software Delivery can also run any task at any stage of the delivery. See "About advanced software deliveries" on page 96. See "Performing an advanced software delivery" on page 104.
Perform a quick delivery of a single software resource.	You can perform a quick delivery of a single software resource that runs with minimum configuration. You can use the task-based Quick Delivery method to specify the software to deliver, the action to perform, and the computers to deliver to. Because the software resources and the delivery settings are predefined, Quick Delivery makes it easy for administrators and non-administrators to deliver software. See "About quick delivery of a single software resource" on page 131. See "Performing a quick delivery of a single software resource" on page 132.
Deliver a package without defining a software resource.	Package Delivery lets you quickly push out any package regardless of whether it is associated with a software resource. See "About Package Delivery" on page 137. See "Delivering a package without defining a software resource" on page 138.
Deliver the tasks and packages that were created in Altiris Software Delivery Solution 6.x.	When you upgrade from Notification Server 6.x to Symantec Management Platform 7.0, you can migrate your software-related tasks and packages. See "How 6.x features compare to Software Management Solution 7.0" on page 17. For more information about 6.x data migration, see the *Symantec Management Platform Release Notes*.
Deliver software to fulfill user requests.	By using the **Software Portal**, users can request and install software through a Web-based interface with little or no administrator involvement. See "About the Software Portal" on page 161.

Table 1-2   What you can do with Software Management Solution *(continued)*

Task	Description
Manage Windows Installer installations on client computers.	You can create policies and tasks to manage Windows Installer applications on managed computers as follows:
	■ Repair Windows Installer applications. You can proactively identify and repair broken applications on selected computers. If an application needs repair, a repair command is sent to the Windows Installer service to initiate self-repair. See "Repairing Windows Installer applications" on page 194. ■ Update the source paths for Windows Installer applications. You can update the source paths of Windows Installer applications with resilient source paths. The updated source paths point to the package servers that you designate. If an application needs modification or repair, Windows Installer can access the needed installation file from one of these servers. See "Updating the source paths of Windows Installer applications" on page 199. See "About managing Windows Installer applications" on page 192.
Manage virtual applications.	You can use software virtualization to facilitate the management of most Windows-based software on managed computers. Software virtualization lets you avoid conflicts between applications and quickly restore a broken application to its original installed state.
	Software Management Solution lets you perform the following virtualization actions:
	■ Virtualize applications during a Managed Software Delivery installation. ■ Deliver and install virtual layers with any Software Management Solution delivery policy or task. ■ Manage the existing virtual layers on the client computers. See "Managing virtual applications" on page 217.

How 6.x features compare to Software Management Solution 7.0

Software Management Solution 7.0 replaces the 6.x versions of Software Delivery Solution and Application Management Solution as well as some features of Software Virtualization Solution. Software Management Solution contains most of the functionality of those solutions as well as many new features and functions.

You can discover how to perform familiar 6.x tasks in Software Management Solution 7.0 by reviewing the comparisons between the features of the different versions.

Comparisons between the tasks in 6.x and the tasks in 7.0 are available as follows:

■ Implementation
See "Comparison of software agents and settings in versions 6.x and 7.0"
on page 18.

■ Software delivery
See "Comparison of software delivery in versions 6.x and 7.0" on page 19.

■ **Software Portal**
See "Comparison of Software Portal features in versions 6.x and 7.0"
on page 23.

■ Application management
See "Comparison of application management in versions 6.x and 7.0"
on page 25.

■ Software virtualization
See "Comparison of virtualized software delivery in versions 6.x and 7.0"
on page 27.

■ Wise Toolkit
See "Comparison of the Wise Toolkit in versions 6.x and 7.0" on page 29.

Comparison of software agents and settings in versions 6.x and 7.0

Software Management Solution 7.0 contains many of the delivery settings that
were available in earlier versions of Software Delivery Solution. However, you
can configure those settings as global defaults instead of re-entering them for
each new software delivery policy or task. The global defaults save time during
the creation of policies and tasks, and they help provide consistency in how your
software deliveries run.

Software Management Solution 7.0 requires a different set of agents than earlier
versions of Software Delivery Solution and Application Management Solution.

See "Implementing Software Management Solution" on page 34.

Table 1-3   Comparison of Software Management Solution agents and settings
                   in versions 6.x and 7.0

Task	Method in 6.x	Method in 7.0
Install agents on the client computer, in addition to the Altiris Agent.	Agent requirements are as follows: ■ Software Delivery agent ■ Task Synchronization agent ■ Software Delivery Task Server agent ■ State Management agent ■ Windows Installer agent	Agent and plug-in requirements are as follows: ■ Software Management Framework agent This agent is installed with the Altiris Agent. ■ Software Management Solution agent for Windows ■ Software Management Solution plug-in for UNIX, Linux, and Mac ■ **Software Portal** agent (Windows only) ■ Application Management agent (Windows only) See "About the agents and plug-ins that Software Management Solution uses" on page 37.
Configure settings for Software Delivery policies and tasks.	Configure the settings when you create each policy or task.	You can configure Managed Software Delivery settings as follows: ■ Configure the default settings that govern all new Managed Software Delivery policies. ■ Override the default settings when you create a Managed Software Delivery policy without the **Managed Software Delivery** wizard. ■ Override the default settings when you edit an existing Managed Software Delivery policy. See "Configuring the default settings for Managed Software Delivery" on page 54. Each type of task in Software Management Solution contains the default settings that control how it runs. You can override the default settings for specific tasks. See "Advanced options for tasks in Software Management Solution" on page 70.

See "How 6.x features compare to Software Management Solution 7.0" on page 17.

Comparison of software delivery in versions 6.x and 7.0

Software Management Solution 7.0 is completely new. With few exceptions, you can perform all the software delivery actions that were available in earlier versions of Software Delivery Solution. However, Software Management Solution provides the additional features and functions that provide more reliable management of your software before, during, and after delivery.

See "About software delivery" on page 87.

In versions earlier than 7.0, the delivery of non-Windows software required the separate installation of Software Delivery Solution for UNIX, Linux, and Mac. Software Management Solution 7.0 combines support for Windows software and non-Windows software in one product.

Table 1-4   Comparison of software delivery in versions 6.x and 7.0

Task	Method in 6.x	Method in 7.0
Deliver software or push out a package.	Create a Software Delivery task in Software Delivery Solution or create a Deliver Software task in Altiris Task Server.	Depending on the complexity of your requirements, create a task or policy as follows: ■ Create a Quick Delivery task to deliver a single software resource. See "Performing a quick delivery of a single software resource" on page 132. ■ Create a Managed Software Delivery policy to fulfill advanced delivery requirements. See "Advanced delivery actions that Managed Software Delivery can perform" on page 97. ■ Create a Package Delivery task to push out a package that is not associated with a software resource. This feature replaces the functionality of the Software Delivery Task Server plug-in. See "Delivering a package without defining a software resource" on page 138. You can also migrate 6.x tasks to the following 7.0 policies and tasks: ■ You can migrate Software Delivery tasks to Legacy Software Delivery policies. We recommend that you use these policies only if you cannot deliver the packages with one of the new delivery methods. We recommend that you use Legacy Software Delivery policies only for 6.x packages that you cannot deliver with Quick Delivery or Managed Software Delivery. See "About Legacy Software Delivery" on page 149. ■ You can migrate Software Delivery Task Server Plug-in tasks to Package Delivery tasks.

Table 1-4   Comparison of software delivery in versions 6.x and 7.0 *(continued)*

Task	Method in 6.x	Method in 7.0
Deliver multiple software packages in sequence.	Create a sequential Software Delivery task on the **Software Delivery Task** page.	Create a Managed Software Delivery policy that contains multiple software resources and tasks. You can also migrate 6.x Sequential Software Delivery tasks to Managed Delivery policies. See "Delivering multiple software resources and tasks sequentially" on page 126.
Deliver software to a UNIX, Linux, or Mac client computer.	Create a Software Delivery task in Software Delivery Solution for UNIX, Linux, and Mac.	Use Quick Delivery, Managed Software Delivery, or Package Delivery as appropriate. Software Management Solution uses the same interfaces for these operating systems as for Windows. See "Methods for delivering software" on page 88. You can also migrate 6.x Software Delivery tasks to Legacy Software Delivery policies. We recommend that you use Legacy Software Delivery policies only for 6.x packages that you cannot deliver with Quick Delivery or Managed Software Delivery. See "About Legacy Software Delivery" on page 149.
Deliver software to a handheld device.	Create a Software Delivery task in Software Delivery Solution for Pocket PC.	Handheld devices are not supported in Software Management Solution 7.0.
Uninstall software from a client computer.	Depending on how the software was installed, uninstall it as follows: ■ Clone a software delivery task for that software and add the uninstall switch to the command line. ■ Create a new task with a package and program to uninstall the software.	The functions are similar to those in 6.x. Depending on how the software was installed, uninstall it as follows: ■ If the software to be uninstalled was installed with a Software Management Solution task or policy, clone the original installation task or policy. Then edit the clone to select an uninstall command line. ■ Create a new Software Management Solution task or policy for the software resource and select an uninstall command line. You can use any of the methods for delivering software. See "Methods for uninstalling software" on page 91.

Table 1-4   Comparison of software delivery in versions 6.x and 7.0 *(continued)*

Task	Method in 6.x	Method in 7.0
Define the packages and command lines that install software.	Define a package in one of the following locations: ■ On the **Software Resources** tab in the **Altiris Console** ■ In the **Software Delivery** wizard Define a program (command line) in the **Software Programs** dialog box, on the **Programs** tab.	Create or edit a software resource in the Software Catalog, associate it with one or more packages, and create one or more command lines. The Command Line Builder can help you create the command lines. The Software Catalog is part of the Symantec Management Platform. For more information, see the topics about creating software resources and command lines in the *Symantec Management Platform Help*. You can also migrate 6.x packages and command lines for both Windows and non-Windows software to 7.0 packages and command lines. Before you can deliver a migrated package with Managed Software Delivery or Quick Delivery, assign the package to a software resource in the Software Catalog. For more information about 6.x data migration, see the *Symantec Management Platform Release Notes.*
Verify that a task or policy was successfully delivered to a managed computer.	Status events are sent to the server for server-side reporting. Details are saved locally on the computer, where you can view them in the Altiris Agent user interface.	You can obtain status and other information about Software Management Solution tasks, policies, and other actions from several sources. Each source provides a different type or format of information depending on your needs. Many of the sources for Software Management status information are the same as in earlier versions. The way that you access those sources might be different. See "Sources of status information in Software Management Solution" on page 79.
Purge software delivery data.	Configure settings on the Software Delivery **Data Purging** page.	Specify the retention period for specific data classes on the **Purging Maintenance** page that appears in the settings for **Notification Server**. See "Options for purging Software Management Solution data" on page 72.

See "How 6.x features compare to Software Management Solution 7.0" on page 17.

Comparison of Software Portal features in versions 6.x and 7.0

Software Management Solution 7.0 contains the features that were available in earlier versions of the **Software Portal**. The **Software Portal** is redesigned on both the server side and the client side to increase its flexibility and ease of use.

See "About the Software Portal" on page 161.

Table 1-5   Comparison of **Software Portal** features in 6.x and 7.0

Task	Method in 6.x	Method in 7.0
Configure the **Software Portal**.	Complete the **Software Portal Settings** page and the **User Preferences** tab. Categorize software requests by using the **Publisher** option in the package **Properties**.	Complete the **Software Portal Settings** page and the **Software Portal Agent Installation** page. See "Configuring the Software Portal settings" on page 181. See "Installing the Software Portal agent" on page 46.
Configure permissions for the **Software Portal**.	Options are as follows: ■ Set options on the **Software Portal** tab on the software package resource page. ■ Use the **Software Portal Configuration** page to assign, remove, or configure permissions on one or more portal items at a time. ■ For sequential tasks, set options on the **Software Portal** tab on the **Sequential Task** page.	Set the following types of permissions: ■ Configure security roles for the administrators and managers who need to use the **Software Portal**. See "Recommended security settings for the Software Portal" on page 175. ■ When you publish each software resource to the **Software Portal**, define the users who can request and install that software. See "Methods for adding software to the Software Portal" on page 176.

	Table 1-5	Comparison of **Software Portal** features in 6.x and 7.0 *(continued)*
Task	**Method in 6.x**	**Method in 7.0**
Add software to the **Software Portal**.	Use the **Software Portal** tab on the **Software Package** page to manage the availability of software that a user can add manually. You can also use the **Software Portal** tab on the **Sequential Task** page.	Options for adding software to the **Software Portal** are as follows: ■ Add (publish) a software resource to the **Software Portal** to deliver a single piece of software with minimum configuration. When you publish a software resource, a Quick Delivery task is created. ■ Publish a Managed Software Delivery policy to the **Software Portal** to deliver one or more software resources with complex delivery requirements. See "Methods for adding software to the Software Portal" on page 176.
Request software from the **Software Portal** on the client computer.	The user opens the **Software Portal** from any of the following locations: ■ From a URL ■ On the **Start** menu ■ On the Altiris Agent's context menu.	The user opens the **Software Portal** from any of the following shortcuts: ■ On the Desktop ■ On the **Start** menu ■ On the Altiris Agent's context menu. New functionality is also provided. For example, the user can add comments to software requests and cancel software requests.
Approve a user's software request.	Administrators can use Alert Manager or Helpdesk Solution to retrieve software requests, approve them, deny them, and send email notifications. The software requests that require approval are added to the Asset Management queue. The administrator uses the **Software Portal** wizard to process the requests.	Approvers of software requests are as follows: ■ Administrator, Software Catalog The Software Catalog administrator can pre-approve software when the software is published to the **Software Portal** from the Software Catalog. ■ Administrator, **Software Portal** The **Software Portal** administrator can approve requests on the **Administrator Portal** page, which appears in the **Symantec Management Console**. ■ Manager A manager can approve requests from the **Manager Portal** page, which appears in the **Software Portal** on the client computer. See "About the approval of software requests" on page 165.

See "How 6.x features compare to Software Management Solution 7.0" on page 17.

Comparison of application management in versions 6.x and 7.0

(Windows only)

In Software Management Solution 7.0, you can use several of the application management features that were available in earlier versions of Application Management Solution.

See "About managing Windows Installer applications" on page 192.

Table 1-6   Comparison of application management in versions 6.x and 7.0

Task	Method in 6.x	Method in 7.0
Evaluate and maintain the correct state of the software on a client computer.	Use package management tasks and state management tasks. The package management tasks can be created either automatically with the Wise Integration Component and package rule templates, or manually.	Create a Managed Software Delivery policy for the software that you plan to check and define a recurring schedule. The Managed Software Delivery policy installs the software to a specific known state on the client computer. On a recurring basis, the policy performs a compliance check to verify that the state is maintained. If the state of the software is out of compliance, Managed Software Delivery performs a remediation to restore the correct state. See "About policy applicability, compliance, and remediation" on page 102. See "Performing an advanced software delivery" on page 104.
Repair Windows Installer applications.	Scan a computer with a Windows Installer scan policy and repair broken applications with a Windows Installer repair policy.	Options for repairing Windows Installer applications are as follows: ■ Create a Managed Software Delivery policy with a recurring schedule. Managed Software Delivery gives you more control over the scanning and remediation than other methods. The software resource's detection rule lets you define how to accurately identify the software on the client computer. When you schedule the policy, you can select when to perform the remediation. See "Performing an advanced software delivery" on page 104. ■ Create a Windows Installer Repair policy or task. The policy or task scans the computer for broken applications. If an application needs repair, the same policy or task sends a repair command to the Windows Installer service to initiate self-repair. See "Repairing Windows Installer applications" on page 194.

Table 1-6   Comparison of application management in versions 6.x and 7.0
(continued)

Task	Method in 6.x	Method in 7.0
Create the rules that evaluate whether a package is installed properly on a collection of computers.	Create package rule templates in Package Rule Management.	Create inventory rules and associate them with specific software resources in the Software Catalog. Inventory rules can determine whether a client computer has the correct environment for an installation of the software or whether it has specific software installed. The Software Catalog is part of the Symantec Management Platform. For more information, see the topics about creating and editing inventory rules in the *Symantec Management Platform Help*. See "About policy applicability, compliance, and remediation" on page 102.
Manage source paths for Windows Installer applications.	Scan computers with a Windows Installer scan policy. Use the **Windows Installer Source Path** wizard to create a program and policy to change the installation source path.	Configure a Source Path Update policy or create a Source Path Update task. See "Updating the source paths of Windows Installer applications" on page 199.
Compare files and registry keys between different client computers and track how computers change over time.	Generate a baseline that identifies the files or registry settings on a computer and then run compliance scans.	The baseline inventory feature in Application Management Solution 6.x is now part of Inventory Solution 7.0. For more information, see the topics about baseline inventory in the *Inventory Solution Help*.
Customize how the Windows Installer agent runs.	Change the configuration INI file that the agent reads at startup, or edit command-line options for the programs that run the agent.	The Application Management agent replaces the Windows Installer agent. You customize the Application Management agent by opening its software resource in the Software Catalog and modifying its command line. The ability to edit a software resource is available in Software Management Framework, which is part of the Symantec Management Platform. For more information, see the topics about command lines in the *Symantec Management Platform Help*.

Table 1-6   Comparison of application management in versions 6.x and 7.0
(continued)

Task	Method in 6.x	Method in 7.0
Evaluate the state of software on managed computers.	The State Management agent evaluates the state of packages on managed computers by using the rules that are specified in state or package management tasks.	The Software Management Framework agent and the Software Management Solution agent evaluate the state of the managed computers. The agents use the rules that are associated with a software resource. See "About the agents and plug-ins that Software Management Solution uses" on page 37.

Comparison of virtualized software delivery in versions 6.x and 7.0

(Windows only)

In Software Management Solution 7.0, you can use several of the software virtualization features that were available in earlier versions of Software Virtualization Solution.

The managed computers on which you plan to use software virtualization must have the Software Virtualization agent installed. The Software Catalog contains a software resource for the Software Virtualization agent, which you can install with any delivery method.

Table 1-7   Comparison of virtualized software delivery in versions 6.x and 7.0

Task	Method in 6.x	Method in 7.0
Virtualize software.	Capture an application and its data into a virtual software package by using any of the capture tools in Software Virtualization Solution. Export the layer to a virtual software archive (VSA) file.	Create a Managed Software Delivery policy to deliver the software. In the policy, select the option to install the software into a virtual layer. This feature eliminates the need to repackage the application into a VSA package. It also lets you retain all the logic that is built in to the original MSI file. See "Virtualizing software during installation" on page 220.

Table 1-7   Comparison of virtualized software delivery in versions 6.x and 7.0 *(continued)*

Task	Method in 6.x	Method in 7.0
Deliver an existing VSA file and import it into a virtual software layer on a client computer.	Options are as follows: ■ Create a Virtual Software task and specify a VSA package. ■ Create an SVS Command task and use the Import layer command.	Deliver and install an existing VSA package as you would any other software package. Create a Software Virtualization task, a Quick Delivery task, a Package Delivery task, or a Managed Software Delivery policy and specify a VSA software resource. See "Methods for delivering software" on page 88. You can also migrate 6.x virtualization data to the following 7.0 tasks and packages: ■ You can migrate 6.x SVS Task Server Plug-in tasks to Software Virtualization tasks. See "Installing and managing a virtual software layer with a Software Virtualization task" on page 225. ■ You can migrate 6.x virtual software packages to 7.0 packages. Before you can deliver a migrated package with Managed Software Delivery, assign the package to a software resource in the Software Catalog. For more information about 6.x data migration, see the *Symantec Management Platform Release Notes*.
Manage virtual software layers on a client computer.	Options are as follows: ■ Create a Virtual Software task. ■ Create an SVS Command task, which requires the SVS Task Server plug-in. ■ Use the SVS User Admin utility to trigger SVS actions from user or group logon and logoff events.	Create any of the following tasks or policies: ■ Software Virtualization task Manages any virtual software layer regardless of how it was created. ■ Quick Delivery task or Package Delivery task Manages only the virtual software layers that were created by importing a VSA file. ■ Managed Software Delivery policy Manages multiple virtual software layers at the same time. See "Methods for installing and managing virtual software" on page 221. You can also migrate 6.x SVS Task Server Plug-in tasks to Software Virtualization tasks.

Comparison of the Wise Toolkit in versions 6.x and 7.0

Software Management Solution 7.0 contains the Wise Toolkit tools that were available in earlier versions of Software Delivery. The Wise Toolkit tools work the same as before, except that you install and access them differently.

Table 1-8   Comparison of the Wise Toolkit in versions 6.x and 7.0

Task	Method in 6.x	Method in 7.0
Install Wise Toolkit	Each tool is installed the first time that you start it.	Use any delivery method in Software Management Solution to install the appropriate software resource. See "Installing the Wise Toolkit tools" on page 50.
Start the tools	On the computer where you installed the tool, start the tool from one of the following locations: ■ On the **Task** view in the **Altiris Console** ■ On the **Start** menu	On the computer where you installed the tool, select it from the **Start** menu.

See "How 6.x features compare to Software Management Solution 7.0" on page 17.

Where to get more information

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

Table 1-9   Documentation resources

Document	Description	Location
Release Notes	Information about new features and important issues. This information is available as an article in the Altiris knowledge base.	http://kb.altiris.com/ You can search for the product name under Release Notes.

Table 1-9 Documentation resources *(continued)*

Document	Description	Location
User's Guide	Information about how to use this product, including detailed technical information and instructions for performing common tasks. This information is available in PDF format.	■ The Documentation Library, which is available in the **Symantec Management Console** on the **Help** menu. ■ The **Product Support** page, which is available at the following URL: http://www.symantec.com/business /support/all_products.jsp When you open your product's support page, look for the **Documentation** link on the right side of the page.
Help	Information about how to use this product, including detailed technical information and instructions for performing common tasks. Help is available at the solution level and at the suite level. This information is available in HTML help format.	The Documentation Library, which is available in the **Symantec Management Console** on the **Help** menu. Context-sensitive help is available for most screens in the Symantec Management Console. You can open context-sensitive help in the following ways: ■ The F1 key ■ 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 1-10 Altiris information resources

Resource	Description	Location
Knowledge base	Articles, incidents, and issues about Altiris products.	http://kb.altiris.com/
Symantec Connect (formerly Altiris Juice)	An online magazine that contains best practices, tips, tricks, forums, and articles for users of this product.	http://www.symantec.com/connect /endpoint-management-virtualization

Section 1

Setting up Software Management Solution

Implementing Software Management Solution

This chapter includes the following topics:

- Implementing Software Management Solution

- About the Software Management Solution installation

- About the agents and plug-ins that Software Management Solution uses

- Installing the Software Management Solution agent

- Extra schedule options section

- Installing the Software Management Solution plug-in for UNIX, Linux, and Mac

- Recommended security privileges for Software Management Solution

- Options for installing the Software Portal agent

- Installing the Software Portal agent

- Installing the Software Virtualization agent

- Web parts for Software Management Solution

- About Wise Toolkit

- Installing the Wise Toolkit tools

Implementing Software Management Solution

Before you use Software Management Solution, you must set it up and prepare it for use.

See "About Software Management Solution" on page 13.

The prerequisites for implementing Software Management Solution are as follows:

- Symantec Management Platform and Software Management Solution must be installed on the Notification Server computer.
  For more information, see the *Symantec Management Platform Installation Guide.*

- The Altiris Agent must be installed on the computers that you plan to manage. Software Management Solution requires that target computers be managed. A managed computer is one on which the Altiris Agent is installed.
  For more information, see the topics about installing the Altiris Agent in the *Symantec Management Platform Help*.

- The Altiris Agent for UNIX, Linux, and Mac must be installed on the non-Windows computers that you plan to manage.
  For more information, see the topics about installing the Altiris Agent for UNIX, Linux, and Mac in the *Symantec Management Platform Help*.

Table 2-1   Process for implementing Software Management Solution

Step	Action	Description
Step 1	Install the Software Management Solution agents and plug-ins on managed computers.	The Software Management Solution agents and plug-ins are required for you to deliver and manage software on client computers.
		Perform this step every time that you need to install the Software Management Solution agent on the client computers that do not have it.
		The agent or plug-in that you install depends on the operating systems that you support in your organization as follows:
		■ Software Management Solution agent for Windows See "Installing the Software Management Solution agent" on page 38. ■ Software Management Solution plug-in for UNIX, Linux, and Mac This plug-in also provides support for the AIX, HP-UX, and Solaris operating systems. See "Installing the Software Management Solution plug-in for UNIX, Linux, and Mac" on page 41.
		You may have performed this step when you installed the Symantec Management Platform or when you added new computers to the network.
		The installation of the Software Management Solution agent contains the options that let you install the **Software Portal** agent at the same time.
		See "Options for installing the Software Portal agent" on page 45.
Step 2	Configure security privileges for Software Management Solution.	Administrators need the appropriate privileges to deliver and manage the software in your organization.
		See "Recommended security privileges for Software Management Solution" on page 43.
		You or another administrator may have already performed this step when you configured security for the Symantec Management Platform.
		For more information, see the topics about setting up security and Software Management Solution settings in the *Symantec Management Platform Help*.

Table 2-1   Process for implementing Software Management Solution
                   (continued)

Step	Action	Description
Step 3	Configure default settings for Managed Software Delivery.	You can configure the settings that control the behavior of Managed Software Delivery policies. Rather than configuring these settings individually for each policy, you can configure the default settings that apply to all new Managed Software Delivery policies. See "Configuring the default settings for Managed Software Delivery" on page 54.
Step 4	(Optional) Implement the **Software Portal**.	The **Software Portal** is installed on the Notification Server computer when Software Management Solution is installed. If you plan to use the **Software Portal**, you must perform additional implementation steps. See "Implementing the Software Portal" on page 173.
Step 5	(Optional) Install the Software Virtualization agent.	If you plan to use software virtualization to manage Windows-based software on client computers, install the Software Virtualization agent on those computers. See "Installing the Software Virtualization agent" on page 47.
Step 6	(Optional) Install Wise Toolkit.	Wise Toolkit provides the tools that let administrators create, customize, and manage installations. See "Installing the Wise Toolkit tools" on page 50.

About the Software Management Solution installation

Software Management Solution is installed from Symantec Installation Manager.

The Symantec Installation Manager (SIM) handles the installation and initial configuration of the Symantec Management Platform. This easy-to-use installation wizard verifies installation readiness and steps you through the product installation and configuration.

If you need to install or uninstall Software Management Solution after the initial platform installation, Symantec Installation Manager is available in the **Symantec Management Console**.

For more information, see the *Symantec Management Platform Installation Guide*.

About the agents and plug-ins that Software Management Solution uses

Certain agents and plug-ins must be installed on the client computers to manage and run the Software Management Solution functions.

Predefined tasks are provided to install these agents and plug-ins. Each predefined task installs one or more software resources that comprise the agents. For example, you can include the Software Portal agent with the installation of the Software Management Solution agent. When you do so, the predefined task installs the software resources for both agents.

Table 2-2   Agents and plug-ins that Software Management Solution uses

Agent or plug-in	Description
Software Management Framework agent	Manages all the software delivery functions in Software Management Solution.
	Software deliveries are closely integrated with the software resources in the Software Catalog. The Software Management Framework agent manages the package downloads and other aspects of software delivery.
	The Software Management Framework agent is installed on the client computers when the Altiris Agent is installed.
	For more information, see the topics about the Software Management Framework agent in the *Symantec Management Platform Help*.
Software Management Solution agent for Windows	Helps to provide support for software delivery, software management, and software virtualization on Windows computers. Optionally, this agent can also install the **Software Portal** agent on client computers.
	The software resource that comprises this agent is named Software Management Solution Agent.
	See "Installing the Software Management Solution agent" on page 38.

Table 2-2	Agents and plug-ins that Software Management Solution uses *(continued)*

Agent or plug-in	Description
Software Management Solution Plug-in for UNIX, Linux, and Mac	Provides the ability to deliver software and manage software on non-Windows computers and to support the **Software Portal** on Mac computers.
	This plug-in also provides support for the AIX, HP-UX, and Solaris operating systems.
	The softeware resources that comprise this agent are as follows:
	■ Software Management Solution Plug-in for AIX ■ Software Management Solution Plug-in for HP-UX ■ Software Management Solution Plug-in for Linux ■ Software Management Solution Plug-in for Mac ■ Software Management Solution Plug-in for Solaris
	See "Installing the Software Management Solution plug-in for UNIX, Linux, and Mac" on page 41.
Software Portal agent	Enables the **Software Portal** Web application on Windows-based client computers. It configures the URL that the users use to access the **Software Portal**. The agent also installs shortcuts to the **Software Portal** interface on the client computers.
	The software resource that comprises this agent is named Software Portal Agent.
	See "Installing the Software Portal agent" on page 46.
Application Management agent	Manages the policies and the tasks that perform Windows Installer repairs or source path updates on Windows computers.
	The software resource that comprises this agent is named Application Management Agent.
	See "About the Application Management agent" on page 203.
Software Virtualization agent	Lets you use software virtualization to manage Windows-based software on client computers.
	The software resource that comprises this agent is named Software Virtualization Agent.
	See "Installing the Software Virtualization agent" on page 47.

Installing the Software Management Solution agent

(Windows only)

Before you use Software Management Solution to deliver or manage software on managed computers, you must install the Software Management Solution agent on those computers.

See "About the agents and plug-ins that Software Management Solution uses" on page 37.

This task is a step in the process for implementing Software Management Solution.

See "Implementing Software Management Solution" on page 34.

If you plan to use the **Software Portal** too, you can install the **Software Portal** when you install the Software Management Solution agent.

See "Options for installing the Software Portal agent" on page 45.

You can also install a Software Management Solution agent for non-Windows computers.

See "Installing the Software Management Solution plug-in for UNIX, Linux, and Mac" on page 41.

To install the Software Management Solution agent

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

2   In the left pane, under **Agents/Plug-ins**, click **Software > Software Management > Windows > Software Management Solution Agent for Windows - Install**.

3   In the right pane, in the **Program name** drop-down list, select the command line for the type of installation to perform.

    To include the **Software Portal** agent in this installation, select one of the command lines that installs the **Software Portal**.

4   Check or uncheck **Enable Verbose Reporting of Status Events** as appropriate.

    This option records the detailed events that are related to the installation and posts them to the Notification Server computer.

5   Under **Applied to**, select where to install the agent.

    For more information, see the topics about specifying the targets of a policy or task in the *Symantec Management Platform Help*.

6   Under **Schedule**, set the schedule for the policy.

    For more information, see the topics about specifying a policy schedule in the *Symantec Management Platform Help*.

    Alternatively, under **Extra schedule options**, you can check **Run once ASAP** to run the policy as soon as possible.

7   Under **Extra schedule options**, click any of the following options:

    ■   **User can run**

- ■ **Notify user when the task is available**

- ■ **Warn before running, can defer for**

See "Extra schedule options section" on page 40.

8 Turn on the policy.

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

9 Click **Save changes**.

Extra schedule options section

This section appears under the **Schedule** section on the **Software Management Solution agent** page and in Legacy Software Delivery policies. It might also appear in other areas of the **Symantec Management Console**.

See "Installing the Software Management Solution agent" on page 38.

See "Delivering software packages with the same configurations as 6.x Software Delivery tasks" on page 150.

Table 2-3   Options in the **Extra schedule options** section

Option	Description
Run once ASAP	Lets you run the policy as soon as possible.
User can run	Lets the user choose when to run the policy by clicking the policy in the Altiris Agent. The user can also choose not to run the policy.
Notify user when the task is available	Displays a message to notify the user that new software is available. When the user clicks the message, the **New Software is Available** dialog box opens. The user can start, dismiss, or defer the policy. If you do not choose to prompt the user, the **New Software is Available** dialog box does not appear.

The **New Software is Available** dialog box appears only if the **Show popup notifications** check box is checked on the client computer's Altiris Agent. |

Table 2-3   Options in the **Extra schedule options** section *(continued)*

Option	Description
Warn before running	Notifies the user before the policy runs by displaying the **Starting Task** dialog box. When you check this check box an additional box appears, in which you type the number of minutes to let the user defer the policy.
	Unless you let the user defer the policy, the policy starts 60 seconds after the **Starting Task** dialog box appears. A progress bar shows the amount of time that remains. The user can dismiss the **Starting Task** dialog box but cannot cancel the policy unless you selected **User can run**.
	The **Starting Task** dialog box appears only if the **Show popup notifications** check box is checked on the client computer's Altiris Agent.

Installing the Software Management Solution plug-in for UNIX, Linux, and Mac

If you plan to deliver software to non-Windows client computers, install the Software Management Solution Plug-in for UNIX, Linux, and Mac on those computers.This plug-in also provides support for the AIX, HP-UX, and Solaris operating systems.

See "About the agents and plug-ins that Software Management Solution uses" on page 37.

The Software Management Solution Plug-in for UNIX, Linux, and Mac supports the **Software Portal** on the Mac operating system. A separate **Software Portal** agent or plug-in is not provided for non-Windows computers.

Note: If the **Altiris Agent** window is open on the client computer when this plug-in is installed, the **Software Portal** link does not appear. To prevent this issue, restart the Altiris Agent on the client computer after the plug-in is installed. After the Altiris Agent restarts, the **Software Portal** link becomes available to the user.

This task is a step in the process for implementing Software Management Solution.

See "Implementing Software Management Solution" on page 34.

You can also install a Software Management Solution agent for Windows computers.

See "Installing the Software Management Solution agent" on page 38.

To install the Software Management Solution Plug-in for UNIX, Linux, and Mac

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

2   In the left pane, under **Agents/Plug-ins**, click **Software > Software
    Management > UNIX/Linux/Mac > Software Management Solution Plug-in
    for UNIX/Linux/Mac Install**.

3   In the right pane, in the **Program name** drop-down list, accept the default
    option to install the plug-in.

4   Check or uncheck **Enable Verbose Reporting of Status Events** as appropriate.

    This option records the detailed events that are related to the installation
    and posts them to the Notification Server computer.

5   Under the **Applied to** section, select where to install the agent and specify
    whether to disable multicasting.

    For more information, see the topics about specifying the targets of a policy
    or task in the *Symantec Management Platform Help*.

6   Under the **Schedule** section, set the schedule for the policy.

    For more information, see the topics about specifying a policy schedule in
    the *Symantec Management Platform Help*.

    Alternatively, under the **Extra schedule options** section, you can check **Run
    once ASAP** to run the policy as soon as possible.

7   Under the **Extra schedule options** section, select any of the following options:

User can run	Lets the user run the policy by clicking the policy in the Altiris Agent. The user can also choose not to run the policy.
Notify user when the task is available	This option does not apply to UNIX, Linux, or Mac OS.
Warn before running	This option does not apply to UNIX, Linux, or Mac OS.

8   Turn on the policy.

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

9   Click **Save changes**.

Recommended security privileges for Software Management Solution

As part of the Software Management Solution implementation, you configure security privileges for the users who need to deliver and manage software on client computers.

See "Implementing Software Management Solution" on page 34.

You configure security for Software Management Solution in the **Symantec Management Console**, on the **Security Roles** settings page, on the **Privileges** tab. Most users require other privileges in addition to the Software Management-related privileges. For example, to run a Quick Delivery task, a user must have right-click menu privileges for Quick Delivery and for scheduling a task.

For more information, see the topics on setting up security, security roles, and security role privilege settings in the *Symantec Management Platform Help*.

We provide security recommendations for two levels of software administrators and one level of non-administrators. You can adapt these recommendations to the size of your software management team.

Table 2-4 Recommended security privileges for Software Management Solution

Type of user	Recommended privileges
Senior software administrators	Senior administrators are responsible for the more critical software management tasks, such as performing complex deliveries. They might also manage the Software Catalog and the Software Library, which means that they can create and manage your organization's software resources and packages. ■ **Right Click Menu - Actions** Software administrators need the privileges that are specific to Software Management Solution as follows: 　■ **Configure Managed Delivery Options** 　■ **Managed Software Delivery** 　■ **Quick Delivery Task** 　■ **Source Path Update** ■ **Right Click Menu - Actions** Senior administrators might need to create and edit software resources, even if they are not responsible for managing the Software Catalog or the Software Library. Therefore, they need some of the Software Management Framework-related privileges. Examples are as follows: 　■ **Edit Command Line** 　■ **Edit Software Resource** 　■ **Edit Package** 　■ **Import Package** For more information, see the topics about right-click menu privileges in the *Symantec Management Platform Help*. ■ **Software Portal Privileges** See "Recommended security settings for the Software Portal" on page 175.
Software administrators	These administrators perform the majority of the software delivery tasks in your organization. ■ **Right Click Menu - Actions** Software administrators need the privileges that are specific to Software Management Solution as follows: 　■ (Optional) **Configure Managed Delivery Options** 　　You might provide this privilege depending on the administrator's level. 　■ **Managed Software Delivery** 　■ **Quick Delivery Task** 　■ **Source Path Update** ■ **Software Portal Privileges** See "Recommended security settings for the Software Portal" on page 175.

Recommended security privileges for Software Management Solution
(continued)

Type of user	Recommended privileges
Non-administrators who can deliver software	You might let non-administrators perform single, routine software deliveries so you can free your software administrators to focus on more complex delivery tasks. For example, help desk employees can deliver a software update without escalating the requirement to the administrators. **Right Click Menu - Actions** ■ **Managed Software Delivery** Typically, these employees do not need to create Managed Software Delivery policies, but you might decide to let them run the policies to deliver software. ■ **Quick Delivery Task**

Options for installing the Software Portal agent

(Windows only)

The Software Portal agent provides access to the **Software Portal** Web application from the client computer and installs shortcuts to the Software Portal interface. If you plan to use the **Software Portal**, you must install the Software Portal agent on the Windows client computers.

You can skip this step for Mac client computers. The Software Management Solution plug-in for UNIX, Linux, and Mac supports the **Software Portal** on the Mac operating system.

Your options for installing the Software Portal agent are as follows:

Include the Software Portal agent with the installation of the Software Management Solution agent.	When you install the Software Management Solution agent, you can run a program (command line) that installs the Software Portal agent at the same time. This method is more convenient but it provides less control over the Software Portal agent's installation. The results of using this method are as follows: ■ Reduces the number of agent rollouts that you need to perform. ■ Installs the Software Portal agent on all computers that get the Software Management Solution agent. ■ Places the **Software Portal**'s shortcuts in all possible locations on the client computers: The Desktop, the **Start** menu, and the Altiris Agent's context menu. See "Installing the Software Management Solution agent" on page 38.
Install the Software Portal agent separately.	This method provides more control over the Software Portal agent's installation but it requires a separate operation. The results of using this method are as follows: ■ Lets you more specifically select which computers to install on. ■ Lets you select where to place the **Software Portal**'s shortcuts on the client computers. See "Installing the Software Portal agent" on page 46.

Installing the Software Portal agent

(Windows only)

The **Software Portal** agent provides access to the **Software Portal** Web application from the client computers. It configures the URL that the users use to access the **Software Portal**. The agent also installs shortcuts to the **Software Portal** interface on the client computers.

This task is a step in the process for implementing the **Software Portal**. Perform this task every time that you need to install the **Software Portal** on the client computers that do not have it.

You can skip this step for Mac client computers. The Software Management Solution plug-in for UNIX, Linux, or Mac supports the **Software Portal** on the Mac operating system.

See "Implementing the Software Portal" on page 173.

The **Software Portal** agent requires that the Software Management Solution agent is installed on the client computers. You can set options in the Software Management Solution agent's installation to install the **Software Portal** agent at the same time.

See "Installing the Software Management Solution agent" on page 38.

To install the Software Portal agent

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

2   In the left pane, under **Settings**, click **Software > Software Portal Settings > Software Portal Agent Settings > Software Portal Agent Installation**.

3   On the **Software Portal Agent Installation** page, under **Configure Links**, specify where to place the shortcut for the**Software Portal** on the client computers.

   Click one or more of the following options:

   ■   **Show link for Software Portal on Desktop**

   ■   **Show link for Software Portal in Start Menu**

   ■   **Show link for Software Portal in Altiris Agent's context menu**
       Places the **Altiris Agent** icon in the notification area on the client computer. The user can right-click the **Altiris Agent** icon to display the context menu and access the **Software Portal**.

4   Under **Select Destination**, select the computers or users on which to install the agent.

   For more information, see the topics about specifying the targets of a policy or task in the *Symantec Management Platform Help*.

5   Under **Apply Schedule**, define the schedule on which to install the agent.

   For more information, see the topics about specifying a policy schedule in the *Symantec Management Platform Help*.

6   Click **Save changes**.

Installing the Software Virtualization agent

(Windows only)

If you plan to use software virtualization to manage Windows-based software on client computers, install the Software Virtualization agent on those computers.

See "Managing virtual applications" on page 217.

By default, the Software Catalog contains a software resource for the Software Virtualization agent. You can use any delivery method to deliver the agent to client computers. You are licensed to deliver the Software Virtualization agent to as many nodes as you purchased for Software Management Solution.

As with any other software resource, when you install the Software Virtualization agent, you can use its default command lines or create your own.

For more information, see the topics about creating and editing command lines in the *Symantec Management Platform Help*.

The Software Virtualization agent requires that the Software Management Solution agent is installed on the client computers.

See "Installing the Software Management Solution agent" on page 38.

To install the Software Virtualization agent

◆ Create any type of software delivery policy or task and specify the software resource for the Software Virtualization agent.

See "Methods for delivering software" on page 88.

Web parts for Software Management Solution

Web parts are the building blocks for portal pages in the **Symantec Management Console**. Web parts are predefined for the products that you have installed. You can edit the predefined Web parts, and you can create new Web parts. Your user privileges determine which of the Web parts you can use and whether you can edit and add Web parts.

For more information, see the topics about portal pages and Web parts in the *Symantec Management Platform Help*.

Table 2-5   Web parts for Software Management Solution

Web part	Description
Open Software Request Status	Displays a pie chart that summarizes all the open requests that are in the **Software Portal** and groups them by status. It also shows the number of requests that are in each status group.
Recent Software Delivery Status	Lists all software deliveries and displays a green bar next to those that succeeded and a red bar next to those that failed. It includes the following delivery types: Managed Software Delivery, Quick Delivery, Package Delivery, and Legacy Software Delivery.

Table 2-5 Web parts for Software Management Solution *(continued)*

Web part	Description
Software Compliance Summary	Displays a pie chart that shows how many software installations are compliant and not compliant among those that were installed with Managed Software Delivery. This data is based on the most recent compliance checks that the currently-active Managed Software Delivery policies performed.
	A software installation is considered compliant when it is in the correct state on the client computers. For example, if the software is installed and it should be installed, it is compliant. If the software is installed but it should not be installed, it is not compliant.
Software Delivery History	Displays a graph that shows the number of deliveries that succeeded and failed among the deliveries that were attempted within the specified time period. It includes the following delivery types: Managed Software Delivery, Quick Delivery, Package Delivery, and Legacy Software Delivery.
Software Delivery Status	Displays a pie chart that shows the number of deliveries that succeeded and failed among all deliveries that were attempted. It includes the following delivery types: Managed Software Delivery, Quick Delivery, Package Delivery, and Legacy Software Delivery.
Software Portal Request Summary	Displays a pie chart that summarizes all the software requests that were placed through the **Software Portal** and groups them by status. It also shows the number of requests that are in each status group.

About Wise Toolkit

Wise Toolkit provides the tools that let administrators create, customize, and manage installations.

Wise Toolkit consists of the following tools:

Wise InstallTailor — Lets you easily customize Windows Installer installations. It simulates the installation, captures the options you select, and creates a transform file (MST) that incorporates those selections. At run time, you apply the transform to a Windows Installer package to customize the installation for a particular group of users.

WiseScript for NS	A WiseScript authoring environment that lets you create scripts to automate administrative tasks. WiseScript is a high-level scripting language in an easy-to-use, structured interface.
	Use a WiseScript to perform the tasks that you cannot easily perform with your other tools. A WiseScript can retrieve information about a computer, prompt for input if necessary, and take action as a result of that information. A WiseScript collects and analyzes the data and takes action in real time.
	You can write a WiseScript to quickly solve an urgent problem. You can also create a library of WiseScripts to resolve common problems and perform routine maintenance. In Software Management Solution, you can create a Quick Delivery or Package Delivery task to deploy your WiseScripts on an as-needed or regularly scheduled basis. You can add any of those tasks to a Managed Software Delivery policy to run the scripts as part of a larger delivery process.
	WiseScript for NS does not fully support the management of computers that run Windows Vista or 64-bit operating systems.

See "Installing the Wise Toolkit tools" on page 50.

For more information, see the topics in the help that is installed with each tool. You can access the help from each tool's **Help** menu. You can also press F1 to display context-sensitive help for an active page or dialog box.

Installing the Wise Toolkit tools

The Wise Toolkit provides the tools that let administrators create, customize, and manage installations.

See "About Wise Toolkit" on page 49.

When you install Software Management Solution, a software resource for the Wise Toolkit is created in the Software Catalog. You can use any delivery method to install these tools. We recommend that you install these tools on an Administrator's Desktop.

To install the Wise Toolkit tools

1   In the **Symantec Management Console**, on the **Manage** menu, click **Software**.

2   In the left pane, under **Software**, click **Software Catalog > Deliverable Software > Releases**.

3 In the right pane, click the following software resource:

Wise Toolkit *x*

where *x* is the version number.

4 On the **Actions** menu, click **Actions** and select the delivery method.

You can use either Managed Software Delivery or Quick Delivery.

See "Creating a Managed Software Delivery policy with the Managed Software Delivery wizard" on page 106.

See "Creating a Quick Delivery task with the Quick Delivery wizard" on page 134.

Configuring Software Management Solution settings

This chapter includes the following topics:

- **About Software Management Solution settings**
- **Configuring the default settings for Managed Software Delivery**
- **Schedule settings for Managed Software Delivery**
- **About recurring software deliveries**
- **About the Wake-on-LAN setting**
- **Download settings in Software Management Solution**
- **About the alternate download location for packages**
- **Run settings in Software Management Solution**
- **Advanced options in Managed Software Delivery policies**
- **Advanced options for tasks in Software Management Solution**
- **Task Options settings in Software Management Solution tasks**
- **Options for purging Software Management Solution data**
- **About replicating Software Management Solution data**

About Software Management Solution settings

Software Management Solution settings control the behavior of the software-related policies and tasks. The default settings let administrators create policies and tasks without having to enter the details that they are not familiar with. Instead, a more experienced administrator can configure the default settings that apply to all the policies and tasks that are created. When necessary, the administrator who runs the specific policies and tasks can change the settings.

Table 3-1   Sources of default settings for Software Management policies and tasks

Policy or task	Source of default settings
Managed Software Delivery	All new Managed Software Delivery policies inherit the default settings that are defined in the Managed Delivery Settings. You can override the default settings for specific Managed Software Delivery policies. See "Configuring the default settings for Managed Software Delivery" on page 54.
Package Delivery Quick Delivery Source Path Update Software Virtualization Windows Installer Repair	Some of the task settings are predefined. Other settings for these tasks are obtained from the Task Management settings or the Altiris Agent settings. You can override the settings for specific tasks. See "Advanced options for tasks in Software Management Solution" on page 70.

Configuring the default settings for Managed Software Delivery

Configuration settings control the behavior of Managed Software Delivery policies. Rather than configuring these settings individually for each policy, you can configure the default settings that apply to all new Managed Software Delivery policies. Then you can change the settings for a specific policy only when needed.

The default settings speed the creation of Managed Software Delivery policies and promote consistency among them.

You can override the default settings for Managed Software Delivery as follows:

■ When you create a Managed Software Delivery policy manually

■ When you edit an existing Managed Software Delivery policy

To configure default settings for Managed Software Delivery

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

2   In the left pane, under **Settings**, click **Software > Managed Delivery Settings**.

3   On the **Managed Delivery Settings** page, complete the following tabs to configure the specific settings:

Schedule tab	Lets you define the schedule on which a Managed Software Delivery policy runs. See "Schedule settings for Managed Software Delivery" on page 55.
Download tab	Lets you define how a Managed Software Delivery policy's downloads are handled. See "Download settings in Software Management Solution" on page 58.
Run tab	Lets you define how a Managed Software Delivery policy runs on the client computer. See "Run settings in Software Management Solution" on page 61.

4   When you finish the configuration, click **Save changes**.

Schedule settings for Managed Software Delivery

The Schedule settings let you define the schedule on which a Managed Software Delivery policy runs. You schedule the compliance check and the remediation action separately.

Managed Software Delivery policies perform compliance checks and remediations. A compliance check uses either the software resource's unique identifier or its detection rule to determine the state of the software on a managed computer. If the software is not in the correct state, the compliance check fails and remediation occurs. The nature of the remediation depends on the action that the Managed Software Delivery policy performs. For example, the remediation can consist of installing or uninstalling the software.

See "About policy applicability, compliance, and remediation" on page 102.

The Schedule settings appear in multiple places in the **Symantec Management Console** as follows:

On the **Managed Delivery Settings** page	Lets you define the default settings for all new Managed Software Delivery policies. You can override these settings for a specific policy.
	See "Configuring the default settings for Managed Software Delivery" on page 54.
On the **Schedule delivery** page that appears during the **Managed Software Delivery** wizard	Lets you change the settings for a specific policy.
	See "Creating a Managed Software Delivery policy with the Managed Software Delivery wizard" on page 106.
Under the **Schedule** section that appears when you create or edit a Managed Software Delivery policy	Lets you change the settings for a specific policy.
	See "Editing a Managed Software Delivery policy" on page 113.

For more information, see the topics on specifying a policy schedule in the *Symantec Management Platform Help*.

Table 3-2   Schedule settings for Managed Software Delivery: **Compliance**

Option	Description
Power on if necessary (using Wake-on-LAN, Intel, AMT, ASF)	Sends a signal to turn on a managed computer if it is turned off when the Managed Software Delivery policy runs.
	See "About the Wake-on-LAN setting" on page 57.
	The client computer must have a network card that is enabled for Wake-on-LAN, and Wake-on-LAN must be enabled in the client computer's BIOS settings.
	This option does not appear during the **Managed Software Delivery** wizard.
Add Schedule	Lets you add one or more schedules to the policy. You can specify as many schedules as you need, and you can have any number of schedules active at one time.
Time zone	Lets you specify the time zone to apply to the schedule.
No repeat	Lets you specify the interval at which to rerun the Managed Software Delivery, if any. This option is available only when you schedule a specific time or a specific window.
	Use this option to perform recurring compliance checks and remediation actions.
	See "About recurring software deliveries" on page 57.
Advanced	Lets you set the options that determine the conditions under which the check is performed and the effective dates for the policy.

Table 3-3 Schedule settings for Managed Software Delivery: **Remediation**

Option	Description
Your point of entry into these settings determines what text appears, as follows: ■ **When computers are found to be out of compliance, run remediation actions** ■ **Choose when to remediate when compliance fails**	Specify when to perform any remediation action that is defined for the Managed Software Delivery. The options are as follows: ■ **Immediately** ■ **At next maintenance window** ■ **Don't run remediation** Lets you run a Managed Software Delivery policy without performing the remediation. For example, you might want to perform an applicability check or a compliance check to determine if a certain configuration exists. A report of the results of the check might be all you need, or you might perform some action other than installing or uninstalling software.

About recurring software deliveries

When you schedule a Managed Software Delivery policy, you can configure its schedule to repeat daily, weekly, monthly, or yearly. Use this scheduling feature to ensure that the software remains in the correct state on the client computers.

Managed Software Delivery installs the software to a specific known state on the client computer. On a recurring basis, Managed Software Delivery can perform a compliance check to verify that the state is maintained. If the state of the software is out of compliance, Managed Software Delivery performs a remediation to restore the correct state.

See "Schedule settings for Managed Software Delivery" on page 55.

See "About policy applicability, compliance, and remediation" on page 102.

About the Wake-on-LAN setting

When you schedule the compliance check for a Managed Software Delivery policy, you can set the policy to turn on the client computer if necessary. This setting uses the Wake-on-LAN network standard.

See "Schedule settings for Managed Software Delivery" on page 55.

The Wake-on-LAN setting is used when a computer that the Managed Software Delivery policy targets is turned off or in sleep mode. A Wake-on-LAN packet is sent to client computers using a server-side task that is set to the policy's compliance schedule. For example, if your delivery policy is scheduled to check compliance at 12:00 p.m. every Wednesday, a corresponding Wake-on-LAN packet

is sent at that same time. The packet ensures that the client computer is turned on, awake, and able to perform the compliance check.

This setting has the following limitations:

- When the policy has a non-repeating schedule and the schedule date and time occur in the past, Wake-on-LAN cannot be performed.

- When the policy is applied to one or more users, it is impossible to know in advance what computer a user might log on to. Therefore, Wake-on-LAN cannot be performed. However, if the policy is also applied to computers, those computers can be awakened.

- This option does not support the waking up of a computer during a maintenance window. Because policy remediation is performed during a maintenance window, it cannot run if the client computer is turned off or in sleep mode. However, you can create a separate server task to wake up a client computer during its maintenance window.

The client computer must have a network card that is enabled for Wake-on-LAN, and Wake-on-LAN must be enabled in the client computer's BIOS settings.

Download settings in Software Management Solution

The **Download** settings let you define how the packages and command lines are downloaded for a policy or a task in Software Management Solution.

These settings appear in the following places:

On the **Managed Delivery Settings** page	Lets you define the default settings for all new Managed Software Delivery policies. You can override these settings for a specific policy.
	See "Configuring the default settings for Managed Software Delivery" on page 54.
In the **Advanced Options** dialog box that you can access when you edit a Managed Software Delivery policy.	Lets you change the settings for any specific software resource that the policy contains. The changes that you make for a specific policy do not change the defaults for other policies.
	See "Editing a Managed Software Delivery policy" on page 113.

In a Software Management Solution task, these settings appear in the **Advanced Options** dialog box, on the **Download Options** tab.

Lets you change the default settings for a specific Software Management Solution task.

See "Advanced options for tasks in Software Management Solution" on page 70.

You cannot change the default settings in a Software Virtualization task.

Table 3-4 **Download** settings

Option	Description
Destination download location	Lets you define the directory on the client computer in which to place the package file. The package downloads to and runs from this location. Options for the download location are as follows: ■ **Altiris agent cache** Places the package files in the default directory for software packages. The default location is as follows: *installation_path*\Altiris\Altiris Agent\Agents\SoftwareManagement\Software Delivery*package_GUID*\cache ■ **Location on destination computer** Lets you override the default directory and download the package directly to a directory that you specify. See "About the alternate download location for packages" on page 60.
Use the default Altiris Agent download settings to download	Lets you download and run the package with the default Download and Execute settings that are defined in the global Altiris Agent settings. These settings determine whether the package runs from the server or on the client computer. Even if the multicasting option is selected in the global Altiris Agent settings, it is not supported by the Software Management Solution tasks.

| | Table 3-4 | **Download** settings *(continued)* |

Option	Description
Use the following settings to download and run	(Windows only) Lets you override the default download settings that are defined for the Altiris Agent. The download settings that you can override are as follows: ■ **Run from the server if bandwidth is above** Runs the package directly from the Notification Server computer if the bandwidth is greater than the connection speed that you select. You also can choose to never run from the server. ■ **Download and run locally if bandwidth is above** Downloads the package or the command line and runs it locally if the bandwidth is greater than the connection speed that you select. ■ **Allow multicasting for package delivery** Uses a multicast download for the package. For this option to work, multicasting must be enabled in the Altiris Agent settings. This check box is not available in the Software Management Solution tasks because they do not support multicasting. For more information, see the topics about bandwidth throttling and multicasting in the *Symantec Management Platform Help*.
Delete package from client computer	Deletes the packages that are downloaded to the client computer but are not used for the amount of time you select in the **If unused for** drop-down list.

About the alternate download location for packages

The download settings for Software Management Solution delivery policies and tasks contains the **Destination download location** option. This option lets you define the directory on the destination computer in which to place the package files. The default location is the Altiris Agent cache. You can also select an alternate download location.

When a delivery task or policy is executed on a client computer, the log.xml event file and other delivery-related XML files are created. The download settings do not affect the location of the XML files.

How different delivery methods use the alternate download location

Delivery method	Where the download location is specified	Download location
Quick Delivery task or Package Delivery task	In the **Advanced Settings** dialog box for the specific task	■ The package is downloaded to the alternate download folder that is defined for the task. ■ The XML files are created in a subfolder under the default download location. The subfolder's name is the same as the GUID that is associated with the package.
Managed Software Delivery policy	In the **Advanced Options** dialog box for the specific policy	■ The package is downloaded to the alternate download folder that is defined for the policy. ■ The XML files are created in a subfolder under the default download location. The subfolder's name is the same as the GUID that is associated with the package.
Managed Software Delivery policy	In the global settings on the **Managed Delivery Settings** page	■ The package is downloaded to a subfolder of the alternate download folder that is defined for the policy. The subfolder's name is the same as the GUID that is associated with the package. ■ The XML files are created in a subfolder under the default download location. The subfolder's name is the same as the GUID that is associated with the package.

Run settings in Software Management Solution

The Run settings let you define how a Managed Software Delivery policy runs on the client computer. They also let you define how much you let the user interact with the policy.

The Run settings are arranged in sections. The appearance and location of the sections depend on how you access the settings.

Table 3-6 Sections on the **Run** tab

Section	Description
Run As section	(Windows only) The options in this section let you define the account under which the policy runs on the client computer. See "Run As settings in Software Management Solution" on page 62.

Table 3-6   Sections on the **Run** tab *(continued)*

Section	Description
User run conditions section	(Windows only) The options in this section let you define the conditions under which the policy runs and the level of user interaction with the policy. See "User run conditions settings in Software Management Solution" on page 63.
Results-based actions section	The options in this section let you define the actions that occur during or after the policy runs on the client computer. In a Managed Software Delivery policy, the **Results-based actions** section appears in the **Advanced Options** dialog box, on its own tab. See "Results-based actions settings in Software Management Solution" on page 67.
Reporting section	The option in this section defines the level of detail that is logged when a policy runs on the client computer. In a Managed Software Delivery policy, the **Reporting** section appears on the **Policy settings** tab. See "Reporting settings in Software Management Solution" on page 69.

Run As settings in Software Management Solution

(Windows only)

The options in this section let you define the account under which a policy or a task runs on the client computer.

These settings appear in the following places:

On the **Managed Delivery Settings** page, on the **Run** tab.	Lets you define default settings for all new Managed Software Delivery policies. See "Configuring the default settings for Managed Software Delivery" on page 54. See "Run settings in Software Management Solution" on page 61.

In a Managed Software Delivery policy, these settings appear in the **Advanced Options** dialog box, on the **Run** tab.	Lets you change the settings for a specific software resource that the policy contains. The changes that you make for a software resource in a specific policy override the global settings. See "Editing a Managed Software Delivery policy" on page 113.
In a Software Management Solution task, these settings appear in the **Advanced Options** dialog box, on the **Run Options** tab.	Lets you change the default settings for a specific Software Management Solution task. See "Advanced options for tasks in Software Management Solution" on page 70. You cannot change the default settings in a Software Virtualization task.

Table 3-7   Options in the **Run As** section

Option	Description
Altiris Agent credential	Lets you run the task with the default authentication settings that are defined in the global Altiris Agent settings. For more information, see the topics about the Agent Connectivity Credential settings and about configuring the global agent settings in the *Symantec Management Platform Help*.
Current logged-on user	Lets you run the task with the current user's credentials. This option overrides the default Authentication settings that are defined in the global Altiris Agent settings.
Specific user	Lets you run the task with a specific user's credentials. For example, you might use specific credentials to perform an administrative task when the system account is locked down. This option overrides the default authentication settings that are defined in the global Altiris Agent settings. When you select this option, enter the following credentials: ■ **Domain** ■ **User Name** ■ **Password** The credentials that you supply must be for a known account on Notification Server and every package server. This option is not available in the default Managed Delivery Settings. You can set a specific user's credentials in individual Managed Software Delivery policies only.

User run conditions settings in Software Management Solution

(Windows only)

The options in this section let you define the conditions under which the policy or the task runs and the level of user interaction.

These settings appear in the following places:

On the **Managed Delivery Settings** page, on the **Run** tab.	Lets you define default settings for all new Managed Software Delivery policies. See "Configuring the default settings for Managed Software Delivery" on page 54. See "Run settings in Software Management Solution" on page 61.
In a Managed Software Delivery policy, most of these settings appear in the **Advanced Options** dialog box, on the **Run** tab. The remaining options appear on the **Policy settings** tab.	Lets you change the settings for a specific software resource that the policy contains. The changes that you make for a software resource in a specific policy override the global settings. See "Editing a Managed Software Delivery policy" on page 113.
In a Software Management Solution task, these settings appear in the **Advanced Options** dialog box, on the **Run Options** tab.	Lets you change the default settings for a specific Software Management Solution task. See "Advanced options for tasks in Software Management Solution" on page 70. You cannot change the default settings in a Software Virtualization task.

Table 3-8   Options in the **User run conditions** section

Option	Description
Task can run (Managed Software Delivery policies only)	Lets you define the condition under which this task can run. The conditions are as follows: ■ **Only when user is logged on** ■ **Whether or not the user is logged on** ■ **Only when no user is logged on** Tasks that run when no user is logged on run silently regardless of how the execution is configured. This option is not available if you selected **Current logged-on user** under the **Run As** section. See "Run As settings in Software Management Solution" on page 62.

Table 3-8   Options in the **User run conditions** section *(continued)*

Option	Description
Repeat this task for each logged on user (Managed Software Delivery policies only)	Runs the task for each user who is logged on to the client computer. This check box is available only if you clicked the following option under **Task can run**: **Only when user is logged on**.
Allow user to interact with installing software (Managed Software Delivery policies) **Allow user interaction** (Software Management Solution tasks)	Lets you specify whether the installation's user interface appears when the package runs. When a package's execution is complex, we recommend that you check this check box and click **Hidden** under **Allow user to interact with installing software**. This check box is not available if you clicked the following option under **Task can run**: **Hidden**. When you do not check this check box, the package runs silently. This check box is primarily intended for non-Windows Installer packages that do not have the built-in ability to run silently. If the package's command line contains options for the user interface, those commands override this setting. For example, if you check this check box but the command line runs the package silently, the installation's user interface does not appear.
Display window	Lets you define how the installation's user interface appears when the package runs. This option is available only if you checked the following check box: **Allow user to interact with installing software**. The user interface options are as follows: ■ **Normal** ■ **Hidden** Normally, this option is not used because it conflicts with the option to let the user interact with the installation. However, you might use this option to hide the main installation window from the user but let the installation run in interactive mode. That way, any errors or messages that result during the installation are presented to the user. Otherwise, when an installation runs in non-interactive mode, any error messages are hidden and can hang the installation. ■ **Maximized** ■ **Minimized** The package's command line overrides this setting.

Table 3-8   Options in the **User run conditions** section *(continued)*

Option	Description
Prompt user before running	Notifies the user before the policy runs by displaying the **Starting Task** dialog box. The policy starts 60 seconds after the dialog box appears. A progress bar shows the amount of time that remains. The user can dismiss the **Starting Task** dialog box but cannot cancel the policy unless you select **Allow user to turn on policy from the Altiris Agent**. The **Starting Task** dialog box appears only if the **Show popup notifications** check box is checked on the client computer's Altiris Agent.
Allow user to defer up to a total of	Lets you allow the user to defer running the policy up to the maximum amount of time that you select. The ability to defer policies lets the user save work and close any open files or programs. This check box is available only if you checked the following check box: **Prompt user before running**. When you check this check box, the **Starting Task** dialog box that appears to the user contains the following options: ■ **Run Now** ■ **Run Later** ■ **Remind me again in** Lets the user select the amount of time to defer the policy. The total amount that the user can defer the policy cannot exceed the maximum time that you specify.
Allow user to turn on policy from the Altiris Agent	Lets the user choose when to run the policy by clicking the policy in the Altiris Agent. The user can also choose not to run the policy. A policy's remediation options override this global setting and its related settings. For example, if this check box is checked here but not in a specific policy, then the user cannot choose when to run that policy. In a Managed Software Delivery policy, this check box appears on the **Policy settings** tab.

Option	Description
User must turn on from Altiris Agent	Requires the user to run the policy. If you select this option, the policy never runs automatically.
	This check box is available only if you checked the following check box: **Allow user to turn on policy from the Altiris Agent**.
	The user can run the policy by clicking it on the **Software Delivery** tab that is on the Altiris Agent.
	The user can also run the policy by clicking **Start Task Now** on the **New Software is Available** dialog box, if the following conditions are met:
	■ If you check **Prompt user when this policy is available on their computer** for the policy. ■ If the **Show popup notifications** check box is checked on the client computer's Altiris Agent.
	In a Managed Software Delivery policy, this check box appears on the **Policy settings** tab.
Prompt user when this policy is available	Displays a message to notify the user that new software is available. When the user clicks the message, the **New Software is Available** dialog box opens. The user can start, dismiss, or defer the policy. If you do not choose to prompt the user, the **New Software is Available** dialog box does not appear.
	This check box is available only if you checked the following check box: **Allow user to turn on policy from the Altiris Agent**.
	The **New Software is Available** dialog box appears only if the **Show popup notifications** option is selected on the client computer's Altiris Agent.
	In a Managed Software Delivery policy, this check box appears on the **Policy settings** tab.

Results-based actions settings in Software Management Solution

These settings let you define the actions that occur during or after the Software Management Solution policy runs on the client computer.

These settings appear in the following places:

On the **Managed Delivery Settings** page, on the **Run** tab.	Lets you define default settings for all new Software Management Solution policies. See "Configuring the default settings for Managed Software Delivery" on page 54. See "Run settings in Software Management Solution" on page 61.
In a Managed Software Delivery policy, these settings appear in the **Advanced Options** dialog box, on the **Results-based actions** tab.	Lets you change the settings for a specific software resource that the policy contains. The changes that you make for a software resource in a specific policy override the global settings. See "Editing a Managed Software Delivery policy" on page 113.

Table 3-9   Options in the **Results-based actions** section or tab

Option	Description
Upon success run	Lets you define an action to occur after the policy runs successfully. The options are as follows: ■ **No action required** ■ **Restart computer** ■ **Log off user**
Allow user to defer action up to	Lets you allow the user to defer the post-execution action up to the maximum amount of time that you select. This option is not available if you clicked the **No action required** option in the **Upon success run** drop-down list.
Force running applications to close	Lets you force any applications that are running on the client computer to close before a post-execution restart or logoff occurs. This option is not available if you clicked the **No action required** option in the **Upon success run** drop-down list.
Terminate after	Lets you define the amount of time to wait before the policy terminates if it stops responding.
Upon failure	Defines whether the policy aborts, continues, or restarts when it fails. When you create a Managed Software Delivery policy, this setting is the same for each software resource and task that the policy contains. You can edit the policy to override this setting for each software resource and task. For example, if the execution of the first software resource fails, you can run subsequent items. Conversely, if one execution in the sequence fails, you can abort the remaining items in the sequence.

Options in the **Results-based actions** section or tab *(continued)*

Option	Description
Max retries	Defines the number of times that the policy retries when it fails.

Reporting settings in Software Management Solution

This section lets you define the level of detail that is logged when a Software Management Solution policy runs on the client computer.

The **Reporting** section appears in the following places:

On the **Managed Delivery Settings** page, on the **Run** tab	Lets you define default settings for all new Software Management Solution policies. See "Configuring the default settings for Managed Software Delivery" on page 54. See "Run settings in Software Management Solution" on page 61.
On the **Policy settings** tab that appears when you edit a Managed Software Delivery policy.	Lets you change the settings for the entire policy, including all the software resources and tasks that it contains. The changes that you make for a specific policy do not affect the default settings or the settings in other policies. See "Editing a Managed Software Delivery policy" on page 113.

Table 3-10 Options in the **Reporting** section

Option	Description
Enable verbose reporting of status events	Records the details of policy status, package download, and execution events and posts them to the Notification Server computer.

Advanced options in Managed Software Delivery policies

This dialog box lets you change the settings for the individual software resources that are in a specific Managed Software Delivery policy. For example, you might download this software's package to a different location or allow the user to interact with this software's installation but not others.

These settings are inherited from the policy but you can change them for any and all the software resources in the policy. The changes that you make for a specific policy do not change the defaults for other policies.

The **Advanced options** dialog box appears when you edit a Managed Software Delivery policy, select a specific software resource, and click **Advanced options**.

See "Editing a Managed Software Delivery policy" on page 113.

Table 3-11   Tabs in the **Advanced options** dialog box

Tab	Description
Download tab	Defines how a specific software resource downloads to the client computer.
	See "Download settings in Software Management Solution" on page 58.
Run tab	Defines how a specific software resource runs on the client computer.
	This tab contains the same settings that are under the **Run As** section and the **User run conditions** section on the **Managed Delivery Settings** page.
	See "Run As settings in Software Management Solution" on page 62.
	See "User run conditions settings in Software Management Solution" on page 63.
Results-based actions tab	Defines the actions that occur during or after the policy runs on the client computer.
	See "Results-based actions settings in Software Management Solution" on page 67.

Advanced options for tasks in Software Management Solution

This dialog box lets you change the settings that define how a specific task runs. These settings are predefined to make task creation easier and to maintain consistency across your organization. However, you can change the default settings for a specific task. For example, you can run the task with different user credentials. The changes that you make for a specific instance of a task do not change the defaults for other instances of that task.

When you create or edit a task in Software Management Solution, the **Advanced** option provides access to the task settings.

See "Editing a task in Software Management Solution" on page 143.

Table 3-12 Tabs in the **Advanced settings** dialog box

Tab	Description
Download Options tab	Contains the settings that define how a specific task downloads and runs on the client computer. The defaults for some of these settings are inherited from the Altiris Agent settings. See "Download settings in Software Management Solution" on page 58.
Run Options tab	Defines how a specific software resource runs on the client computer. See "Run As settings in Software Management Solution" on page 62. See "User run conditions settings in Software Management Solution" on page 63.
Task options tab	Contains the settings that define how a specific software management task runs on the client computer. The defaults for these settings are inherited from the Task Server settings. See Table 3-13 on page 72.

The tasks that use these settings are as follows:

■ Package Delivery
See "About Package Delivery" on page 137.

■ Quick Delivery
See "About quick delivery of a single software resource" on page 131.

■ Source Path Update
See "About source path updates for Windows Installer applications" on page 198.

■ Windows Installer Repair
See "About Windows Installer repair" on page 193.

See "Editing a task in Software Management Solution" on page 143.

Task Options settings in Software Management Solution tasks

This tab lets you edit the settings that define how a specific Software Management Solution task runs on the client computer. The defaults for these settings are inherited from the Task Server settings.

The Task Options tab appears in the **Advanced settings** dialog box, which you can access when you create or edit a task in Software Management Solution.

See "Advanced options for tasks in Software Management Solution" on page 70.

See "Editing a task in Software Management Solution" on page 143.

Table 3-13   Options on the **Task Options** tab

Option	Description
Ensure no other tasks are running while this task is running	Lets you prevent other tasks from running until the current task finishes.
End task after	Lets you define the amount of time to wait before the task ends if it stops responding.
	For example, if you expect the task to run for no longer than 20 minutes, then set this option to 30 minutes.

Options for purging Software Management Solution data

Software Management Solution data is stored in the Configuration Management Database on the Notification Server computer. The data is grouped in resource data classes. A resource data class defines one or more fields, and the properties of the fields, that a resource of that class may have.

Settings in the Symantec Management Platform determine how long the data is retained in the database before it is purged. You can specify the retention period for specific data classes. These settings are on the **Purging Maintenance** page that appears in Notification Server.

For more information, see the topics on resource data classes and purging the Configuration Management Database in the *Symantec Management Platform Help*.

The data classes that represent Software Management Solution data are as follows:

- **Computer Events:**
  AeX SWD Execution

AeX SWD Status

AeX SWD Package

SoftwareManagementSolution MSI Repair

- **Events:**
SoftwareManagementSolution App State Failures
SoftwareManagementSolutionAppRepair

- **Policy Compliance Remediation**

- **Virtual Software Events:**
Software Virtualization Events

About replicating Software Management Solution data

Software Management Solution supports hierarchy and replication. These features let you create tasks and policies at the top-level Notification Server computer and replicate them to child-level Notification Server computers.

Hierarchy defines the information flows across multiple Notification Server computers in an enterprise. Hierarchy uses replication to copy and synchronize shared objects and data between multiple Notification Server computers within the same hierarchical structure.

Software Management Solution supports full and differential replication. Differential replication replicates only those items that changed since the last replication.

Hierarchy replicates each object or piece of data in one direction only.

For more information, see the topics about hierarchy and replication in the *Symantec Management Platform Help*.

Table 3-14   Software Management Solution data that can be replicated

Data	Direction of replication
Tasks: Quick Delivery, Package Delivery, Source Path Update, Windows Installer Repair Any tasks that are replicated with the default replication rules cannot be edited on the child computers.	Down

Table 3-14   Software Management Solution data that can be replicated
(continued)

Data	Direction of replication
Policies: Managed Software and Legacy Software Delivery, including any Legacy Software Delivery policies that are in subfolders Any policies that are replicated with default replication rules cannot be edited on the child computers. However, those policies can be scheduled on the child computers.	Down
Software resources This data is defined in the Symantec Management Platform but it is used in Software Management Solution.	Down
Managed Software Delivery global settings	Down
Software publishing information from software resources and Managed Software Delivery policies	Down
Software Portal settings and the Software Portal agent settings	Down
Events	Up
Data classes	Down
Reports	Down
Computer and user resources and collections This data is defined in the Symantec Management Platform but it is used in Software Management Solution.	Not applicable
Security Permissions, Roles, Privileges This data is defined in the Symantec Management Platform but it is used in Software Management Solution.	Down

Some of the Software Management Solution data that cannot be replicated is as follows:

- All the read-only items that the solution installs

- All the packages for the agents that are used in Software Management Solution as follows:

  - Application Management Agent

  - Software Management Solution Agent (Windows)

- ■ Software Management Solution Plug-in for AIX

- ■ Software Management Solution Plug-in for HP-UX

- ■ Software Management Solution Plug-in for Linux

- ■ Software Management Solution Plug-in for Mac

- ■ Software Management Solution Plug-in for Solaris

- ■ Software Portal Agent

- ■ Software Virtualization Agent

■ The package for installing the Wise Toolkit

Performing common tasks in Software Management Solution

This chapter includes the following topics:

- About the Software Management worker view

- Sources of status information in Software Management Solution

- About Software Management Solution event files

- About Software Management Solution reports

- Running a Software Management Solution report

About the Software Management worker view

The **Software Management worker view** in the **Symantec Management Console** provides a single place to perform software-related action and view certain software reports. You can review the status of current software policies and tasks, create new policies and tasks, access the Software Catalog, and configure software-related settings.

The **Software Management worker view** is available from the **Home** menu, under **Software > Software Delivery**. The view menu appears in the left pane of the **Symantec Management Console** and contains links to software-related functions.

Table 4-1	Sections and options in the **Software Management worker view**

Section	Options
Manage Software Catalog	Lets you access the software releases, service packs, and updates that are in the Software Catalog. For more information about the Software Catalog, see the *Symantec Management Platform Help*.
Deliver/Manage Software	Lets you create and edit the policies and tasks in Software Management Solution and approve requested software from the **Administrator Portal**. See "Methods for delivering software" on page 88.
Software Compliance	Lets you run compliance reports in the following ways: ■ **By Managed Delivery Policy** ■ **By Computer** See "About Software Management Solution reports" on page 82.
Quick Delivery Status	Lets you run Quick Delivery status reports in the following ways: ■ **By Task** ■ **By Computer** See "About Software Management Solution reports" on page 82.
Settings	Lets you configure the following settings: ■ **Configure Software Library Location** For more information, see the topic about configuring the Software Library in the *Symantec Management Platform Help*. ■ **Rollout Software Management Solution plug-in** See "Installing the Software Management Solution agent" on page 38. ■ **Rollout Software Portal plug-in** See "Installing the Software Portal agent" on page 46. ■ **Configure Software Portal** See "Configuring the Software Portal settings" on page 181. ■ **Configure Software Portal Administrators** For more information, see the topics on setting up security, security roles, and security role privilege settings in the *Symantec Management Platform Help*. ■ **Configure Software Portal Managers** For more information, see the topics on setting up security, security roles, and security role privilege settings in the *Symantec Management Platform Help*. ■ **Configure Managed Delivery Defaults** See "Configuring the default settings for Managed Software Delivery" on page 54.

Sources of status information in Software Management Solution

You can obtain status and other information about Software Management Solution tasks, policies, and other actions from several sources. Each source provides a different type or format of information depending on your needs.

Table 4-2   Sources of status information for Software Management Solution

Information	Source	Description
A wide range of information about software delivery, compliance, software requests, application management, and software virtualization	Reports	The predefined Software Management Solution reports are an excellent source for compliance and delivery status information. See "About Software Management Solution reports" on page 82.
Graphical representations of the status of Software Management tasks, policies, and requests	Software Management Solution Web parts	Web parts are the building blocks for portal pages in the **Symantec Management Console**. You can add the Software Management Solution Web parts to any portal page that you can access. See "Web parts for Software Management Solution" on page 48.
Status of Software Management tasks and policies	**Software Management worker view** in the **Symantec Management Console**	The Software Management worker view provides a single place to view software-related status reports. See "About the Software Management worker view" on page 77.

	Table 4-2	Sources of status information for Software Management Solution *(continued)*

Information	Source	Description
Status and details for a specific task	Task status views on the Notification Server computer	You can view a task's status and details in the following places: ■ The **Task Status** section on the task details page You can open any Software Management Solution task to view its **Task Status** section. This section lists the instances of the task and the status of each instance. For each instance, you can drill down to the details of its delivery and execution and to the computers on which the task was run. See "Editing a task in Software Management Solution" on page 143. ■ The Job and Task Status Web part You can add this Web part to the **Jobs and Task Portal** page or to any other portal page. This Web part displays individual instances of each task. For each instance, you can drill down to the details of its delivery and execution and to the computers on which the task was run.
Status of tasks and policies on a specific client computer	Altiris Agent	You can check the status of a task or policy on the Altiris Agent on the client computer. For more information, see the topics about viewing the task status on the Altiris Agent in the *Symantec Management Platform Help*.
Detailed information about downloads and executions on a specific client computer	Software event files on the client computer	The Software Management Solution agent creates files on the client computer that record information about the Software Management Solution events on that computer. The event files are as follows: ■ AexSWDPolicy.xml Records the execution details and status for every software delivery task and policy that runs on the client computer. ■ log.xml Records the download status for each command line and package that a specific software resource contains. See "About Software Management Solution event files" on page 81.

| Table 4-2 | | Sources of status information for Software Management Solution *(continued)* |

Information	Source	Description
Events that occur within the Symantec Management Platform	Altiris Log	The Altiris Log records the events that occur within the Symantec Management Platform, including errors. When a task or policy does not behave as you expected, you can open the log and view the specific event to diagnose problems. The Altiris Log Viewer lets you open and view the Altiris Log. For more information, see the topics about the Altiris Log and the Altiris Log Viewer in the *Symantec Management Platform Help*.

About Software Management Solution event files

The Software Management Solution agent creates files on the client computer that record information about the Software Management Solution events on that computer. You can view these files to obtain detailed information about downloads and executions on a specific client computer.

| Table 4-3 | | Software Management Solution event files |

Event file	Description	Location on the client computer
AexSWDPolicy.xml	Records the execution details and status for every software delivery task and policy that runs on the client computer. The detailed information includes the package identification, the execution options, the command line, and the results of the execution.	*installation path*\Altiris\Altiris Agent\Agents\SoftwareManagement\Software Delivery
log.xml	Records the download status for each command line and package that a specific software resource contains. By default, this file records the last 30 download attempts. You can change this value by editing the following registry key on the client computer: HKLM\SOFTWARE\Altiris\Communications\Package Delivery\Download history size	*installation_path*\Altiris\Altiris Agent\Agents\SoftwareManagement\Software Delivery*package_GUID*\cache See "About the alternate download location for packages" on page 60.

About Software Management Solution reports

Predefined reports let you easily view and analyze your Software Management Solution data. The reports are grouped in folders by type in the **Symantec Management Console**.

You can also create your own custom reports.

For more information, see the topics about custom Notification Server reports in the *Symantec Management Platform Help*.

By default, all the Software Management Solution reports support resource scoping, which limits the data that users can access based on their security roles.

The Software Management Solution reports use the scoping feature as follows:

- When a user runs a report, the report contains only the data that the user has permissions for.

- When a user saves a snapshot of a report, the snapshot is scoped according to that user's permissions. The users who have a lower security role than the original user cannot view the snapshot. The users who have a higher security role than the original user can see only the data that the original user was allowed to access.

- You can clone a report and edit the clone's SQL query to customize how the data is scoped when it is extracted for that report. You can also include scoping information when you create an SQL query for a custom report.

- You can clone a report and edit the clone to select the fields that are scoped when data is extracted from that report's snapshots.

For more information, see the topics about configuring the scoping fields in a report and about defining an SQL query in the *Symantec Management Platform Help*.

Table 4-4   Types of predefined reports in Software Management Solution

Report type and folder	Description
6.0 Legacy Reports	Contains the reports that appeared in Software Delivery Solution 6.x. This folder does not contain any custom reports that were defined in 6.0. The Legacy Reports can contain data from Software Management Solution 7.0 as appropriate. They can also contain any data that you might have migrated from Software Delivery Solution 6.x.
Application Management	Contains the reports that display information about the Windows Installer applications that are broken or that have inaccessible source paths.
Compliance	Contains the reports that display information about the compliance actions and the remediation actions that Managed Software Delivery performs.
Delivery	Contains the reports that display information about the status of the software downloads and executions. If you migrated software delivery data from Software Delivery Solution 6.x, the new delivery reports contain data from both 6.x and 7.0.
Portal	Contains the reports that display the status of software requests that are made through the **Software Portal**.
Virtualized Software Resources	Contains the reports that display information about the actions (events) that have been performed on the virtual layers that are installed on client computers.

Running a Software Management Solution report

You can view reports to get information about the actions that you perform in Software Management Solution.

For more information, see the topics about reports in the *Symantec Management Platform Help*.

To run a Software Management Solution report

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

2   In the left pane, under **Reports**, expand **Software** and expand the folder that contains the report that you plan to run.

    See "About Software Management Solution reports" on page 82.

3   Under the folder that you expanded, select a report.

4   When the report appears in the right pane, you can print the report or save it in a variety of formats. Other actions might be available depending on the type of report.

Section 2

Delivering software

Introducing software delivery

This chapter includes the following topics:

- About software delivery
- Methods for delivering software
- Methods for uninstalling software
- How Software Management Solution integrates with the Software Catalog and Software Library

About software delivery

Software Management Solution lets you deliver and install software safely and accurately on managed client computers. You can create tasks and policies to respond to software delivery needs from elementary to complex.

Software Management Solution integrates with the Software Catalog and the Software Library that are part of the Symantec Management Platform. By leveraging this information, Software Management Solution ensures that the correct software gets installed, remains installed, and runs without interference from other software. This integration lets your administrators focus on delivering the correct software instead of redefining the packages, command lines, and so on for each delivery.

See "How Software Management Solution integrates with the Software Catalog and Software Library" on page 93.

Software Management Solution supports packages for the Windows, UNIX, Linux, and Mac operating systems. With few exceptions, all the functions in Software Management Solution work the same for all platforms. For example, you use the

same method to create a delivery task for a Windows, UNIX, Linux, or Mac OS package.

You can use Software Management Solution tasks or policies to fulfill any of the following delivery requirements:

- Perform a quick delivery of a single software resource.

- Perform one or more advanced delivery actions.
  For example, you can deliver multiple software resources and periodically check the client computer to verify that they are in the correct state.

- Deliver software automatically in response to a direct request from a user.

- Deliver a package that is not associated with a software resource.

- Deliver software with a policy that you migrated from Software Delivery Solution 6.x.

- Create a new virtual software layer on a client computer.

See "Methods for delivering software" on page 88.

Methods for delivering software

You can deliver software to one or more managed computers by creating and running a Software Management task or policy. The method that you use to create the task or policy depends on your delivery requirements.

| Table 5-1 | Methods for delivering software |

Your requirement	Delivery method	Description
Perform a quick delivery of a single software resource.	Quick Delivery	You can use the task-based Quick Delivery method to specify the software to deliver, the action to perform, and the computers to deliver to. Quick Delivery uses the default task settings, which you can change when necessary. Because of its simplicity, Quick Delivery is an ideal way for non-administrators, such as help desk personnel, to deliver software safely and accurately. The software that you deliver in this way must be defined as a deliverable software resource in the Software Catalog. See "About quick delivery of a single software resource" on page 131.
Perform one or more of the following advanced delivery actions: ■ Deliver on a recurring schedule. ■ Install to a known state and ensure that the state is maintained. ■ Install software with the other software that it depends on. ■ Install a software resource that replaces other software. ■ Sequentially install multiple software and tasks. ■ (Windows only) Install software into a virtual software layer. ■ Run any client task at any stage of the delivery. A client task is one that is defined in Notification Server and is intended to run on a client computer.	Managed Software Delivery	Managed Software Delivery is a policy-based delivery method that lets you fulfill advanced delivery requirements. A single Managed Software Delivery policy can perform multiple delivery actions. The software that you deliver in this way must be defined as a deliverable software resource in the Software Catalog. Managed Software Delivery leverages the software resource information and the logic that is in the Software Catalog. For example, Managed Software Delivery uses the software resource's dependencies, package, and detection rule. See "About advanced software deliveries" on page 96.

Table 5-1	Methods for delivering software *(continued)*

Your requirement	Delivery method	Description
Deliver software in response to a direct request from a user.	**Software Portal**	(Windows and Mac only) With the **Software Portal**, users can request software and responds to those requests. If the user is pre-approved to install the software, the installation occurs without the administrator's involvement. Otherwise, the administrator only needs to approve the requests and deliver the software that is not in the Software Catalog. See "About the Software Portal" on page 161.
Deliver a package that is not associated with a software resource.	Package Delivery	Package Delivery is a task-based delivery method. It lets you deliver any package regardless of whether it is associated with a software resource. See "About Package Delivery" on page 137.
Deliver software with a policy that you migrated from Software Delivery Solution 6.x.	Legacy Software Delivery	When you upgrade from Notification Server 6.x to Symantec Management Platform 7.0, you can migrate your 6.x software delivery tasks to Legacy Delivery policies. You can continue to use those policies as they are. You can also assign their packages to software resources to deliver a 6.x software package with Quick Delivery or Managed Software Delivery. See "About Legacy Software Delivery" on page 149.
(Windows only) Install software into a new virtual software layer on a client computer.	Software Virtualization task Quick Delivery Package Delivery	Imports a virtual software archive (VSA) file to a managed client computer and creates a new virtual software layer. A VSA file is an installation file for one or more Windows-based applications or sets of data. See "Methods for installing and managing virtual software" on page 221.

| Table 5-1 | | Methods for delivering software *(continued)* |

Your requirement	Delivery method	Description
(Windows only) Virtualize an application and install it into a new virtual software layer on a client computer.	Managed Software Delivery	You can create and manage new virtual software layers or manage existing layers on client computers. A Managed Software Delivery policy lets you perform complex layer management tasks. See "Installing and managing a virtual software layer with a Managed Software Delivery policy" on page 230.

Methods for uninstalling software

You can uninstall software from one or more managed computers by running a Software Management policy or task.

The method that you use to uninstall software depends on how the software was installed.

| Table 5-2 | Methods for uninstalling software |

Installation method	Uninstall method
The software was installed with a Software Management Solution task or policy.	You can clone the original installation task or policy and then edit the clone to select an uninstall command line.

Table 5-2   Methods for uninstalling software *(continued)*

Installation method	Uninstall method
The software was not installed with Software Management Solution.	If a software resource is defined for that software, you can create a software delivery task or policy and select an uninstall command line.
	See "Methods for delivering software" on page 88.
	If a software resource is not defined for that software, you can create one in the Software Catalog.
	For more information, see the topics about creating software resources and command lines in the *Symantec Management Platform Help*.
	If you prefer not to create a software resource, you can use a Package Delivery task. For Windows software, you can obtain the uninstall command line from the registry of a computer that contains that software. The command line is in the UninstallString key in the following folder:
	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion\Uninstall*application folder*
The software was installed into a virtual layer with a Software Management Solution task or policy.	You can clone the original installation task or policy and then edit the clone to select a deactivate and delete command line.
The software was installed into a virtual layer, but not with Software Management Solution.	You can use a Software Virtualization task to deactivate and delete any virtual software layer that was installed with one of the following products: Altiris Software Virtualization Solution or Symantec Workspace Virtualization. You can specify the name of the layer to act upon.
	See "Installing and managing a virtual software layer with a Software Virtualization task" on page 225.

Managed Software Delivery provides the ability to perform more complex uninstall tasks. For example, you can use a Managed Software Delivery policy to not only uninstall obsolete software but also install new software at the same time.

See "About installing software that replaces other software" on page 124.

Managed Software Delivery can also regularly check computers for the presence of unauthorized software and uninstall any unauthorized software that is found. For example, you can use a Managed Software Delivery policy to remove game software from client computers on a recurring basis.

How Software Management Solution integrates with the Software Catalog and Software Library

In Software Management Solution, Quick Delivery and Managed Software Delivery leverage the software resource information that is in the Software Catalog and Software Library. When you create a task or policy, you select a software resource to deliver. Any information about the software that the task or the policy needs is available from the software resource.

The Software Catalog and Software Library are part of the Symantec Management Platform.

For more information, see the topics about the Software Catalog, the Software Library, and software resources in the *Symantec Management Platform Help*.

Table 5-3   How features in Software Management Solution use software resource information

Feature	Usage of software resource information
Quick Delivery	The **Quick Delivery** wizard limits the selections that you need to make to deliver software. You select the software resource to deliver, the command line to use, and the destinations to target. The software resource provides any other information that is required for the delivery. This simplified delivery method lets you entrust certain deliveries to non-administrators such as help desk personnel. See "About quick delivery of a single software resource" on page 131.
Managed Software Delivery	The software resource information is essential for the complex deliveries that Managed Software Delivery performs. Managed Software Delivery uses the software resource's rules to intelligently perform applicability and compliance checks and to remediate the software that is out of compliance. These checks conserve bandwidth by ensuring that the software is not downloaded to computers on which it is already installed. The **Managed Software Delivery** wizard can use the software resource's associations to alert you to the following situations: ■ When the selected software depends on other software resources ■ When an update to the selected software is available ■ When other software supersedes the selected software ■ (Windows only) When the selected software resource conflicts with another software resource See "About advanced software deliveries" on page 96.

Table 5-3 How features in Software Management Solution use software resource information *(continued)*

Feature	Usage of software resource information
Software Portal	(Windows and Mac OS only) In each software resource, you can configure settings for making that software available to the **Software Portal**. The settings determine which users are allowed to request that software and whether their requests require approval. See "About the Software Portal" on page 161.

See "About Software Management Solution" on page 13.

Performing advanced software deliveries

This chapter includes the following topics:

- About deferring the execution of software remediation

- About installing software that replaces other software

- About delivering multiple software resources and tasks

- Delivering multiple software resources and tasks sequentially

- About the status of Managed Software Delivery policies

About advanced software deliveries

In many organizations, administrators spend the majority of their software delivery time on a minority of advanced delivery activities. Managed Software Delivery simplifies advanced software deliveries by letting you deliver software as a unit, which can include multiple software resources as well as dependencies. For example, you can create a single Managed Software Delivery policy that installs an application and its associated patches and service packs. Managed Software Delivery can also run any task at any stage of the delivery. For example, it can run a task that performs a restart or runs a script.

Managed Software Delivery is a policy-based delivery method that lets you respond to an assortment of advanced delivery requirements.

See "Performing an advanced software delivery" on page 104.

The power of Managed Software Delivery lies in the following abilities:

- To intelligently perform the compliance checks and the remediation actions that let you not only deliver software but also manage it.

- To leverage the software resource information and the logic that is in the Software Catalog such as dependencies, packages, and detection rules.

- To conserve bandwidth by downloading packages only when they are needed. If a client computer does not have the appropriate configuration for the software or if the software is already installed, the package is not downloaded.

- To perform multiple delivery actions with a single policy.

See "Advanced delivery actions that Managed Software Delivery can perform" on page 97.

The software that you deliver in this way must be defined as a software resource in the Software Catalog. If the software is not defined, contact an administrator who can edit the Software Catalog.

For more information, see the topics about the Software Catalog in the *Symantec Management Platform Help*.

If you need to perform a quick delivery of a single software resource, use Quick Delivery instead of Managed Software Delivery.

See "About quick delivery of a single software resource" on page 131.

Advanced delivery actions that Managed Software Delivery can perform

Managed Software Delivery is a policy-based delivery method that lets you respond to an assortment of advanced delivery requirements. A single Managed Software Delivery policy can perform multiple delivery actions.

See "About advanced software deliveries" on page 96.

Table 6-1 Advanced delivery actions that Managed Software Delivery can perform

Delivery action	Description
Deliver software	In its simplest form, Managed Software Delivery delivers a single software resource with its associated package and command line. It downloads the software and installs it on the managed computer according to a defined schedule. It does not perform a compliance check and it always considers the computer to be compliant.
Perform the delivery on a recurring schedule	You can set the Managed Software Delivery schedule to repeat daily, weekly, monthly, or yearly. The most common use of a recurring delivery is to check and remediate software on the client computer.
Check and remediate software on the client computer	Managed Software Delivery installs the software to a specific known state on the client computer. On a recurring basis, Managed Software Delivery can perform a compliance check to verify that the state is maintained. If the state of the software is out of compliance, Managed Software Delivery performs a remediation to restore the correct state. See "About policy applicability, compliance, and remediation" on page 102.
Deliver software dependencies to the client computer as needed	Managed Software Delivery checks the client computer for the dependencies of a software resource that it delivers. When a client computer does not contain the dependency software, Managed Software Delivery can perform either of the following actions: ■ Trigger a compliance failure and stop the delivery. ■ Perform a remediation by installing the missing dependency.

	Table 6-1	Advanced delivery actions that Managed Software Delivery can perform *(continued)*

Delivery action	Description
Detect supersedence associations on the client computer	When you create a Managed Software Delivery policy for a software resource that supersedes other software, you can set supersedence options. These options determine whether Managed Software Delivery replaces the superseded software. Managed Software Delivery's support of supersedence associations makes it easy to deliver software upgrades. For example, you want to distribute Norton AntiVirus 2008 to the managed computers that are running Norton AntiVirus 2007. If a managed computer contains Norton AntiVirus 2007, Managed Software Delivery can uninstall it and install Norton AntiVirus 2008. See "About installing software that replaces other software" on page 124.
Sequentially install multiple software resources and tasks	You can deliver multiple software resources and tasks with a single Managed Software Delivery policy. When Managed Software Delivery evaluates compliance for a group of software, only the software that is out of compliance is downloaded and installed. You can add any client tasks to the execution queue to perform custom operations before, during, or after the software remediation process. For example, you can add a task that performs a restart or runs a script. A client task is one that is defined in Notification Server and is intended to run on a client computer. See "About delivering multiple software resources and tasks" on page 125.
Install the software into a virtual software layer and perform multiple layer actions	(Windows only) Managed Software Delivery lets you install Windows-based software into a virtual software layer on a managed computer. The Software Virtualization agent must be installed on the managed computer; otherwise, the software is installed normally. You might virtualize the software for the following reasons: ■ To prevent conflicts on the managed computer when you deliver the software that conflicts with other software in your environment. When you install the software into a virtual layer, it does not conflict with other software even if the conflicting software is installed later. ■ To fix an application that is broken on the managed computer. You can quickly reset the broken application's layer to restore the application to its original configuration. See "Installing and managing a virtual software layer with a Managed Software Delivery policy" on page 230.
Execute software installations offline	In a Managed Software Delivery policy, you can set different schedules for the compliance check and the remediation (in this case, installation). The separate schedules allow for the offline execution of the Managed Software Delivery. When the compliance check determines that a remediation is required, the policy downloads the appropriate package. Remediation can occur even if the client computer is not connected to the server because the client computer already has the package that it needs. See "About deferring the execution of software remediation" on page 124.

See "Performing an advanced software delivery" on page 104.

About the execution of Managed Software Delivery policies

When a Managed Software Delivery policy runs on a managed computer, it performs a series of tasks that are grouped into the following phases:

■ Compliance
See Table 6-2.

■ Remediation
See Table 6-3.

When you schedule a Managed Software Delivery policy, you can assign different schedules for compliance and remediation. For example, you can schedule the compliance status to be reported during the day and the remediation to occur only during a maintenance window.

See "About policy applicability, compliance, and remediation" on page 102.

The ability to separate compliance and remediation also allows for the offline execution of Managed Software Delivery policies. When the compliance check determines that a remediation is required, the policy downloads the appropriate package. Remediation can occur even if the client computer is not connected to the server because the client computer already has the package that it needs.

See "About deferring the execution of software remediation" on page 124.

Table 6-2   Process for the compliance phase of Managed Software Delivery

Step	Action	Description
Step 1	Policy execution	Starts the policy's compliance process at the scheduled time on the client computer.
Step 2	Applicability check	(Windows only) Determines whether the client computer has the correct environment for an installation of the software. If the computer does not have the correct environment, the policy execution stops. The applicability check runs for each software resource in the Managed Software Delivery policy that is associated with an applicability rule.

Table 6-2   Process for the compliance phase of Managed Software Delivery
(continued)

Step	Action	Description
Step 3	Compliance check	Evaluates the software resource's unique identifier or detection rule to determine whether the software resource is installed on the client computer. The software resource's unique identifier is used when the software resource is not associated with a detection rule.
		The compliance check runs for each software resource in the Managed Software Delivery policy.
		This compliance check determines whether the software is in the correct state. The correct state of a software resource can mean that it is installed or that it is not installed.
		If all the software in the Managed Software Delivery policy is in the correct state, it is compliant. Therefore, remediation is not needed and the policy execution stops. If any or all of the software is not in the correct state, it is out of compliance. Therefore, remediation is required and the policy execution continues.

Table 6-2 Process for the compliance phase of Managed Software Delivery *(continued)*

Step	Action	Description
Step 4	Package download	Downloads the package for each software resource or task in the Managed Software Delivery policy that requires a package.
		The package download might not be required when the remediation action is to uninstall the software. In that case, the package download is skipped.
		The Managed Software Delivery policy downloads the package as follows:
		■ Download the package to the client computer.
		■ Create a snapshot of the package that is on the client computer and compare it to the snapshot on the package server. If the package is already on the client computer because of a recurring delivery or a delivery re-attempt, its existing snapshot is used for comparison.
		■ If the snapshots do not match, re-download the package. A mismatch can occur when some kind of interception has corrupted the package.
		When the package download is successful, the compliance process is finished and the policy is ready for the remediation process.

Table 6-3 Process for the remediation phase of Managed Software Delivery

Step	Action	Description
Step 1	Compliance check	Determines whether the software is installed on the client computer.
		This compliance check ensures that the software is still in the same state as it was during the compliance process. For example, if the remediation was scheduled to run later than the compliance process, the software might have been installed or uninstalled in the interim.
		If the remediation is still required, the process continues.

Table 6-3   Process for the remediation phase of Managed Software Delivery
(continued)

Step	Action	Description
Step 2	Remediation action	Installs, uninstalls, or performs any other remediation action that the software requires.
		If the Managed Software Delivery policy contains multiple software resources and tasks, they are executed in the order in which they appear in the policy.
		You can override the policy's remediation settings and schedule for individual software resources and tasks within the policy.
Step 3	Compliance check	Determines whether the software resource is installed on the client computer.
		This compliance check provides the information for reporting the results to Notification Server.
Step 4	Report to Notification Server	The Altiris Agent on the client computer reports the results of the Managed Software Delivery process to Notification Server. You can obtain information about the results from the compliance reports and the delivery reports in Software Management Solution.
		See "Running a Software Management Solution report" on page 83.

See "About advanced software deliveries" on page 96.

About policy applicability, compliance, and remediation

Managed Software Delivery can intelligently perform the applicability, compliance, and remediation actions that let you not only deliver software but also manage it. These actions ensure that you deliver the correct software to the correct computers and that the software remains in the correct state on the computers.

See "About the execution of Managed Software Delivery policies" on page 99.

When you schedule a Managed Software Delivery policy, you can assign different schedules for compliance and remediation. For example, you can schedule the

compliance process to occur during the day and the remediation to occur only during a maintenance window.

The compliance process and remediation process in Managed Software Delivery are especially effective when you schedule the policy to run on a recurring basis. The recurring policy ensures that the software remains in the correct state on the client computers.

Table 6-4   Applicability, compliance, and remediation actions

Action	Description
Applicability	(Windows only) The applicability check determines whether the client computer has the correct environment for an installation of the software. If the computer does not have the correct environment, the policy execution stops.
Compliance	A compliance check uses the software resource's unique identifier to determine whether the software is installed on the client computer. For Windows-based software, you can define a detection rule that contains additional information about the software and makes the detection process even more accurate. For more information, see the topics about detection and applicability rules in the *Symantec Management Platform Help*. The compliance check always checks for the presence of the software on the client computer. The check returns True if the software is installed and False if the software is not installed. The correct state of a software resource can mean that it is installed or that it is not installed. A Managed Software Delivery policy is considered compliant if all the software resources that it contains are in the correct state on the client computer. If the software is not in the correct state, it is considered to be out of compliance.

Table 6-4   Applicability, compliance, and remediation actions *(continued)*

Action	Description
Remediation	Remediation is the act of fixing any software that is out of compliance on the client computer. The nature of the remediation depends on the command-line action that the Managed Software Delivery policy performs. For example, an installation command runs when the compliance check returns False, and an uninstall command runs when the compliance check returns True.
	Examples of how the type of command line determines the remediation action are as follows:
	■ Installation command line
	You want to install Symantec AntiVirus 2008 on all managed computers that do not have it installed. You create the Managed Software Delivery policy and select an installation command line. When the policy runs, the compliance check determines whether Symantec AntiVirus 2008 is installed.
	If the software is installed, the check returns True. Because the correct state of the software is to be installed, the software is considered to be compliant and the policy execution stops. If the software is not installed, the check returns False. The software is out of compliance and must be installed.
	■ Uninstall command line
	You want to ensure that Solitaire is not installed on any managed computers. You create the Managed Software Delivery policy and select an uninstall command line. When the policy runs, the compliance check determines whether Solitaire is installed.
	If the software is installed, the check returns True. Because the correct state of the software is to be uninstalled, the software is out of compliance and must be uninstalled. If the software is not installed, the check returns False. The software is considered to be compliant and the policy execution stops.

See "About deferring the execution of software remediation" on page 124.

Performing an advanced software delivery

You can perform advanced software deliveries and manage the software that is installed on the managed computers.

See "About advanced software deliveries" on page 96.

The software that you deliver in this way must be defined as a software resource in the Software Catalog. If the software is not defined, contact an administrator who can edit the Software Catalog.

For more information, see the topics about the Software Catalog in the *Symantec Management Platform Help*.

Table 6-5 Process for performing advanced software deliveries

Step	Action	Description
Step 1	Create a Managed Software Delivery policy.	The options for creating a Managed Software Delivery policy are as follows: ■ Use the **Managed Software Delivery** wizard. The **Managed Software Delivery** wizard provides a quick way to create and schedule a policy for a single software resource and its dependency software. We recommend that you use the wizard because it can include any dependency software and warn you of software associations automatically. See "Creating a Managed Software Delivery policy with the Managed Software Delivery wizard" on page 106. ■ Create the policy without the wizard. Use this method to create a Managed Software Delivery policy when you need to add multiple software resources and tasks or override the default settings. You also can publish the policy to the **Software Portal**. However, you must add any dependency software or determine software associations yourself. You can accomplish the same goals by editing a policy that you created with the wizard. See "Creating a Managed Software Delivery policy" on page 110.
Step 2	(Optional) Edit the Managed Software Delivery policy.	You can edit the Managed Software Delivery policy to change or add functionality as follows: ■ Add software resources or tasks and arrange the order in which they run. ■ Change the settings for the entire policy. ■ Change the settings for specific software resources and tasks. ■ Edit the schedule or the destinations. See "Editing a Managed Software Delivery policy" on page 113.
Step 3	Select the delivery destinations.	Select the managed computers to deliver to. See "About the destinations for a Managed Software Delivery policy" on page 114. When you use the **Managed Software Delivery** wizard to create the policy, you select the destinations during the wizard.

	Table 6-5	Process for performing advanced software deliveries *(continued)*
Step	**Action**	**Description**
Step 4	Schedule the policy.	Define the schedule on which a Managed Software Delivery policy runs. You schedule the compliance check and the remediation check separately.
		See "Schedule settings for Managed Software Delivery" on page 55.
		When you use the **Managed Software Delivery** wizard to create the policy, you can define the schedule during the wizard.
Step 5	After the policy runs, view reports.	The Software Management reports let you monitor the software deliveries.
		The delivery reports provide information about the status of the software downloads and executions. For example, the software downloads for each computer, including the status and the download date. The compliance reports provide information about the compliance actions and the remediation actions.
		See "Running a Software Management Solution report" on page 83.

Creating a Managed Software Delivery policy with the Managed Software Delivery wizard

You can perform one or more advanced software delivery actions with a single Managed Software Delivery policy. Creating a Managed Software Delivery policy is the first step in performing an advanced software delivery.

See "Performing an advanced software delivery" on page 104.

See "About advanced software deliveries" on page 96.

The **Managed Software Delivery** wizard provides a quick way to create and schedule a policy for a single software resource and its dependency software. We recommend that you use the wizard because it can include any dependency software and warn you of software associations.

When you create a Managed Software Delivery policy with the **Managed Software Delivery** wizard, the policy is enabled automatically. If you do not want the policy to be available to managed computers immediately, edit the policy and disable it. You also might edit the policy to add information about what to deliver.

See "Editing a Managed Software Delivery policy" on page 113.

The software that you deliver in this way must be defined as a software resource in the Software Catalog. If the software resource is not defined, contact an administrator who can edit the Software Catalog.

You can run the **Managed Software Delivery** wizard from the **Software Catalog** view or from other areas of the **Symantec Management Console**. Your point of entry into the **Managed Software Delivery** wizard determines the amount of default information that is populated.

Create the policy without the wizard if you need to do any of the following things:

- Add multiple software resources and tasks.

- Override the default settings.

- (Windows and Mac OS only) Add the policy to the **Software Portal**.

See "Creating a Managed Software Delivery policy" on page 110.

To create a Managed Software Delivery policy with the Managed Software Delivery wizard

1   In the **Symantec Management Console**, on the **Manage** menu, click **Software**.

2   In the left pane, under **Software**, click the **Software Catalog** folder or expand it and select a subfolder.

3   In the right pane, on the Software Catalog page, right-click a software resource and click **Actions > Managed Software Delivery**.

4   In the **Managed Software Delivery** wizard, on the **Select software resource** page, specify the software to deliver and other delivery options and then click **Next**.

    See "Select software resource page" on page 108.

5   On the **Select destinations** page, specify the destinations to deliver the software to and then click **Next**.

    See "About the destinations for a Managed Software Delivery policy" on page 114.

6   On the **Schedule delivery** page, define the schedule for running the Managed Software Delivery and then click **Next**.

    See "Schedule settings for Managed Software Delivery" on page 55.

7   (Optional) On the **Specify dependencies and updates** page, select any dependencies, updates, or service packs that are defined for this software resource and then click **Next**.

Dependencies	Check **Verify dependencies** and select the check box for each dependency to include.
Updates or service packs	Select the check box for each update or each service pack to include.

8   To complete the wizard, click **Deliver Software**.

See "About the execution of Managed Software Delivery policies" on page 99.

Select software resource page

This page lets you specify the software to deliver and the options for its delivery. This page appears in the **Managed Software Delivery** wizard.

See "Creating a Managed Software Delivery policy with the Managed Software Delivery wizard" on page 106.

Table 6-6   Options on the **Select software resource** page

Option	Description
Software	Lets you select the software resource to deliver. If you started Managed Software Delivery from the Software Catalog, the software resource that you selected in the catalog appears.
	You can use the **Select software** option to select a software resource if one does not appear by default or to select a different software resource.

Options on the **Select software resource** page *(continued)*

Option	Description
Command line	Lets you select the command line to run. This list contains all the command lines that are defined for this software resource. You can select a command line other than the default command line that appears.
	A policy that contains a custom type command line does not perform an applicability check or compliance check. Those checks are valid only when the type of action that the command line performs is known. Currently, the applicability check and compliance check are run with installation and uninstall command lines only.
	The additional options for selecting a command line are as follows:
	■ Omit the command line if the package does not require one. For example, if the package is a Word template that is placed in a directory on the client computer but does not require installation. ■ Edit an existing command line before you select it. ■ Create a new command line. For more information, see the topics about adding and editing command lines in the *Symantec Management Platform Help*.
	Warning: Any additions or changes that you make to the command lines here are applied to the software resource in the Software Catalog. Those changes affect any other policies that use the changed command line.
Package	Lets you select a package to download if the command line requires a package. The list contains all the packages that are associated with this software resource. The package that is defined in the command line is the default.
	You can omit the package if the command line does not require one. For example, if the command line uninstalls a package that is already on the client computer, it can use the package ID.
Automatically upgrade software that has been superseded by this software	Uninstalls and replaces the software that this software supersedes. Select this option when a software upgrade requires the earlier version of the software to be uninstalled instead of updated.
	This option is available only if you meet the following conditions:
	■ You select a software resource that supersedes other software ■ You select an installation command line
	For this option to work, the superseded software resource must have a default uninstall command line.
	Warning: When you uninstall software from a client computer, you can break other applications that depend on the uninstalled software.
	See "About installing software that replaces other software" on page 124.

<div align="center">

Table 6-6   Options on the **Select software resource** page *(continued)*

</div>

Option	Description
Do not install if a newer version of this software is already installed	Does not install the software if a newer version of this software is already installed on the client computer. For example, use this option if you do not want to install Norton AntiVirus 2008 on a computer that has Norton AntiVirus 2009. This option is available only if you meet the following conditions: ■ You select a software resource that other software supersedes. ■ You select an installation command line. **Warning:** If you try to install when a newer version is installed, and both versions cannot coexist on the same computer, the installation fails. See "About installing software that replaces other software" on page 124.
Install this policy's software into a virtual layer	(Windows only) Installs Windows-based software into a virtual software layer on a managed computer. The Software Virtualization agent must be installed on the managed computer; otherwise, the software is installed normally. See "Methods for virtualizing software" on page 219.
Layer Name	Lets you type the name of the virtual software layer into which this software is installed. The layer's GUID is assigned automatically. If you do not provide a layer name, the layer name defaults to the installation file name plus the command-line name.

Creating a Managed Software Delivery policy

A single Managed Software Delivery policy lets you perform one or more advanced software delivery actions. Creating a Managed Software Delivery policy is the first step in performing an advanced software delivery.

See "Performing an advanced software delivery" on page 104.

See "About advanced software deliveries" on page 96.

When you create a Managed Software Delivery policy, you can add multiple software resources and tasks or override the default settings. You also can publish the policy to the **Software Portal** for Windows and Mac client computers.

The software that you deliver in this way must be defined as a software resource in the Software Catalog. If the software resource is not defined, contact an administrator who can edit the Software Catalog.

If you need to quickly create and schedule a Managed Software Delivery policy, use the **Managed Software Delivery** wizard instead.

See "Creating a Managed Software Delivery policy with the Managed Software Delivery wizard" on page 106.

To create a Managed Software Delivery policy

1   In the **Symantec Management Console**, on the **Manage** menu, click **Policies**.

2   In the left pane, under **Policies**, click **Software > All Managed Software Delivery**.

3   In the right pane, on the **Managed Software Delivery** page, click **Add**.

4   In the upper left of the **New Managed Software Delivery** page, click and type over the following text:

New Managed Software Delivery	Type a name to identify this policy in any list of policies. Make the name descriptive enough for others to easily identify this policy and the software that it delivers or manages.
Add description	Type a description to provide further information about this policy. Do not include critical information in the description because it is not intended to appear in all the lists that contain the name.

5   On the same page, under **Policy Rules/Actions**, on the **Software** tab, click **Add**. On the **Add** menu, select one of the following options:

   ■ **Software resource**
     Lets you select from the deliverable software resources that are defined in the Software Catalog.

   ■ **Task**
     Lets you select from the client tasks that are defined in Notification Server.

6   Repeat step 5 for each software resource and task that you want to add.

7   (Optional) To change the default settings for this policy, under **Policy Rules/Actions**, enter additional settings on the **Policy settings** tab and the **Software Publishing** tab.

   See "Policy Rules/Actions section" on page 115.

8   (Optional) To change the default settings for a specific software resource or task, under **Policy Rules/Actions**, click the software resource or task. At the right of the page, do any of the following:

   ■ Change any of the options that are available on the page.

   ■ In a software resource, click **Advanced options** to display and change additional settings.

See "Advanced options in Managed Software Delivery policies" on page 69.

- In a task, click **Show Task** to display and change additional settings.
  See "Editing a task in Software Management Solution" on page 143.

9   Expand the **Applied to** section to add or change the delivery destinations.

See "About the destinations for a Managed Software Delivery policy" on page 114.

10 Expand the **Schedule** section to define the delivery schedule.

See "Schedule settings for Managed Software Delivery" on page 55.

11 Turn on the policy.

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

12 At the bottom of the page, click **Save changes**.

About editing a Managed Software Delivery policy

You can edit a Managed Software Delivery policy for any of the following reasons:

To add software resources	You can add any software resources to the execution queue.
	Examples are as follows:
	■ You can deliver multiple software resources that comprise a set of base applications.
	■ As you discover unauthorized software on client computers, you can add that software to a recurring uninstallation policy to keep it uninstalled.
	■ If the software in the policy requires other software, you can add the dependency software so that all the software is installed together.
	When you create a Managed Software Delivery policy with the **Managed Software Delivery** wizard, the dependencies are added automatically.
To add tasks	You can add any client task to the execution queue to perform custom operations. For example, you can add a task that performs a restart or runs a script. A client task is one that is defined in Notification Server and is intended to run on a client computer.
To rearrange the order of the software resources and tasks	When you add multiple software resources and tasks to a Managed Software Delivery policy, you can set the sequence in which they run.

To override the default policy settings	Every new Managed Software Delivery policy inherits the default settings that are defined for Managed Software Delivery. You can override the default settings for the entire policy. See "Configuring the default settings for Managed Software Delivery" on page 54.
To override the policy settings for specific software resources and tasks	The software resources and tasks that you add to the policy inherit settings from the policy. You can edit the settings for individual software resources and tasks. For example, although the policy remediation runs at the next maintenance window, you can choose to remediate a specific task immediately.
To edit the destinations	When new managed computers are added to your organization, you can add them to an existing Managed Software Delivery policy.
To edit the schedule	You can add schedules for the compliance check or change the remediation option.

When you change a Managed Software Delivery policy, the updated policy is sent to the client computers, including those on which the policy has run.

See "Editing a Managed Software Delivery policy" on page 113.

Editing a Managed Software Delivery policy

You can edit any existing Managed Software Delivery policy.

See "About editing a Managed Software Delivery policy" on page 112.

When you change a Managed Software Delivery policy, the updated policy is sent to the client computers, including those on which the policy has run.

To edit a Managed Software Delivery policy

1   In the **Symantec Management Console**, on the **Manage** menu, click **Policies**.

2   In the left pane, under **Policies**, click **Software > Managed Software Delivery**.

3   In the right pane, double-click a Managed Software Delivery policy.

4   On the policy page, do any of the following:

  ■ Change the policy's name or description. Click either one in the upper left of the page and type over the existing text.
    Make the name descriptive enough for others to easily identify this policy and the software that it delivers or manages.

Do not include critical information in the description because it is not intended to appear in all the lists that contain the name.

■ Expand the **Policy Rules/Actions** section to add software resources and tasks and to change the policy settings.
See "Policy Rules/Actions section" on page 115.

■ Expand the **Applied to** section to add or change the delivery destinations.
See "About the destinations for a Managed Software Delivery policy" on page 114.

■ Expand the **Schedule** section to add or change the delivery schedule.
See "Schedule settings for Managed Software Delivery" on page 55.

5   On the policy page, turn on the policy or turn off the policy as needed.

At the upper right of the page, click the colored circle and then click **On** or **Off**.

6   When you finish editing the Managed Software Delivery policy, click **Save changes**.

Select Software dialog box

This dialog box lets you select a software resource to act upon. This dialog box can appear in multiple areas of the product that require a software resource to be specified. For example, it appears when you add a software resource to a Managed Software Delivery policy.

About the destinations for a Managed Software Delivery policy

You can apply a Managed Software Delivery policy to selected resource targets, computers, users, and resources. You can use any combination of these options to define the computers to which the policy applies.

When you create or edit a Managed Software Delivery policy, the **Applied to** section or the **Select destinations** page appears. You use those pages to specify the destinations to deliver the software to.

For more information, see the topics about applying a policy to targets, computers, resources, and users in the *Symantec Management Platform Help*.

Managed Software Delivery supports user-based policies by letting you specify users and user groups as policy targets. This feature lets you deliver software to any managed computer that a specific user logs on to. When the user logs on to

a computer, the Altiris Agent refreshes any policy that targets that user. The policy runs on that computer according to the schedule that you defined for it.

For more information, see the topics about user-based policies in the *Symantec Management Platform Help*.

See "Creating a Managed Software Delivery policy with the Managed Software Delivery wizard" on page 106.

See "Creating a Managed Software Delivery policy" on page 110.

See "Editing a Managed Software Delivery policy" on page 113.

Policy Rules/Actions section

This section appears when you create or edit a Managed Software Delivery policy. It lets you add software resources and tasks to the policy and change the settings for the policy.

See "Creating a Managed Software Delivery policy" on page 110.

See "Editing a Managed Software Delivery policy" on page 113.

Table 6-7   Tabs in the **Policy Rules/Actions** section

Tab	Description
Software tab	Lets you define the software and tasks to deliver and set the options for each software resource and task.
	See "Policy Rules/Actions: Software tab" on page 115.
Policy settings tab	Lets you change the default settings for the Managed Software Delivery policy.
	See "Policy Rules/Actions: Policy settings tab" on page 119.
Software Publishing tab	(Windows and Mac OS only) Lets you publish the Managed Software Delivery policy to the **Software Portal**.
	See "Software Publishing tab" on page 120.
	See "Adding a Managed Software Delivery policy to the Software Portal" on page 179.

Policy Rules/Actions: Software tab

This tab lets you define the software to deliver. You can select a single software resource or you can select multiple software resources and tasks to create a

sequential delivery policy. This tab also lets you set options for the individual software resources and tasks.

This tab appears when you create or edit a Managed Software Delivery policy.

See "Creating a Managed Software Delivery policy" on page 110.

See "Editing a Managed Software Delivery policy" on page 113.

This tab contains the following sections:

Left pane	Displays the sequence of software resources and task that this policy delivers. You can add software resources and tasks.
	See Table 6-8.
	When you click a specific software resource or task, its settings appear in the right pane.
Right pane	Lets you override the policy settings for the specific policy or task. The settings that appear differ depending on whether you click a software resource or a task.
	See Table 6-9.
	See Table 6-10.

Table 6-8   Options for adding software resources and tasks

Option	Description
Add	Lets you add a software resource or a task to the delivery sequence.
	See "Delivering multiple software resources and tasks sequentially" on page 126.
Up and down arrow symbols	Let you arrange the sequence in which the software resources and tasks are run. Plan the sequence before you enable the policy.
	If you change the sequence after the policy runs, you trigger the following actions:
	■ The policy is updated on the client computers the next time it is requested.
	■ The policy's schedule is reset so that it runs again, even if you originally scheduled the policy to run one time only.

Table 6-9   Settings for software resources

Option	Description
Perform software compliance check using	Displays a link that indicates the software resource whose detection rule is used for the compliance check. You can click the link to view and edit the rule.
	For more information, see the topics about editing inventory rules and about detection and applicability rules in the *Symantec Management Platform Help*.

Table 6-9   Settings for software resources *(continued)*

Option	Description
Command line	Lets you select the command line to run. This list contains all the command lines that are defined for the software resource that you selected. You can select a command line other than the default command line that appears.
	You can omit the command line if the package does not require one.
Package	Lets you select the package to download if the command line requires a package. The list contains all the packages that are associated with this software resource. The package that is defined in the command line is the default.
	You can omit the package if the command line does not require one. For example, if the command line uninstalls a package that is already on the client computer.
Override policy remediation schedule	Set the remediation of this software resource to occur on a different schedule than the policy itself.
	You can use this option to run one of the software resources or tasks during a maintenance window because it affects the system resources.
	For example, you create a Managed Software Delivery policy to roll out a new virus checker application and then perform a full system scan. Because the scan can take the entire maintenance window to run, you roll out the software silently during the day. As a result, the full maintenance window is available for the scan task to run.
Advanced options	Change the settings for this software resource only. For example, you might download this software's package to a different location or allow the user to interact with this software's installation but not others.
	See "Advanced options for tasks in Software Management Solution" on page 70.
Automatically upgrade software that has been superseded by this software	Uninstalls and replaces the software that this software supersedes. Select this option when a software upgrade requires the earlier version of the software to be uninstalled instead of updated.
	This option is available only if you meet the following conditions:
	■ You select a software resource that supersedes other software.
	■ You select an installation command line.
	For this option to work, the superseded software resource must have a default uninstall command line.
	Warning: When you uninstall software from a client computer, you can break other applications that depend on the uninstalled software.
	See "About installing software that replaces other software" on page 124.

Table 6-9   Settings for software resources *(continued)*

Option	Description
Do not install if a newer version of this software is already installed	Does not install the software if a newer version of this software is already installed on the client computer. For example, use this option if you do not want to install Norton AntiVirus 2008 on a computer that has Norton AntiVirus 2009.
	This option is available only if you meet the following conditions:
	■ You select a software resource that other software supersedes.
	■ You select an installation command line.
	Warning: If you try to install when a newer version is installed, and both versions cannot coexist on the same computer, the installation fails.
	See "About installing software that replaces other software" on page 124.

Table 6-10   Settings for tasks

Option	Description
Override the policy settings for this task	Enables the remaining options in this section and lets you configure settings for delivering this specific task.
Upon failure the Managed Delivery will	Defines whether the task aborts, continues, or restarts when it fails.
	When you create a Managed Software Delivery policy, this setting is the same for each task that the policy contains. You can edit the policy to override this setting for each ask. For example, if the execution of the first task fails, you can run subsequent software resource and tasks. Conversely, if one execution in the sequence fails, you can abort the remaining items in the sequence.
Terminate after	Lets you define the amount of time to wait before the task terminates if it stops responding.
Max retries	Defines the number of times that the task retries when it fails.
Choose when to remediate when compliance fails	Specify when to perform any remediation action that is defined for this task.
	The options are as follows:
	■ **Immediately**
	■ **At next maintenance window**
	■ **Don't run remediation** Lets you run a task without performing the remediation. For example, you might want to perform an applicability check or a compliance check to determine if a certain configuration exists. A report of the results of the check might be all you need, or you might perform some action other than installing or uninstalling software.

Table 6-10   Settings for tasks *(continued)*

Option	Description
Show Task	Opens the task editing dialog box so you can view or edit the task.
	When you edit the task itself instead of its settings, any other instances of that task are also changed. For example, you create a Package Delivery task to install an FTP client and you add that task to several Managed Software Delivery policies. If you change that task in one Managed Software Delivery policy, the change affects that task as well as all the policies that contain it.

Policy Rules/Actions: Policy settings tab

This tab lets you change the settings for a Managed Software Delivery policy.

Some options on the **Policy Settings** tab apply to Windows operating systems only and are noted as such.

Table 6-11   Options on the **Policy Settings** tab

Option	Description
Display name	Lets you define the name that appears in the Altiris Agent for this policy. The default name is New Managed Software Delivery.
	Make the name descriptive enough for users to easily identify this software.
Display description	Lets you type a description to further identify this software and make it more recognizable on the Altiris Agent.
Install this policy's software into a virtual software layer	(Windows only) Installs Windows-based software into a virtual software layer on a managed computer. The Software Virtualization agent must be installed on the managed computer; otherwise, the software is installed normally.
	See "Methods for virtualizing software" on page 219.
Layer Name	Lets you type the name of the virtual software layer into which this software is installed. The layer's GUID is assigned automatically.
	If you do not provide a layer name, the layer name defaults to the installation file name plus the command-line name.
Allow user to turn on policy from the Altiris Agent	(Windows only) Lets the user run the policy by clicking the policy in the Altiris Agent. The user can also choose not to run the policy.
	The policy's remediation options override this setting and its related settings. For example, if the remediation is scheduled to occur at the next maintenance window, the user cannot run the remediation immediately.

Table 6-11   Options on the **Policy Settings** tab *(continued)*

Option	Description
User must turn on from Altiris Agent	(Windows only) Requires the user to run the policy. If you select this option, the policy never runs automatically.
	This check box is available only if you checked the following check box: **Allow user to turn on policy from the Altiris Agent**.
	The user can run the policy by clicking it on the **Software Delivery** tab that is on the Altiris Agent.
	The user can also run the policy by clicking **Start Task Now** on the **New Software is Available** dialog box, if the following conditions are met:
	■ If you check **Prompt user when this policy is available on their computer** for the policy. ■ If the **Show popup notifications** check box is checked on the client computer's Altiris Agent.
Prompt user when this policy is available	(Windows only) Displays a message to notify the user that new software is available. When the user clicks the message, the **New Software is Available** dialog box opens. The user can start, dismiss, or defer the policy. If you do not choose to prompt the user, the **New Software is Available** dialog box does not appear.
	This check box is available only if you checked the following check box: **Allow user to turn on policy from the Altiris Agent**.
	The **New Software is Available** dialog box appears only if the **Show popup notifications** check box is checked on the client computer's Altiris Agent.
Enable verbose reporting of status events	Records the details of policy status, package download, and execution events and posts them to the Notification Server computer.

Software Publishing tab

(Windows and Mac OS only)

This tab lets you publish a software resource or a Managed Software Delivery policy to the **Software Portal**. By publishing software to the **Software Portal**, you make it available for users to request.

The **Software Publishing** tab appears in multiple places in the **Symantec Management Console** as follows:

■ On the software resource page that appears when a software resource is edited. Access the tab from this location to publish the software resource to the **Software Portal**.

■ Under the **Policy Rules/Actions** section that appears when you create or edit a Managed Software Delivery policy. Access the tab from this location to publish the Managed Software Delivery policy to the **Software Portal**.

Table 6-12   Options on the **Software Publishing** tab

Option	Description
Publish to Software Portal	Enables the remaining options on this tab so that you can configure the settings for publishing the software resource or Managed Software Delivery policy.
Software Name	Identifies this software in any list of software in the **Software Portal**. Make the name descriptive enough for users to easily identify this software. Follow your organization's standards for naming software, if any.
Description	Lets you type a description to further identify this software and make it more recognizable.
Add User	Lets you add a user or a group of users to the list of users who have permission to request this software resource. See "Add User dialog box" on page 180.
Approved	Pre-approves the software resource for this user. When this user requests this software resource, a software delivery task is created to install it. No further action is required. This setting applies to the user or group that is selected in the list to the left.
Requires Approval	Specifies that a manager or administrator must review and approve any request for this software by this user. This setting applies to the user or group that is selected in the list to the left.
Recommended	Makes this software resource appear in this user's **Software Portal** display by default. This setting applies to the user or group that is selected in the list to the left.

Select Task dialog box

This dialog box lets you select one or more tasks to act upon. This dialog box can appear in multiple areas of the product that require a task to be specified. For example, it can appear when you add a task to an existing Managed Software Delivery policy in Software Management Solution.

About software delivery deferral options for the user

(Windows only)

You can give the user some control over when to execute a software delivery and when to restart or log off after the execution. In Software Management Solution, these options are available for Managed Software Delivery policies only.

Table 6-13   Software delivery deferral options for the user

User's option	Description	Location of the settings	Settings
Defer the execution of a Managed Software Delivery policy	The ability to defer the policy execution is useful when you deliver software during working hours. The user can dismiss the **Starting Task** dialog box but cannot cancel the policy altogether. The deferral lets the user save work and close any open files or programs.	The settings for this option appear in the following places: ■ On the **Managed Delivery Settings** page, on the **Run** tab, under **User run conditions**. ■ In an existing Managed Software Delivery policy, in the **Advanced options** dialog box, on the **Run** tab, under **User run conditions**. See "User run conditions settings in Software Management Solution" on page 63.	The required settings are as follows: ■ **Prompt user before running** ■ **Allow user to defer up to a total of** Lets you allow the user to defer running the policy up to the maximum amount of time that you select.

Table 6-13 Software delivery deferral options for the user *(continued)*

User's option	Description	Location of the settings	Settings
Choose when to run the policy or choose not to run the policy	You might let the user control the execution when the software is optional or is not critical for that user.	The settings for this option appear in the following places: ■ On the **Managed Delivery Settings** page, on the **Run** tab, under **User run conditions**. See "User run conditions settings in Software Management Solution" on page 63. ■ In an existing Managed Software Delivery policy, on the **Policy settings** tab. See "Policy Rules/Actions: Policy settings tab" on page 119.	The settings are as follows: ■ **Allow user to turn on policy from the Altiris Agent** ■ (Optional) **User must turn on from Altiris Agent** **Note:** The policy's remediation options override this setting and its related settings.
Defer a restart or a logoff	You can set a Managed Software Delivery policy to require a restart or a logoff after the task finishes. Because the restarts and logoffs can cause a user to lose unsaved work, you can let the user defer them.	The settings for this option appear in the following places: ■ On the **Managed Delivery Settings** page, on the **Run** tab, under **Results-based actions**. ■ In an existing Managed Software Delivery policy, in the **Advanced options** dialog box, on the Results-based actions tab. See "Run settings in Software Management Solution" on page 61.	The required settings are as follows: ■ **Upon success run** Lets you specify whether to require a restart or a logoff after the policy runs successfully. ■ **Allow user to defer action up to** Lets you allow the user to defer the post-execution action up to the maximum amount of time that you select.

About deferring the execution of software remediation

In a Managed Software Delivery policy, you can set different schedules for the compliance check and the remediation. You can configure these options in the default settings for all Managed Software Delivery policies. You can also change the default settings for specific Managed Software Deliveries.

During a Managed Software Delivery, the package download occurs during the compliance check and the program execution occurs during the remediation. When you schedule a Managed Software Delivery policy, you define the schedule for the compliance check and then select an option to schedule the remediation.

See "About the execution of Managed Software Delivery policies" on page 99.

The separate schedules allow for the offline execution of the Managed Software Delivery. You can schedule an offline execution by selecting the option to perform the remediation during the next maintenance window.

For example, you support a large number of remote users who connect to your network a few times a week. You need to install a new application on all their computers and you want the installation to occur during a maintenance window. However, you cannot guarantee that the users are connected to the network when a maintenance window is scheduled. Therefore, you can create a Managed Software Delivery policy and schedule the compliance check to occur as soon as a user connects to your network. Then you schedule the remediation (installation) to occur during the next maintenance window. When a user connects to the network, the compliance check occurs and if a remediation is required, the package download occurs. During the maintenance window, the installation occurs on the user's computer. The installation can occur even if the client computer is not connected to the network, because the computer already has the package that it needs.

See "Schedule settings for Managed Software Delivery" on page 55.

See "About advanced software deliveries" on page 96.

About installing software that replaces other software

Managed Software Delivery can use the supersedence associations that are defined for software resources to install software that replaces other software. A supersedence association is one in which one software resource replaces another software resource.

Supersedence associations are supported in Managed Software Delivery installations only.

See "About advanced software deliveries" on page 96.

When you create a Managed Software Delivery policy for a software resource that has a supersedence association with other software, a message notifies you.

Depending on the nature of the association, your options are as follows:

The selected software supersedes other software	The policy can uninstall the superseded software from the client computer before the selected software is installed.
Other software supersedes the selected software	You can take either of the following steps: ■ Create the Managed Software Delivery policy for the superseding software instead and ensure that you distribute only the current version of the software. ■ Install the superseded software anyway. You can make the installation conditional by configuring it not to install the software if a newer version is already installed.

The supersedence settings appear in the following places:

■ In the **Managed Software Delivery** wizard, on the **Select software resource** page.
  See "Select software resource page" on page 108.

■ In the **Policy Rules/Actions** section that appears when you edit a Managed Software Delivery policy or create one without the **Managed Software Delivery** wizard.
  See "Policy Rules/Actions: Software tab" on page 115.

For more information, see the topics about supersedence and about associations between software resources in the *Symantec Management Platform Help*.

About delivering multiple software resources and tasks

You can deliver multiple software resources and tasks with a single Managed Software Delivery policy. When Managed Software Delivery evaluates compliance for a group of software, only the software that is out of compliance is downloaded and installed. You can add any client tasks to the execution queue to perform custom operations before, during, or after the software remediation process. A client task is one that is defined in Notification Server and is intended to run on a client computer.

For example, you can create a single Managed Software Delivery policy that performs the following actions:

- Run a task that uses a script to set a registry key on the managed computer.

- Determine whether the software resource or its dependencies are already installed.

- Install the software and any of its dependencies that are not already installed.

- Run a task that performs a restart.

- Install an additional software resource into a virtual layer because it is known to conflict with other software that might be on the managed computer.

- Run every week to determine whether the registry key is still correct and the software is still installed.

- Reset the registry key to the correct value if necessary.

- Reinstall any software that the compliance check determines is broken or not present.

The default settings for Managed Software Delivery determine what happens if the policy fails. Initially, this setting is the same for each software resource and task that the policy contains. You can edit the policy to override this setting for each software resource and task. For example, if a critical execution in the sequence fails, you can abort the remaining items in the sequence. Conversely, if a less-critical execution fails, you might decide to run the subsequent tasks anyway.

See "Delivering multiple software resources and tasks sequentially" on page 126.

Delivering multiple software resources and tasks sequentially

You can deliver multiple software resources and tasks with a single Managed Software Delivery policy. When Managed Software Delivery evaluates compliance for a group of software, only the software that is out of compliance is downloaded and installed. You can add any client task to the execution queue to perform custom operations before, during, or after the software remediation process. For example, you can add a task that performs a restart or runs a script.

See "About delivering multiple software resources and tasks" on page 125.

Table 6-14   Process for delivering multiple software resources and tasks

Step	Action	Description
Step 1	Create a Managed Software Delivery policy.	The options for creating a Managed Software Delivery policy are as follows: ■ Use the **Managed Software Delivery** wizard. The **Managed Software Delivery** wizard provides a quick way to create and schedule a policy for a single software resource and its dependency software. We recommend that you use the wizard because it can include any dependency software and warn you of software associations automatically. See "Creating a Managed Software Delivery policy with the Managed Software Delivery wizard" on page 106. ■ Create the policy without the wizard. Use this method to create a Managed Software Delivery policy when you need to add multiple software resources and tasks or override the default settings. You also can publish the policy to the **Software Portal**. However, you must add any dependency software or determine software associations yourself. See "Creating a Managed Software Delivery policy" on page 110.
Step 2	Select the delivery destinations.	Select the managed computers to deliver to. See "About the destinations for a Managed Software Delivery policy" on page 114. When you use the **Managed Software Delivery** wizard to create the policy, you select the destinations during the wizard.
Step 3	Schedule the policy.	Define the schedule for the entire policy. You can schedule the compliance check and the remediation separately. When you use the **Managed Software Delivery** wizard to create the policy, you can define the schedule during the wizard. See "Schedule settings for Managed Software Delivery" on page 55.
Step 4	Add the additional software resources and tasks to the policy.	You can add multiple software resources and tasks when you create the policy without the **Managed Software Delivery** wizard. When you use the **Managed Software Delivery** wizard to create the policy, you can select only one software resource. Edit the policy to add software and tasks. See "Policy Rules/Actions: Software tab" on page 115.
Step 5	Arrange the sequence in which the software resources and tasks are run.	Move the software resources and tasks up or down in the list to rearrange their order. Plan the sequence before you enable the policy. See "Policy Rules/Actions: Software tab" on page 115.

	Table 6-14	Process for delivering multiple software resources and tasks *(continued)*

Step	Action	Description
Step 6	(Optional) Change the settings for individual software resources or tasks.	When you add software resources and tasks to a Managed Software Delivery policy, they inherit the settings from the policy. You can change the settings for any specific software resource or task that is in the policy.
		The settings that you can change for a specific software resource or task include the remediation schedule, the download settings, and the run settings.
		See "Policy Rules/Actions: Software tab" on page 115.

About the status of Managed Software Delivery policies

The information in the Software Catalog lets Software Management Solution report the status of Managed Software Delivery policies with greater accuracy than other methods.

When a Managed Software Delivery policy completes an action on a client computer, it performs a compliance check to evaluate the success of the execution. The compliance check uses the software resource's unique identifier to determine whether that software is installed on a client computer. For Windows software, you can define a detection rule that contains additional information about the software and makes the detection process even more accurate. After the compliance check, the Managed Software Delivery policy reports the status information to Notification Server.

See "About policy applicability, compliance, and remediation" on page 102.

This method of determining a policy's success is more accurate than using the package's exit code. A package can return an exit code that indicates success when in fact, the delivery was completed but the installation was not successful.

For example, you can use a Package Delivery task to install an MSI package that contains a custom action. However, because the custom action is placed in the wrong section of the MSI, it is not installed on a Windows Vista computer. Even though the package is not installed, the package execution is reported as successful because the exit code is returned. If you use a Managed Software Delivery policy instead, the compliance check can determine that the package is not installed. Therefore, you get an accurate report of the delivery status.

See "Sources of status information in Software Management Solution" on page 79.

See "About the execution of Managed Software Delivery policies" on page 99.

Performing quick software deliveries

This chapter includes the following topics:

- About quick delivery of a single software resource

- Performing a quick delivery of a single software resource

- About the Quick Delivery wizard

- Creating a Quick Delivery task with the Quick Delivery wizard

- Software settings for Quick Delivery tasks

About quick delivery of a single software resource

You can perform a quick delivery of a single software resource that runs with minimum configuration. You can use the task-based Quick Delivery method to specify the software to deliver, the action to perform, and the computers to deliver to.

Because the software resources and the delivery settings are predefined, Quick Delivery makes it easy for administrators and non-administrators to deliver software. For example, help desk personnel can easily deliver hotfixes because all they have to do is select the correct hotfix from the Software Catalog. They do not need to know which package to select or how to create the command line.

Most organizations can use Quick Delivery for the majority of their software delivery needs. Quick Delivery helps you reduce the amount of time that you spend on routine deliveries so that you can devote more time to advanced activities.

See "Performing a quick delivery of a single software resource" on page 132.

The software that you deliver in this way must be defined as a deliverable software resource in the Software Catalog. If the software is not defined, contact an administrator who can edit the Software Catalog.

After the initial instance of a Quick Delivery task runs, you can edit and rerun it. For example, you can deliver the software to different computers or run a different command line on the same computers. You can also edit the delivery settings for the task. For example, you can change the user credentials under which the task runs.

See "Editing a task in Software Management Solution" on page 143.

If you need to perform compliance checks or other advanced delivery activities, use Managed Software Delivery instead of Quick Delivery.

See "About advanced software deliveries" on page 96.

Performing a quick delivery of a single software resource

You can deliver software without the need to know which package to select or how to create the command line.

See "About quick delivery of a single software resource" on page 131.

The software that you deliver in this way must be defined as a deliverable software resource in the Software Catalog. It must also have at least one command line.

Table 7-1   Process for performing a quick delivery of a single software resource

Step	Action	Description
Step 1	Create a Quick Delivery task.	The options for creating a Quick Delivery task are as follows: ■ Use the **Quick Delivery** wizard. The **Quick Delivery** wizard is the fastest and easiest way to create and run a Quick Delivery task with minimum configuration. See "Creating a Quick Delivery task with the Quick Delivery wizard" on page 134. ■ Create the task without the wizard. Use this method when you need to change the task's default settings or run the task on a specific schedule. You can accomplish the same goals by editing a task that you created with the wizard. See "Creating a task in Software Management Solution" on page 142.

Table 7-1   Process for performing a quick delivery of a single software resource
                   (continued)

Step	Action	Description
Step 2	(Optional) Change the task settings.	Every task inherits the default settings that control how the task runs. You can override the default settings for a particular task. See "Advanced options for tasks in Software Management Solution" on page 70.
Step 3	Schedule the task and select the delivery destinations.	When you use the **Quick Delivery** wizard to create the task, you select the destinations during the wizard. Those destinations apply to that instance of the task only. You do not have to schedule the task because it runs as soon as possible. When you edit the task or create it without the wizard, you define the schedule and the delivery destinations every time you run the task. Your options for scheduling the task are as follows: ■ Run the task now. This option runs the task as soon as possible, unless it must wait for a maintenance window. ■ Schedule the task to run at a specific time. See "Scheduling a task and selecting computers in Software Management Solution" on page 144.
Step 4	After the task runs, view the reports.	The Software Management reports let you monitor the software deliveries. The delivery reports provide information about the status of the software downloads and executions. For example, the software downloads for each computer, including the status and the download date. See "Running a Software Management Solution report" on page 83.

About the Quick Delivery wizard

The **Quick Delivery** wizard is the fastest and easiest way to create and run a Quick Delivery task with minimum configuration. During the wizard, you specify the software resource to deliver, the action to perform, and the destinations to deliver to. The resulting Quick Delivery task runs as soon as possible without further configuring or scheduling. We recommend that non-administrators use the **Quick Delivery** wizard because it provides the fewest options and therefore the fewest opportunities for errors.

Warning: When a Quick Delivery task runs automatically, you can recall, stop, or disable it only if the task needs to wait for a maintenance window.

The advantages of using the **Quick Delivery** wizard are as follows:

- It speeds the task creation.

- It does not let non-administrators change the delivery settings.
  In most cases, it is important to prevent non-administrators from changing the delivery settings when they deliver software.

- It sets the task to run as soon as possible.

When you create a Quick Delivery task without the wizard, it does not run automatically. You must run it or schedule it.

See "Creating a Quick Delivery task with the Quick Delivery wizard" on page 134.

See "About quick delivery of a single software resource" on page 131.

Creating a Quick Delivery task with the Quick Delivery wizard

A Quick Delivery task lets you deliver software without the need to know which package to select or how to create the command line. Creating a Quick Delivery task is the first step in performing a quick delivery of a single software resource. The **Quick Delivery** wizard is the fastest and easiest way to create and run a Quick Delivery task with minimum configuration.

See "Performing a quick delivery of a single software resource" on page 132.

See "About the Quick Delivery wizard" on page 133.

The software that you deliver in this way must be defined as a deliverable software resource in the Software Catalog.

When you run the **Quick Delivery** wizard from the **Software Catalog** view, it populates the most default information. However, you can run the **Quick Delivery** wizard from other areas of the **Symantec Management Console**. Your point of entry into the **Quick Delivery** wizard determines the amount of default information that is populated.

If you need to change the task's default settings or run the task on a specific schedule, create the task without the **Quick Delivery** wizard.

See "Creating a task in Software Management Solution" on page 142.

To create a Quick Delivery task with the Quick Delivery wizard

1   In the **Symantec Management Console**, on the **Manage** menu, click **Software**.

2   In the left pane, under **Software**, click the **Software Catalog** folder or expand it and select a subfolder.

3   In the right pane, on the **Software Catalog** page, select a deliverable software resource.

4   Click **Actions**.

5   On the **Actions** menu, click **Actions > Quick Delivery Task**.

6   In the **Quick Delivery Task** dialog box, specify the following items:

   ■   The software resource to deliver

   ■   The command line to run
       The list contains the names of the command lines that are defined for the software resource.

   ■   Whether to accept the maintenance windows

   ■   The destinations to deliver the software resource to

   See "Software settings for Quick Delivery tasks" on page 135.

7   Click **OK**.

See "About quick delivery of a single software resource" on page 131.

Software settings for Quick Delivery tasks

This section lets you define or edit the details of a Quick Delivery task, including the software that it delivers.

See "About quick delivery of a single software resource" on page 131.

When you edit a Quick Delivery task, the **Task Status** section appears beneath the **Software settings** section on the page. Under the **Task Status** section, you can schedule the task, select the destination computers, and view the status of the task.

See "Scheduling a task and selecting computers in Software Management Solution" on page 144.

Table 7-2 Software settings for Quick Delivery tasks

Option	Description
Name When you edit a task, this option is not labeled. In the upper left of the task page, you can click the existing name to edit it.	Identifies this task in any list of tasks throughout the product. Make the name descriptive enough for others to easily identify this task and the software that it delivers or manages. Follow your organization's standards for naming tasks, if any.
Description When you edit a task, this option is not labeled. In the upper left of the task page, you can click the existing description to edit it.	Lets you type a description to further identify this task and make it more recognizable. Do not include critical information in the description because it is not intended to appear in all the lists that contain the name.
Software resource	Lets you select the software to deliver.
Command line	Lets you select a command line to run. This drop-down list contains all the command lines that are defined for the software resource that you selected. If the software resource has multiple packages, be sure to select the correct command line for the selected package.
Package	Lets you select the package to deliver, if this software resource has multiple packages. This option is not available in the **Quick Delivery** wizard.
Advanced	Lets you change the settings that control how this task runs. See "Advanced options for tasks in Software Management Solution" on page 70. This option is not available in the **Quick Delivery** wizard.

See "Creating a task in Software Management Solution" on page 142.

See "Editing a task in Software Management Solution" on page 143.

Delivering packages

This chapter includes the following topics:

- About Package Delivery
- Delivering a package without defining a software resource
- Package settings for Package Delivery tasks

About Package Delivery

When all you need to do is quickly push out a package, use Package Delivery. This task-based delivery method lets you deliver any package regardless of whether it is associated with a software resource.

You might use Package Delivery for the following reasons:

- To deliver a package that your organization chooses not to manage in the Software Catalog.
- To quickly deliver a new package that is not yet in the Software Catalog.
- To deliver a package that is in the Software Catalog, but with a command line that is not defined for the package.
  For example, a package is in the Software Catalog and is associated with predefined command lines. You need to deliver that package with a specialized command line, but you do have the privileges to edit the package or its software resource. You can create a Package Delivery task for that package and type the command line that you need.
- To run a task that you migrated from the Task Server Plug-in in Software Delivery Solution 6.x to Software Management Solution 7.0.
  The migrated tasks let you perform deliveries with the same configurations as the 6.x tasks.

See "Delivering a package without defining a software resource" on page 138.

Delivering a package without defining a software resource

A Package Delivery task lets you deliver any package regardless of whether it is associated with a software resource.

See "About Package Delivery" on page 137.

Table 8-1   Process for delivering a package without defining a software resource

Step	Action	Description
Step 1	Create a Package Delivery task.	A Package Delivery task lets you perform a routine package delivery. See "Creating a task in Software Management Solution" on page 142. See "Package settings for Package Delivery tasks" on page 139.
Step 2	(Optional) Change the task settings.	Every task inherits the default settings that control how the task runs. You can override the default settings for a particular task. See "Advanced options for tasks in Software Management Solution" on page 70.
Step 3	Schedule the task and select the delivery destinations.	Define the schedule and the delivery destinations every time you run the task. Your options for scheduling the task are as follows: ■ Run the task now. This option runs the task as soon as possible, unless it must wait for a maintenance window. ■ Schedule the task to run at a specific time. See "Scheduling a task and selecting computers in Software Management Solution" on page 144.

Table 8-1   Process for delivering a package without defining a software
                   resource *(continued)*

Step	Action	Description
Step 4	After the task runs, view the reports.	The Software Management reports let you monitor the software deliveries.
		The delivery reports provide information about the status of the software downloads and executions. For example, the software downloads for each computer, including the status and the download date.
		See "Running a Software Management Solution report" on page 83.

Package settings for Package Delivery tasks

This section lets you define or edit the details of a Package Delivery task, including the package that it delivers.

See "About Package Delivery" on page 137.

When you edit a Package Delivery task, the **Task Status** section appears beneath the **Package settings** section on the page. Under the **Task Status** section, you can schedule the task, select the destination computers, and view the status of the task.

See "Scheduling a task and selecting computers in Software Management Solution" on page 144.

Table 8-2   Package settings for Package Delivery tasks

Option	Description
Name When you edit a task, this option is not labeled. In the upper left of the task page, you can click the existing name to edit it.	Identifies this task in any list of tasks throughout the product. Make the name descriptive enough for others to easily identify this task and the software that it delivers or manages. Follow your organization's standards for naming tasks, if any.

Table 8-2 Package settings for Package Delivery tasks *(continued)*

Option	Description
Description When you edit a task, this option is not labeled. In the upper left of the task page, you can click the existing description to edit it.	Lets you type a description to further identify this task and make it more recognizable. Do not include critical information in the description because it is not intended to appear in all the lists that contain the name.
Package	Lets you select a package to deliver. You can browse the Software Library for a package or you can add a new package. You can source the new package from the Software Library, a UNC path, a URL, or a directory on the Notification Server computer. For more information, see the topics about adding and editing a package in the *Symantec Management Platform Help*.
Command line	Lets you select or define a command line to run. You can select any command line that is predefined for the package, or you can click **New** to define a new command line.
Advanced	Lets you change the settings that control how this task runs. See "Advanced options for tasks in Software Management Solution" on page 70.

See "Creating a task in Software Management Solution" on page 142.

See "Editing a task in Software Management Solution" on page 143.

Creating and managing Software Management tasks

This chapter includes the following topics:

- Types of tasks in Software Management Solution
- Creating a task in Software Management Solution
- Editing a task in Software Management Solution
- Scheduling a task and selecting computers in Software Management Solution

Types of tasks in Software Management Solution

Notification Server tasks let you download and run packages, programs, commands, and other items to client computers. You use tasks to perform most of the actions in Software Management Solution.

Table 9-1   Types of tasks in Software Management Solution

Type of task	Description
Package Delivery	Lets you deliver any package regardless of whether it is associated with a software resource.
	See "Delivering a package without defining a software resource" on page 138.

Table 9-1   Types of tasks in Software Management Solution *(continued)*

Type of task	Description
Quick Delivery	Lets you perform a quick delivery of a single software resource. Creating this task is the first step in the Quick Delivery process. The software that you deliver in this way must be defined as a deliverable software resource in the Software Catalog. See "Performing a quick delivery of a single software resource" on page 132.
Source Path Update	Lets you update the source paths of Windows Installer applications with the resilient source paths that point to the package servers that you designate. See "Updating the source paths of Windows Installer applications" on page 199.
Software Virtualization	(Windows only) Lets you manage virtual software layers on managed computers or deliver a VSA file to managed computers. See "Managing virtual applications" on page 217.
Windows Installer Repair	Lets you proactively identify and repair broken Windows Installer applications on selected computers. See "Repairing Windows Installer applications" on page 194.

See "Creating a task in Software Management Solution" on page 142.

See "Editing a task in Software Management Solution" on page 143.

Creating a task in Software Management Solution

Creating a task is typically the first step in performing the software-related actions in Software Management Solution. This procedure describes how to create any type of task in Software Management Solution.

See "Types of tasks in Software Management Solution" on page 141.

See "Scheduling a task and selecting computers in Software Management Solution" on page 144.

To create a task

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

2   In the left pane, under **Jobs and Tasks**, expand **Software** and select the type of task to create.

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

4 In the **Create new task** dialog box, complete the options to define the task.

The type of task that you selected determines the options that appear, as follows:

- Package Delivery
  See "Package settings for Package Delivery tasks" on page 139.

- Quick Delivery
  See "Software settings for Quick Delivery tasks" on page 135.

- Source Path Update (Windows only)
  See "Configuration settings for Source Path Update tasks" on page 201.

- Software Virtualization (Windows only)
  See "Software Virtualization settings" on page 226.

- Windows Installer Repair
  See "Windows Installer Repair settings" on page 196.

5 (Optional) In the **Create new task** dialog box, click **Advanced** to change the default settings that control how this task runs.

You cannot change the default settings in a Software Virtualization task.

See "Advanced options for tasks in Software Management Solution" on page 70.

6 In the **Create new task** dialog box, click **OK**.

Editing a task in Software Management Solution

You can edit any type of Software Management Solution task.

See "Types of tasks in Software Management Solution" on page 141.

To edit a task

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

2 In the left pane, under **Jobs and Tasks**, expand **Software** and select the type of task to edit.

3 In the right pane, double-click a task.

The type of task that you selected determines the page that appears.

4 Do any of the following:

- In the top section, click **Advanced** to change the task's settings for this instance.
See "Advanced options for tasks in Software Management Solution" on page 70.

- In the top section, edit the task's details. The type of task that you selected determines the options that appear.
See "Package settings for Package Delivery tasks" on page 139.
See "Software settings for Quick Delivery tasks" on page 135.
See "Configuration settings for Source Path Update tasks" on page 201.
See "Software Virtualization settings" on page 226.
See "Windows Installer Repair settings" on page 196.

- Under **Task Status**, click **Quick Run** to run the task on a single destination as soon as possible.

- Under **Task Status**, click **New Schedule** to schedule the task and select the destination computers.
See "Scheduling a task and selecting computers in Software Management Solution" on page 144.

- Under **Task Status**, double-click an existing instance of this task to re-schedule it.
You might want to reschedule an existing instance if the task failed due to an incorrect setting. In that case, you can fix the setting and reschedule the task instead of creating a new task.

5   When you finish editing the task, on the task's main page, click **Save changes**.

Scheduling a task and selecting computers in Software Management Solution

Software Management tasks use the task management component of Notification Server that provides flexibility in targeting computers and scheduling tasks. For example, when you schedule tasks, you can configure multiple schedules for an individual task, use maintenance windows, or use shared schedules. When you select computers, you can build and re-use predefined groups of computers.

To schedule a task and to select computers

1   Open the task for editing.

2   On the task page, click either of the following:

- **Quick Run**

Lets you run the task on a single destination as soon as possible, unless it must wait for a maintenance window. This option is not available for some tasks.

■ **New Schedule**
Add schedule
Lets you schedule the task to run at a specific time. The name of the option depends on the type of task.

To see these options, you might have to click a tab or expand a section on the task page.

For more information, see the topics about task schedule options in the *Symantec Management Platform Help*.

3 Select the computers to run the task on.

For more information, see the topics about specifying the targets of a policy or task in the *Symantec Management Platform Help*.

4 (Optional) To create multiple schedules and computer lists for this task, repeat step 2 through step 3.

5 On the task page, save the changes.

Delivering 6.x software packages

This chapter includes the following topics:

About the delivery of Altiris 6.x software packages

When you upgrade from Notification Server 6.x to Symantec Management Platform 7.0, you can migrate 6.x software packages for both Windows and non-Windows software. Then you can use Software Management Solution tasks and policies to deliver the migrated packages.

For more information about the migration of software delivery data, see the *Software Management Solution Release Notes*.

Table 10-1   Methods for delivering Altiris 6.x software packages

Method	Description
Quick Delivery, Managed Software Delivery, or the **Software Portal**	These delivery methods use the enhanced delivery functionality of Software Management Solution 7.0. They also leverage the software resource information that is in the Software Catalog and Software Library. See "How Software Management Solution integrates with the Software Catalog and Software Library" on page 93. Before you can deliver a 6.x software package with any of these delivery methods, assign the package to a software resource. For more information about 6.x data migration, see the *Symantec Management Platform Release Notes*. These delivery methods leverage the software resource information that is in the Software Catalog and Software Library.
Package Delivery	Whether or not you do assign a migrated package to a software resource, you can use a Package Delivery task to deliver that package. You can also migrate 6.x Software Delivery Task Server Plug-in tasks to Package Delivery tasks to deliver packages with the same configurations as in 6.x. See "Delivering a package without defining a software resource" on page 138.
Legacy Software Delivery	Legacy Software Delivery policies are the result of migrating 6.x Software Delivery tasks to 7.0 policies. Legacy Software Delivery lets you deliver a 6.x software package with the same configurations as in the 6.x task. We recommend that you use this method only for 6.x packages that you cannot deliver with Quick Delivery or Managed Software Delivery. See "About Legacy Software Delivery" on page 149.

Table 10-1   Methods for delivering Altiris 6.x software packages *(continued)*

Method	Description
Software Virtualization task	Software Virtualization tasks let you deliver virtual software archive (VSA) files and import them into virtual software layers on client computers. Use this method when you migrate 6.x VSA packages.
	You also can migrate 6.x SVS Task Server Plug-in tasks to Software Virtualization tasks.
	See "Installing and managing a virtual software layer with a Software Virtualization task" on page 225.

About Legacy Software Delivery

Legacy Software Delivery policies deliver software packages with the same configurations as the Software Delivery tasks that you migrated from Software Delivery Solution 6.x.

For more information about the migration of software delivery data, see the *Software Management Solution Release Notes*.

You can take the following actions on an existing Legacy Software Delivery policy:

- Run the policy to deliver the software.
  See "Delivering software packages with the same configurations as 6.x Software Delivery tasks" on page 150.

- Edit or clone an existing policy.
  See "Accessing a Legacy Software Delivery policy" on page 150.

You cannot create new Legacy Software Delivery policies.

Use Legacy Software Delivery policies only for 6.x packages that you cannot deliver with Quick Delivery or Managed Software Delivery. Otherwise, we recommend that you use the latter delivery methods.

Because a Legacy Software Delivery policy uses some of the 7.0 functionality, it is not the same as a 6.x software delivery task.

See "How Legacy Software Delivery policies differ from 6.x Software Delivery tasks" on page 151.

Accessing a Legacy Software Delivery policy

During the upgrade to Symantec Management Platform 7.0, you can migrate 6.x Software Delivery tasks to 7.0 Legacy Software Delivery policies. Access the Legacy Software Delivery policies to edit, clone, and run them.

See "About Legacy Software Delivery" on page 149.

To access a Legacy Software Delivery policy

1   In the **Symantec Management Console**, on the **Manage** menu, click **Policies**.

2   In the left pane, under **Policies**, click **Software**.

3   Depending on the kind of task that you migrated, expand one of the following subfolders:

Windows software delivery task	**Legacy Software Delivery** folder
UNIX, Linux, or Mac OS delivery task	**Legacy Software Delivery for UNIX/Linux/Mac** folder

Delivering software packages with the same configurations as 6.x Software Delivery tasks

During the upgrade to Symantec Management Platform 7.0, you can migrate 6.x Software Delivery tasks to 7.0 Legacy Software Delivery policies. Legacy Software Delivery lets you deliver a 6.x software package with the same configurations as in the 6.x task.

See "About Legacy Software Delivery" on page 149.

Table 10-2   Delivering 6.x software packages

Step	Action	Description
Step 1	Access the migrated Legacy Software Delivery policy.	When you migrate 6.x Software Delivery tasks to Legacy Software Delivery policies, the resulting policies are placed in specific folders in the **Symantec Management Console**. See "Accessing a Legacy Software Delivery policy" on page 150.

Table 10-2   Delivering 6.x software packages *(continued)*

Step	Action	Description
Step 2	(Optional) Edit the Legacy Software Delivery policy.	You can edit the Legacy Software Delivery policy to change or add functionality as follows: ■ Edit or change the package or program that the policy installs. ■ Change the settings for the policy.
Step 3	Select the delivery destinations.	Select the managed computers to deliver to. The destination selection is the same as for a Managed Software Delivery policy. See "About the destinations for a Managed Software Delivery policy" on page 114.
Step 4	Schedule the policy.	Define the schedule on which the Legacy Software Delivery policy runs. The schedule definition is the same as for other policies. For more information, see the topics on specifying a policy schedule in the *Symantec Management Platform Help*. You can also check any of the check boxes to configure additional schedule settings. See "Extra schedule options section" on page 40.

How Legacy Software Delivery policies differ from 6.x Software Delivery tasks

During the upgrade to Symantec Management Platform 7.0, you can migrate 6.x Software Delivery tasks to 7.0 Legacy Software Delivery policies.

See "About Legacy Software Delivery" on page 149.

A Legacy Software Delivery policy is not the same as a 6.x Software Delivery task. It uses 7.0 functionality to define the delivery destinations and to schedule and enable the policy.

| | Table 10-3 | How a Legacy Software Delivery policy differs from a 6.x Software Delivery task |

Screen element	Differences in a 7.0 Legacy Software Delivery policy
New page layout	A Legacy Software Delivery policy contains the following sections: ■ **Policy Rules/Actions** Contains the **General** tab, **Advanced** tab, and **Status** tab. ■ **Applied to** Lets you add or change the delivery destinations. For more information, see the topics about specifying the targets of a policy in the *Symantec Management Platform Help*. ■ **Schedule** Lets you add or change the delivery schedule. See "Schedule settings for Managed Software Delivery" on page 55.
General tab	The **General** tab in a Legacy Software Delivery policy differs from a 6.x Software Delivery task in the following ways: ■ The options to select a policy's target and schedule are no longer on this tab. ■ The **Package Name** link opens the 7.0 **Select Software** dialog box instead of the 6.x **Package Selector** dialog box. ■ The **Go to Package** link opens the 7.0 **Add or Edit Package** dialog box instead of the package's **Package** tab. ■ The **Go to Program** link opens the 7.0 **Add or Edit Command Line** dialog box instead of the package's **Programs** tab. ■ For UNIX, Linux, or Mac OS deliveries, the **Removal** section and the **Availability** section are eliminated.
Advanced tab	The **Advanced** tab in a Legacy Software Delivery policy differs from a 6.x software delivery task in the following ways: ■ This tab contains the **Download and Execution Options** section. ■ This tab contains the **Program options** section. This section contains some of the options from the 6.x package's **Advanced** tab. ■ In UNIX, Linux, or Mac OS policies, this tab contains the same options as the Windows delivery policies.

About assigning 6.x software packages to software resources

When you upgrade from Notification Server 6.x to Symantec Management Platform 7.0, you can migrate 6.x software packages for both Windows and non-Windows software. After you migrate a 6.x software package, we recommend that you deliver

it with Quick Delivery, Managed Software Delivery, or the Software Portal. Before you can use any of those delivery methods, you must assign the 6.x software package to a software resource.

For more information, see the topics about data migration in the *Symantec Management Platform Installation Guide*.

You can assign a 6.x software package to a new software resource or an existing software resource. If the existing software resource already contains packages, the 6.x package is added to the list of packages. When you assign software packages to software resources, you can select a single package or multiple packages. If you select a single package, the **Assign Package to Software Resource** wizard is used. If you select multiple packages, a package assignment task is created for the selected packages.

See "Assigning an Altiris 6.x software package to a software resource" on page 153.

See "Assigning multiple Altiris 6.x software packages to software resources" on page 154.

When you assign a 6.x software package to a software resource, the location of the package's files does not change. However, after you assign a software package to a software resource, you can add the package's files to the Software Library.

When you assign a package to a software resource, the Software Portal settings **Install Software** and **Install On Approval** are migrated to the software resource.

For more information, see the topic about the Software Publishing tab in the *Software Management Solution Help*.

Assigning an Altiris 6.x software package to a software resource

After you migrate 6.x software packages to Software Management Solution, you should assign them to software resources. You must assign them to software resources to deliver them with any of the following 7.0 delivery methods: Quick Delivery, Managed Software Delivery, or the Software Portal.

See "About assigning 6.x software packages to software resources" on page 152.

When you assign a 6.x software package to a software resource, you can edit the package's command lines. Afterwards, you can access the software resource in the Software Catalog and edit any of its data.

You can also assign multiple packages to software resources at the same time. If you migrated numerous 6.x software packages, you can save time by assigning multiple packages at the same time.

To assign an Altiris 6.x software package to a software resource

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

2   In the left pane, under **All Resources**, click **Package > Software Package**.

3   In the right pane, on the package's right-click menu, click **Actions > Assign to Software Resource**.

    This action appears only for the migrated packages that are not assigned to a software resource.

4   On the **Select software resource** page, click one of the following options:

    ■   **Create new software resource**
        Click this option if the software resource is not in the Software Catalog. After you select this option, define the properties that identify the software resource. These properties appear on the software resource's **Properties** tab.

    ■   **Use existing software resource**
        Click this option if the software resource is in the Software Catalog. After you click this option, click **Select software resource**, and select the software resource to assign the package to.

5   Click **Next**.

6   (Optional) On the **Set Command line properties** page, edit the properties of the package's command lines, and select a default command line.

    This page displays all the command lines that are associated with the package. If you selected an existing software resource on the **Select software resource** page, the command lines that are already associated with the software resource are also displayed.

    When a command line's type is **Custom**, **Set as the default command line** is disabled.

7   Click **Finish**.

Assigning multiple Altiris 6.x software packages to software resources

After you migrate 6.x software packages to Software Management Solution, you should assign them to software resources. You must assign them to software

resources to deliver them with any of the following 7.0 delivery methods: Quick Delivery, Managed Software Delivery, or the Software Portal.

See "About assigning 6.x software packages to software resources" on page 152.

For more information, see the topics about delivery methods in the *Software Management Solution Help*.

You can assign multiple 6.x software packages to software resources at the same time. If you migrated numerous 6.x software packages, you can save time by assigning multiple packages at the same time. When you assign multiple software packages, a package assignment task is created. The package assignment task lets you add packages and edit any of the packages before you assign them to software resources. After you assign packages to software resources, you can then access each software resource in the Software Catalog and edit its software resource data.

You can also assign a single package to a software resource. Use this method if you only have a few packages to assign to software resources.

See "Assigning an Altiris 6.x software package to a software resource" on page 153.

To assign multiple Altiris 6.x software packages to software resources

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

2   In the left pane, under **All Resources**, click **Package > Software Package**.

3   In the right pane, select two or more 6.x packages that are not assigned to a software resource.

    You must select at least two packages to create a package assignment task. After the task is created, you can add other packages.

4   On the right-click menu, click **Actions > Assign to Software Resource**.

    If the **Assign to Software Resource** action does not appear, all of the packages that you selected have been assigned to a software resource.

5   Click the **Manage Task** tab to open the task.

6   To add other 6.x packages, under the **Software Settings** section, click **Add Packages**.

    See "Adding 6.x software packages to a package assignment task" on page 156.

7   To edit a 6.x package, under the **Software Settings** section, double-click the package name.

    When you edit a package, you can modify its command lines and assign it to a new software resource or existing software resource.

    See "Editing 6.x software packages" on page 157.

8   To change the default command line for the software resource, under **Software Settings**, in the **Command Line Type** drop-down list, click **Install**, **Uninstall**, or **Repair**.

    You can only set a command line as the default if that command line was associated with the 6.x package. The default command line that you select appears in the **Default Command Line** column. You can also set the default command line when you edit the package.

    See "Editing 6.x software packages" on page 157.

9   If you made any changes to the packages in the **Software Settings** section, click **Save changes**.

10 Under the **Task Status** section, click **New Schedule**, and schedule when to run the task.

    When the task runs, it assigns the 6.x packages that are listed in the **Software Settings** section to software resources. The task is saved in the **Assign Packages to Software Resources** folder. To access this folder, on the **Manage** menu, click **Jobs and Tasks > System Jobs and Tasks > Software**.

Adding 6.x software packages to a package assignment task

A package assignment task is created when you select multiple 6.x software packages and begin the process of assigning these packages to software resources. The package assignment task lets you add other software packages. When you add packages to the task, a list of the 6.x packages that are not assigned to a software resource appears. This list makes it easy to identify the packages that are not assigned to a software resource. You can then select from this list the packages that you want to assign to software resources.

See "About assigning 6.x software packages to software resources" on page 152.

To add 6.x software packages to a package assignment task

1   Access the package assignments task.

    See "Assigning multiple Altiris 6.x software packages to software resources"
    on page 154.

2   Under **Software Settings**, click **Add Package**.

3   In the **Add Software Packages** dialog box, click **>** or **>>** to move packages
    from the left pane to the right pane.

    The **>** option moves any packages that are selected and the **>>** option moves
    all of the packages . You can also use the search field to find packages.

4   On the **Add Software Packages** dialog box, click **OK**.

Editing 6.x software packages

A package assignment task is created when you select multiple 6.x software
packages and begin the process of assigning them to software resources. This task
lists the 6.x software packages that were selected. You can edit any of the packages
in the task. When you edit a package, you can assign it to a new software resource
or to an existing software resource. You can also edit the command lines of the
package.

See "About assigning 6.x software packages to software resources" on page 152.

To edit 6.x software packages

1   Access the package assignment task.

    See "Assigning multiple Altiris 6.x software packages to software resources"
    on page 154.

2   Under **Software Settings**, double-click a package.

3   To define the package's software resource, in the **Edit Software Details** dialog
    box, on the **Select Software** tab, select one of the following options:

    ■   **Create new software resource**
        Click this option if the software resource is not in the Software Catalog.
        After you select this option, define the properties that identify the software
        resource. These properties appear on the software resource's **Properties**
        tab.

    ■   **Use existing software resource**
        Click this option if the software resource is in the Software Catalog. After
        you click this option, click **Select software resource**, and select the
        software resource to assign the package to.

4 To edit the package's command lines, in the **Edit Software Details** dialog box, on the **Set Command Line** tab, edit any of the fields for the listed command lines.

If you select **Custom** as a **Command type**, then you cannot check **Set as the default command line** option.

5 In the **Edit Software Details** dialog box, click **OK**.

Section 3

Delivering software from user requests

Introducing the Software Portal

This chapter includes the following topics:

- About the Software Portal
- About Software Portal user roles
- About the software in the Software Portal

About the Software Portal

The **Software Portal** lets users submit requests and install software through a Web-based interface with little or no administrator involvement. This self-service approach to software delivery reduces help desk calls and simplifies the process of requesting and delivering software. Because the **Software Portal** uses predefined software information and delivery settings, it can automate most of the deliveries that result from the software requests.

The administrator who sets up the Software Catalog decides which software each user or group of users is allowed and specifies which software requires approval. These settings determine the amount of intervention that is required for specific software requests. Requests for pre-approved software require no further action from anyone. Requests for other standard software require approval from a manager or an administrator but upon approval, the software delivery is automatic. Only the requests for non-standard software require the manager or the administrator to take further action to deliver the software.

The **Software Portal** is installed on the client computers. Therefore, the users can create requests and the managers can approve the requests without requiring access to the **Symantec Management Console**.

The **Software Portal** supports requests for Windows and Mac OS software.

See "Implementing the Software Portal" on page 173.

See "Software request work flow" on page 167.

See "Processing a software request on the Administrator Portal page" on page 185.

About Software Portal user roles

Several types of users interact with the **Software Portal**. Each type of user has its own privileges and responsibilities. The security privileges in Notification Server let specific user roles manage and approve the users' software requests.

See "Recommended security settings for the Software Portal" on page 175.

Table 11-1   Users of the **Software Portal**

User role	Privileges and responsibilities
Administrator, **Software Portal**	This administrator requires **Software Portal** privileges to administer software requests. The **Software Portal** administrator's tasks are as follows: ■ Approve users' software requests when necessary. For example, the administrator might approve a request that the manager is not allowed to approve. ■ Approve any user's request when a manager is not available. ■ Deliver the approved software that is not in the Software Catalog or that is not assigned to the user. The same person might perform both the **Software Portal** administrator and the Software Catalog administrator roles.
Administrator, Software Catalog	The Software Catalog administrator manages the Software Catalog, which represents the software that is known to be in your organization. This administrator requires Software Management Framework privileges. For more information, see the topics about Software Management Framework privileges in the *Symantec Management Platform Help*. The Software Catalog administrator's tasks in the Software Portal are as follows: ■ Define the software that appears in the **Software Portal** for specific users or groups. ■ Pre-approve software for specific users or groups. Pre-approval streamlines the request process by eliminating the need for additional intervention from the manager, administrator, or help desk. For example, the administrator can pre-approve a group of software tools that users in a specific department require.

Table 11-1   Users of the **Software Portal** *(continued)*

User role	Privileges and responsibilities
Manager	The **Software Portal** manager approves users' software requests in the **Software Portal**. The manager can be any employee in your organization who has the authority to allow users to acquire software. Typically, a department manager fills this role.
	Because the **Software Portal** is installed on the client computer, the manager can approve requests without access to the **Symantec Management Console**.
	The **Software Portal** manager requires **Software Portal** privileges to manage and approve software requests.
User	The user on a client computer submits requests for software on the **Home** page in the **Software Portal**. The user can be any employee in the organization who needs software.
	Because the **Software Portal** is installed on the client computer, the user can create requests without access to the **Symantec Management Console**.
	Typically, users do not have access to the **Symantec Management Console** and do not have Notification Server security roles.

See "About the approval of software requests" on page 165.

About the software in the Software Portal

An administrator adds software to the **Software Portal** and configures the settings and the permissions that let users request the software. The terms that describe these settings and permissions appear on the **Software Portal** pages where the software is displayed.

See "Methods for adding software to the Software Portal" on page 176.

Table 11-2   Terms that describe the software in the **Software Portal**

Term	Description
Listed	The software that is in the Software Catalog and published to the **Software Portal** for the current user.
	Listed software is available for the user to request. If it is not recommended for the current user, it does not appear on the user's **Home** page by default.
	The term **Listed** can also apply to a request for listed software.

Table 11-2   Terms that describe the software in the **Software Portal** *(continued)*

Term	Description
Unlisted	Software that meets any of the following conditions: ■ The software is not in the Software Catalog. ■ The software is in the Software Catalog but is not published to the **Software Portal**. ■ The software is published to the **Software Portal** but not for the current user. Unlisted software cannot be delivered automatically on request. The term **Unlisted** can also apply to a request for unlisted software.
Approved	The listed software that is pre-approved for a specific user. Typically, the software that does not require a license is pre-approved. For example, Adobe Reader and the Google Toolbar do not require a license. Approved software is delivered or scheduled for delivery as soon as the user submits a request for it. No further action is needed. The person who publishes the software to the **Software Portal** can pre-approve it.
Recommended	The listed software that is recommended for a specific user. For example, the software that is part of the user's set of core applications should be recommended. Recommended software appears on the user's **Home** page by default. The user can also display all the software that is published for them. The person who publishes the software to the **Software Portal** can designate it as recommended.

See "About the Software Portal" on page 161.

Introducing software requests

This chapter includes the following topics:

■ About the approval of software requests

■ Software request work flow

■ Methods for delivering software from approved software requests

■ Statuses of software requests in the Software Portal

■ About request status notifications

About the approval of software requests

Every software request that is created in the **Software Portal** must be approved before the software is installed. Different user roles can approve the software requests, depending on the type of request and the stage of the software request process.

See "About Software Portal user roles" on page 162.

Table 12-1   Users who can approve software requests

Approver	When their approval is needed
Administrator, Software Catalog	The Software Catalog administrator can pre-approve software for specific users or groups when the software is published to the **Software Portal**.
	Pre-approval streamlines the request process by eliminating the need for additional intervention from the manager, administrator, or help desk. For example, the administrator can pre-approve a group of software tools that users in a specific department require.
Administrator, **Software Portal**	A request requires an administrator's approval in the following situations:
	■ When the user is not assigned to a manager In this case, the request is sent directly to the administrator. ■ When a manager is out of the office or does not respond to a software request. ■ When the request is for an unlisted software resource and the manager assigns the request to the administrator An unlisted software resource is not in the Software Catalog or is not published to the **Software Portal** for the person who creates the request. A request for an unlisted software resource requires the manager or the administrator to take additional action. A manager who has access to the software can approve the request and provide the software to the user. A manager who does not have access to the software can approve the request and assign it to the administrator, who can provide the software. For example, the administrator can obtain new software or create a software delivery task.
	See "Processing a software request on the Administrator Portal page" on page 185.
Manager	A request requires a manager's approval when the software is not pre-approved for a user who is assigned to that manager. The software can be listed or unlisted.
	When a manager approves a request for listed software, the software is delivered. When a manager approves a request for unlisted software, the manager can choose to assign it to the **Software Portal** administrator for additional action.

Software request work flow

Figure 12-1 shows how a software request is processed through the **Software Portal**.

See "About the Software Portal" on page 161.

See "About Software Portal user roles" on page 162.

This diagram does not illustrate the additional steps that are required to deliver unlisted software. Unlisted software is either not in the Software Catalog or is not published to the **Software Portal**. Therefore, it cannot be delivered automatically and someone must take additional steps to deliver it.

See "About the approval of software requests" on page 165.

Figure 12-1   Software request work flow diagram for listed software
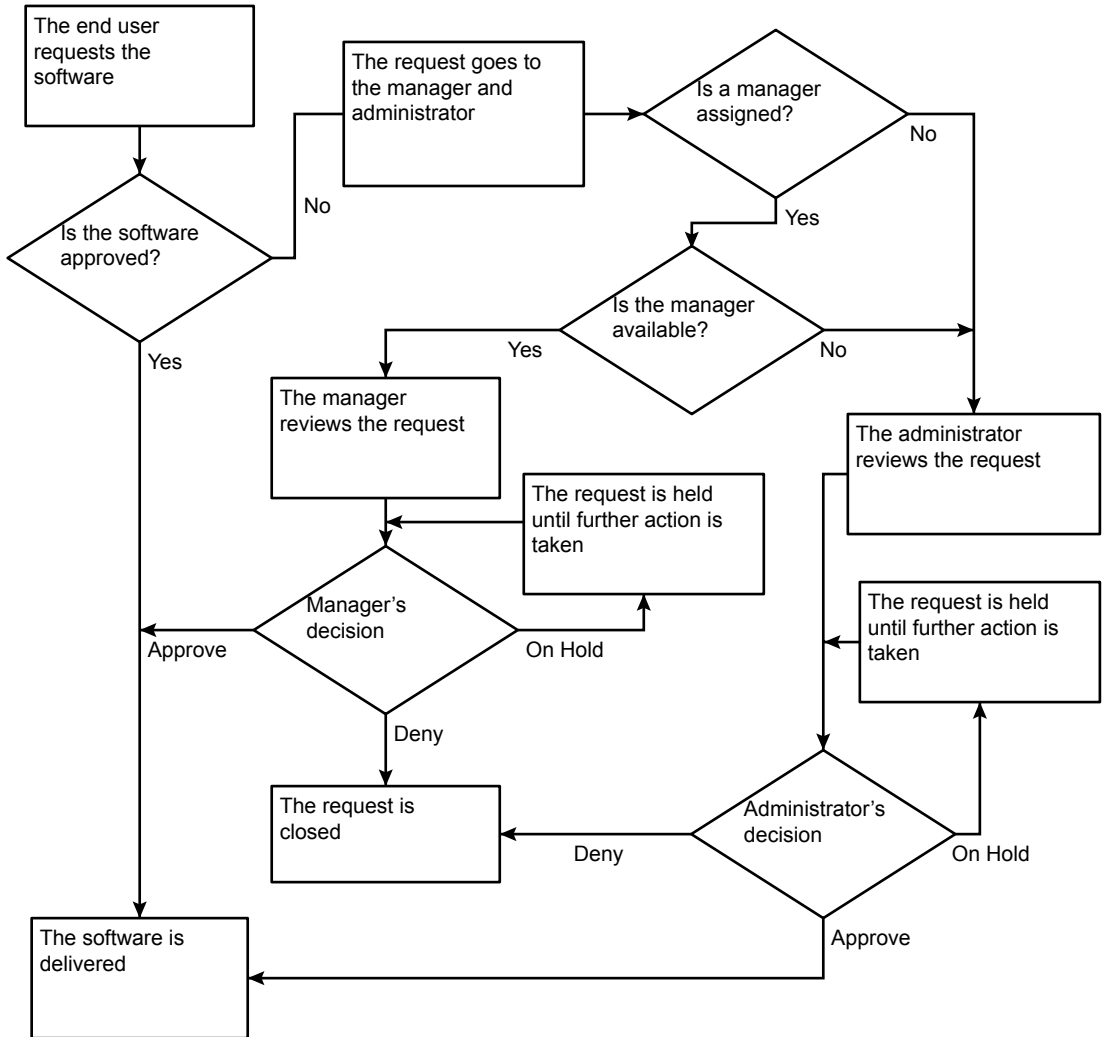
Methods for delivering software from approved software requests

When a manager or administrator approves a software request, the software is delivered to the user.

The delivery method for requested software depends on whether the software is listed or unlisted as follows:

Listed software	Listed software is delivered automatically upon approval of the software request. The method that was used to publish the software to the **Software Portal** determines whether a task or a policy performs the delivery.
	See Table 12-2.
Unlisted software	Unlisted software cannot be installed automatically. The approver must take additional action outside of the **Software Portal** to deliver the software.
	An unlisted software resource is not in the Software Catalog or is not published to the **Software Portal** for the person who creates the request.
	See Table 12-3.

Table 12-2 Delivery methods for listed software

Publication method	Delivery method
Software resource	The first approved request for that software creates a Quick Delivery task. Each subsequent request for that software creates a new instance of the first Quick Delivery task. The new instance is delivered to the user who requested the software.
Managed Software Delivery policy	A request for that software adds the user to the destinations for the policy. The software is delivered according the schedule that is defined for that policy.

See "Methods for adding software to the Software Portal" on page 176.

Table 12-3   Delivery methods for unlisted software

Software resource's state	Typical approver	Delivery method
The software resource is not in the Software Catalog and it does not need to be added. For example, the software might be a special utility that only a few people in the organization need.	Administrator or manager	The administrator or the manager obtains the software and gives it to the user to install.
The software resource is not in the Software Catalog and it needs to be added. For example, the software application is one that you plan to manage.	Administrator	Add the software resource to the Software Catalog and create a software delivery policy or task to deliver it. For more information, see the topics about populating the Software Catalog in the *Symantec Management Platform Help*. See "Methods for delivering software" on page 88.
The software resource is in the Software Catalog but was not published at all or was not published for the user who requested it.	Administrator	Create a software delivery policy or task to deliver the software. See "Methods for delivering software" on page 88.

Statuses of software requests in the Software Portal

The status of a software request indicates its place in the **Software Portal** approval process. As a software request is processed, the user, manager, and administrator can check its status at any time.

A software request is created when a user uses the **Software Portal** to request software. A manager or an administrator processes a software request by changing its status.

See "Processing a software request on the Administrator Portal page" on page 185.

Users of the **Software Portal** can check the status of software requests from the following locations:

- Under the **Request Status** section on the user's **Home** page, the **Manager Portal** page, or the **Administrator Portal** page, depending on your user role.

- In any of the **Request Details** dialog boxes that appear when a request is opened.

- In the reports that are available in the **Symantec Management Console**. Typically, these reports are available to the administrator only.
  See "Running a Software Management Solution report" on page 83.

- In the Web parts that are associated with the **Software Portal**.
  See "Web parts for Software Management Solution" on page 48.

Some of the statuses are used for reporting purposes only and do not appear on any pages or dialog boxes in the **Software Portal**.

Table 12-4   Statuses of software requests in the **Software Portal**

Status	Description
Approved (Complete)	The request is approved and the software is either installed or scheduled for installation.
Approved (Pending)	The request is for unlisted software and a manager approved it and sent it to an administrator for approval.
Canceled	The user canceled the request.
Closed	A request is closed when it has any of the following statuses: ■ Approved (Complete) ■ Canceled ■ Denied The Closed status does not appear in the **Request Status** list or in the **Request Details** dialog boxes. However, it is included in the messages that appear when someone tries to edit a request that is closed.
Denied	The manager or the administrator denied the request.
Failure	An attempt to deliver the requested software was made and it failed. This status describes the software delivery rather than the software request. It appears on the **Software Portal** reports and the Web parts that appear in the **Symantec Management Console**.

Table 12-4   Statuses of software requests in the **Software Portal** *(continued)*

Status	Description
On Hold	The manager or the administrator placed the request on hold pending further research.
	For example, the manager might place a request on hold and enter comments to ask the user to justify the need for the software. The administrator might need to check the availability of a license or obtain the software.
Open	The request is not closed. For example, an On Hold request is considered to be Open.
Scheduled	The request is approved and is scheduled for delivery.
Submitted	The user created the request but no one has taken further action on it.
Success	The requested software was delivered successfully. This status describes the software delivery rather than the software request. It appears on the **Software Portal** reports and the Web parts that appear in the **Symantec Management Console**.

See "About the software in the Software Portal" on page 163.

About request status notifications

The **Software Portal** can facilitate communication about software requests by sending email messages automatically as a result of certain actions. An email notice can be triggered when a software request's status changes and when someone adds a comment to a software request.

When you configure your user profile, you can specify for the receipt of email messages about requests. These preferences become the default for any software requests that you create or review. You can override the default email settings for specific software requests.

The automated email messages ensure that you receive the most current information about the software requests and prevent delays in processing them. For example, the user creates a software request for a new application. The manager denies the request because the user specified an obsolete version. Any change to a software request's status requires a comment to be entered. Therefore, the manager's denial can trigger an email to the user to explain why the request is denied. As a result, the user can take immediate action to provide the required information.

Setting up the Software Portal

This chapter includes the following topics:

- Implementing the Software Portal
- Recommended security settings for the Software Portal
- Methods for adding software to the Software Portal
- Adding a software resource to the Software Portal
- About deleting a published software resource
- Adding a Managed Software Delivery policy to the Software Portal
- Add User dialog box
- Configuring the Software Portal settings

Implementing the Software Portal

Before you or any users can use the **Software Portal**, you must set it up and prepare it for use.

See "About the Software Portal" on page 161.

The minimum prerequisites for implementing the **Software Portal** are as follows:

- Software Management Solution must be installed on the Notification Server computer. The **Software Portal** is installed on the Notification Server computer when Software Management Solution is installed.
  For more information, see the *Symantec Management Platform Installation Guide.*

■ The Software Management Solution agent must be installed on the computers on which you implement the **Software Portal**.
See "Installing the Software Management Solution agent" on page 38.

■ The Software Management Solution plug-in for UNIX, Linux, or Mac must be installed on the Mac computers on which you implement the **Software Portal**. For more information, see the topics about installing the Altiris Agent for UNIX, Linux, or Mac in the *Symantec Management Platform Help*.

Additional steps in the Software Management Solution implementation process can be performed, but the **Software Portal** implementation does not require them.

See "Implementing Software Management Solution" on page 34.

Table 13-1   Process for implementing the **Software Portal**

Step	Action	Description
Step 1	Configure security roles for the administrators and managers who need to use the **Software Portal**.	The security settings provide the permissions to manage and approve the users' software requests.
		See "Recommended security settings for the Software Portal" on page 175.
		Typically, users do not have access to the **Symantec Management Console** and do not have Altiris security roles.
Step 2	Configure the **Software Portal** settings.	The **Software Portal** settings customize the portal's behavior and appearance. You can change these settings at any time after you implement the **Software Portal**.
		See "Configuring the Software Portal settings" on page 181.
Step 3	Install the **Software Portal** agent on the client computers.	(Windows only) Perform this step every time that you need to install the **Software Portal** on the client computers that do not have it.
		The **Software Portal** agent provides access to the **Software Portal** Web application from the client computer. The agent also installs shortcuts to the **Software Portal** interface on the client computer.
		See "Installing the Software Portal agent" on page 46.
		You may have performed this step when you installed the Software Management Solution agent on the client computers.
		See "Options for installing the Software Portal agent" on page 45.

Table 13-1   Process for implementing the **Software Portal** *(continued)*

Step	Action	Description
Step 4	Define the software that appears in the **Software Portal**.	Before a user can request software from the **Software Portal**, you must define the software that the user can request. Perform this step whenever you add users or software resources to Notification Server.
		Examples are as follows:
		■ When the finance department hires a new employee, you add that employee to the software resources that the members of the finance department require.
		■ When an administrator adds a new software resource to the Software Catalog, they add the users who are allowed to request that software.
		You can define software in the **Software Portal** in the following ways:
		■ Publish a software resource to perform a quick delivery of a single software resource with a minimum of configuration. See "Adding a software resource to the Software Portal" on page 177.
		■ Publish a Managed Software Delivery policy to take advantage of its ability to respond to complex delivery requirements. See "Adding a Managed Software Delivery policy to the Software Portal" on page 179.
Step 5	Instruct the users and managers to configure their profiles.	Anyone who uses the **Software Portal** on a client computer must configure their user profile before they can create and process requests.
		For more information, see the topics on setting up the **Software Portal** and the user profile in the *Software Portal Help*.

Recommended security settings for the Software Portal

As part of the **Software Portal** implementation, you configure security privileges for the administrators and managers who need to use the **Software Portal**. The security privileges let specific user roles manage and approve the users' software requests.

See "Implementing the Software Portal" on page 173.

See "About Software Portal user roles" on page 162.

Typically, users do not have access to the **Symantec Management Console** and do not have Notification Server security roles.

You configure security for the **Software Portal** in the **Symantec Management Console** on the **Security Roles** page.

For more information, see the topics about assigning privileges to a security role in the *Symantec Management Platform Help*.

Table 13-2   Recommended privilege settings for the **Software Portal**

Security role	Recommended privileges	Description
Software Portal Administrators	**Administer Software Requests**	This setting is on the **Privileges** tab, under **Software Portal Privileges**. This setting provides access to the **Administrator Portal** page in the **Symantec Management Console**. The **Software Portal** administrator approves special requests and can also approve any requests if a manager is not available. The administrator also delivers the approved software that is not in the Software Catalog or that is not assigned to the user.
Software Portal Managers	**Manage and Approve Software Requests**	This setting is on the **Privileges** tab, under **Software Portal Privileges**. This setting provides access to the **Manage** tab in the **Software Portal**, from which the manager approves software requests. The manager can be any employee in your organization who has the authority to allow users to acquire software. Typically, a department manager fills this role.

Methods for adding software to the Software Portal

(Windows and Mac OS only)

Before a user can request software from the **Software Portal**, you must add the software that the user can request. The process of adding software to the **Software Portal** is known as publishing.

Publishing software to the **Software Portal** consists of the following actions:

- Selecting the software to publish

- Defining the users who are allowed to request that software

- Specifying whether a user needs approval to install that software

You can publish software to the `Software Portal` in the following ways:

Software resource	Publish a software resource to the **Software Portal** to deliver a single piece of software with minimum configuration. Most organizations can publish the majority of software in this way. See "Adding a software resource to the Software Portal" on page 177.
Managed Software Delivery policy	Publish a Managed Software Delivery policy to the **Software Portal** to deliver one or more software resources with complex delivery requirements. See "Adding a Managed Software Delivery policy to the Software Portal" on page 179. See "About advanced software deliveries" on page 96.

Adding a software resource to the Software Portal

(Windows and Mac OS only)

You can add (publish) a software resource to the **Software Portal** to deliver a single piece of software with minimum configuration. When you publish a software resource, a Quick Delivery task is created. After a software request is approved, the Quick Delivery task runs and installs the software on the user's computer as soon as possible.

See "About quick delivery of a single software resource" on page 131.

When a software resource is published to the **Software Portal**, its publishing settings are saved in the Software Catalog as a reference to the software resource. You cannot delete a software resource from the Software Catalog if references are associated with that software resource. To ensure that you can delete the software resource, you must delete its references first.

See "About deleting a published software resource" on page 178.

Warning: Currently, you can publish any deliverable software resource to the **Software Portal** and it appears in the portal's list of available software. However, if a software request does not have a command line, it cannot be requested and a message appears when someone tries to do so.

This task is a step in the process for implementing the **Software Portal**.

See "Implementing the Software Portal" on page 173.

You can also publish Managed Software Delivery policies to the **Software Portal**.

Warning: If the software resource that you publish has dependencies on other software, the dependency software is not delivered as a result of a user request. Instead, create and publish a Managed Software Delivery policy for that software so that the dependencies are installed.

See "Adding a Managed Software Delivery policy to the Software Portal" on page 179.

To add a software resource to the Software Portal

1 In the **Symantec Management Console**, on the **Manage** menu, click **Software**.

2 In the left pane, under **Software**, click the **Software Catalog** folder or expand it and select a subfolder.

3 In the right pane, on the **Software Catalog** page, double-click a software resource.

4 On the software resource page, click the **Software Publishing** tab.

5 On the **Software Publishing** tab, enter the details and select the settings for publishing this software resource.

See "Software Publishing tab" on page 120.

6 On the software resource page, click **Save changes**.

7 Close the software resource page.

About deleting a published software resource

(Windows and Mac OS only)

You can delete a software resource that is published to the Software Portal. However, you cannot delete a software resource that has references. A reference is an association between the software resource and another item in the Symantec Management Platform.

When a software resource is published to the Software Portal, a reference to its publishing settings is created. The publishing settings include the permissions, software name, and software description. Because these references are saved with the software resource, you can temporarily un-publish the software from the Software Portal without losing its settings.

For example, you publish a software resource to the Software Portal and set permissions for 12 user groups. Later, you need to make that software unavailable for a specific time, so you uncheck the **Publish to Software Portal** check box on the **Software Publishing** tab. When you decide to make the software available again, you can check the **Publish to Software Portal** check box and the software's Software Portal settings are preserved. You do not have to reset the permissions for those user groups.

See "Software Publishing tab" on page 120.

Before you can delete a software resource, you must delete all its references.

For more information, see the topics about deleting a software resource in the *Symantec Management Platform Help.*

Adding a Managed Software Delivery policy to the Software Portal

(Windows and Mac OS only)

You can add (publish) an existing Managed Software Delivery policy to the **Software Portal** to deliver one or more software resources with complex delivery requirements.

See "About advanced software deliveries" on page 96.

For example, you can publish a Managed Software Delivery policy that installs a software resource and the other software that it depends on. The user can request the main software without having to request the dependency software or even know that a dependency exists.

This task is a step in the process for implementing the **Software Portal**.

See "Implementing the Software Portal" on page 173.

You can also publish software resources to the **Software Portal**.

See "Adding a software resource to the Software Portal" on page 177.

To add a Managed Software Delivery policy to the Software Portal

1   In the **Symantec Management Console**, on the **Manage** menu, click **Policies**.

2   In the left pane, under **Policies**, click **Software > Managed Software Delivery**.

3   Select a managed software delivery policy.

4   In the right pane, expand the **Policy Rules/Actions** section and click the **Software Publishing** tab.

5   On the **Software Publishing** tab, enter the details and select the settings for publishing this software resource.

See "Software Publishing tab" on page 120.

6   In the right pane, click **Save changes**.

7   Close the managed delivery page.

Add User dialog box

This dialog box lets administrators define the users or groups of users who can request a particular software resource in the **Software Portal**. It also lets managers specify the users or groups of users whose software requests they can process.

The administrators and the managers access the **Add User** dialog box from the following locations:

Administrators	Administrators can access the **Add User** dialog box from the following places in the **Symantec Management Console**:
	
	■ The **Software Publishing** tab that appears when the administrator adds a software resource to the **Software Portal**.
	  See "Adding a software resource to the Software Portal" on page 177.
	■ The **Software Publishing** tab that appears when the administrator adds a Managed Software Delivery policy to the **Software Portal**.
	  See "Adding a Managed Software Delivery policy to the Software Portal" on page 179.

Managers	Managers can access the **Add User** dialog box from their **User Profile** page in the **Software Portal**.

Table 13-3   Options in the **Add User** dialog box

Option	Description
User Domain	Lets you type the domain in which to search for users.
Search for user	Lets you search the specified domain for a specific user or a group of users. You can type part of the user name or group name, or you can leave the search box empty to search all users.
Select users	Displays the search results, from which you can select a user or group to add. You can select and add multiple users and groups.

Configuring the Software Portal settings

Before you use the **Software Portal**, configure the settings that customize its behavior and appearance. You can change these settings at any time after you implement the **Software Portal**.

This task is a step in the process for implementing the **Software Portal**.

See "Implementing the Software Portal" on page 173.

To configure the Software Portal settings

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

2   In the left pane, under **Settings**, click **Software > Software Portal Settings> Software Portal Settings**.

3   On the **Software Portal Settings** page, in the **Maximum number of open requests per user** box, type the number of requests that a user can have open at any time. The default number of requests is three, which is the recommended number.

    A user who exceeds the allowed number of requests cannot create a new request until one of their other requests is closed.

    A Managed Software Delivery policy that contains dependencies or multiple tasks counts as one request.

4   On the **Software Portal Settings** page, under **UI Settings**, specify the following information:

Company logo	Lets you brand the **Software Portal** with your organization's logo or another image.
	Specify an image file to add to the **Software Portal** display. The image appears in the upper-right corner of the **Software Portal** window.
	Specifications for the image file are as follows:
	■ Format: JPG, GIF, BMP, PNG.
	■ Maximum recommended image dimensions: 80 pixels wide by 20 pixels high.
	■ Image resolution: The resolution is not restricted but we recommend a low resolution such as 72 pixels per inch to conserve bandwidth.

Company name	Type the name of your organization as it should appear in the **Software Portal** window.

5   Click **Save changes**.

Reviewing and approving software requests

This chapter includes the following topics:

■ Administrator Portal page

■ Finding and filtering software requests

■ Processing a software request on the Administrator Portal page

Administrator Portal page

This page lets an administrator view and approve the users' software requests.

The **Administrator Portal** page appears in the **Symantec Management Console** on the Notification Server computer and is available to the **Software Portal** administrator. The **Software Portal** administrator approves special requests and can also approve any requests if a manager is not available. The administrator also delivers the approved software that is not in the Software Catalog or that is not assigned to the user.

Table 14-1   Sections on the **Administrator Portal** page

Section	Description
Filtering options	Lets you use filter options to find specific types of software requests.
	Table 14-2
	See "Finding and filtering software requests" on page 184.

Table 14-1   Sections on the **Administrator Portal** page *(continued)*

Section	Description
Requested Software	Lets you review the software requests and decide what action to take. See "Processing a software request on the Administrator Portal page" on page 185. See "About the approval of software requests" on page 165.

Table 14-2   Options in the **Filtering Options** section

Option	Description
Status	Lets you search for the requests with one of the following statuses: ■ **Approve** ■ **Deny** ■ **Open** ■ **On Hold**
Request type	Lets you search for the requests that are for listed or unlisted software.
Request Category	Lets you search for the requests that are in one of the following categories: ■ **Approved Software** ■ **Software Requiring Approval** ■ **Approved Managed Delivery** ■ **Managed Delivery Requiring Approval** ■ **All Approved** ■ **All Requiring Approval**
Assignment	Lets you search for the requests that are assigned to either the administrator or a manager.
Managers	Lets you search for the requests that are assigned to a specific manager.

Finding and filtering software requests

You can search for specific types of software requests on the **Administrator Portal** page.

To find and filter software requests

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

2   In the left pane, under **Settings**, click **Software > Software Portal Settings > Administrator Portal**.

3   On the **Administrator Portal** page, expand the **Filtering options** section.

4   Select the filter criteria.

    See "Administrator Portal page" on page 183.

5   Click **Search**.

Processing a software request on the Administrator Portal page

Some software requests require an administrator to approve or take other action on a software request. To process a software request, you change its status.

The request statuses that you can set are as follows:

■   **Approve**

■   **On Hold**

■   **Deny**

See "Statuses of software requests in the Software Portal" on page 170.

See "About the approval of software requests" on page 165.

To process a software request on the Administrator Portal page

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

2   In the left pane, under **Settings**, click **Software > Software Portal Settings > Administrator Portal**.

3   On the **Administrator Portal** page, under **Requested Software**, select the software request.

    Only the requests that require your attention are displayed. Use the search feature to find and display other requests if necessary.

    See "Finding and filtering software requests" on page 184.

4   Take either of the following actions:

    ■   To open the request for review, comments, or a status change, click **Edit**.

- ■ To quickly change the status without opening the request, click **Change Status** and on the **Change Status** menu, select the status.

5   If you opened the software request, in the **Listed Software Request Details** dialog box or the **Unlisted Software Request Details** dialog box, take any of the following actions:

- ■ Change the status.

- ■ Enter comments to explain why you have changed the status or to request additional information.
  Comments are required whenever you change the status.

- ■ To review the request's comments and actions, expand the **Request History** section.

6   If this request is for unlisted software, you can click one of the following links:

Import new software resource	If you know that the software resource is not in the Software Catalog, click this link to import it. The **Import Software** wizard opens.
	For more information, see the topics about importing a package to create a software resource in the *Symantec Management Platform Help*.
Search for available software resource	The software resource might be in the Software Catalog. However, it might not have been published at all or it might not have been published for this user. Click this link to open the Software Catalog so you can determine if the requested software is in the catalog.
Create Quick Delivery task	If the software resource is in the Software Catalog, click this link to start the **Quick Delivery** wizard and create a Quick Delivery task.
	See "Creating a Quick Delivery task with the Quick Delivery wizard" on page 134.
Create Managed Delivery task	If the software resource is in the Software Catalog, click this link to start the **Managed Software Delivery** wizard and create a Managed Software Delivery policy.
	See "Creating a Managed Software Delivery policy with the Managed Software Delivery wizard" on page 106.

7   In the **Listed Software Request Details** dialog box or the **Unlisted Software Request Details** dialog box, click **OK**.

8   If you approve a request for the unlisted software, take steps to obtain the software.

Section **4**

Managing applications on client computers

Managing Windows Installer applications

This chapter includes the following topics:

About managing Windows Installer applications

You can create policies and tasks to manage Windows Installer applications on managed computers. The policies and the tasks work with Windows Installer to enhance its functionality.

You can manage Windows Installer applications in the following ways:

Initiate the repair of Windows Installer applications.	You can proactively identify and repair broken applications on selected computers. If an application needs repair, a repair command is sent to the Windows Installer service to initiate self-repair.
	You can use a policy or a task to identify the applications that need repair.
	See "About Windows Installer repair" on page 193.
Update the source paths for Windows Installer applications.	You can update the source paths of Windows Installer applications with resilient source paths. The updated source paths point to the package servers that you designate. If an application needs modification or repair, Windows Installer can access the needed installation file from one of these servers.
	You can use a policy or a task to update the source paths.
	See "About source path updates for Windows Installer applications" on page 198.
View reports to monitor the state of Windows Installer applications.	When you create policies or tasks to manage Windows Installer applications, data is gathered on broken applications and inaccessible source paths. The Application Management reports that are listed under the Software reports display this data. Use this data to monitor the state of Windows Installer applications. For example, the **Software Resources - Broken Elements** report displays the computers that had broken applications during a specified date range. For each computer, the report lists each occurrence of a broken application and identifies its broken element.
	See "Running a Software Management Solution report" on page 83.

About Windows Installer repair

You can proactively identify and repair broken applications on selected computers. If an application needs repair, a repair command is sent to the Windows Installer service to initiate self-repair.

You can repair Windows Installer applications with a policy or task as follows:

Policy   Use a policy as your primary means to repair Windows Installer applications. A policy not only repairs the applications that are currently broken, but it can also repair any applications that break in the future. To repair current and future applications, schedule the policy to run on a recurring basis.

           A policy can perform a quick repair or a full repair.

Task   Typically, you use a task to repair a specific application. For example, if a user reports a broken application, you can create a task to repair that specific application on that user's computer.

           A task can perform a full repair only.

See "Types of Windows Installer repairs" on page 193.

See "Repairing Windows Installer applications" on page 194.

The Software Management Solution agent must be installed on the client computers for you to perform Windows Installer repairs.

See "Installing the Software Management Solution agent" on page 38.

Instead of using a Windows Installer Repair policy or task to repair Windows Installer applications, you can use the remediation feature of Managed Software Delivery. Managed Software Delivery provides more control over the criteria that are used to determine when a repair is needed. Instead of a predefined key path, it uses the meta data that is associated with the software resource, which your Software Catalog administrator defines. Managed Software Delivery can also repair multiple software resources with a single policy. A Windows Installer Repair policy or task can repair one application or all applications.

See "About policy applicability, compliance, and remediation" on page 102.

See "About managing Windows Installer applications" on page 192.

Types of Windows Installer repairs

Before you repair Windows Installer applications on managed computers, determine the type of repair to perform.

Table 15-1   Types of Windows Installer repairs

Features	Windows Installer Quick Repair	Windows Installer Full Repair
Type of scan	Runs a quick scan that identifies Windows Installer applications and verifies that each component's key path is installed correctly. If the component's key path is not installed correctly, the policy tries to repair the component and reports the results. For example, if the Microsoft Word key path file, winword.exe, is not installed in the correct path, the policy tries to repair Word.	Runs a quick scan, like the quick repair, and then runs a deep scan. The deep scan identifies Windows Installer applications and verifies that all of the component's resources are installed correctly. If any element of a component is not installed correctly, the policy or the task repairs that component and reports the results.
Scan time and resources	A Windows Installer Quick Repair takes less time and fewer resources than a Windows Installer Full Repair.	A Windows Installer Full Repair takes more time and resources than a Windows Installer Quick Repair.
What it discovers	A quick repair discovers only broken or missing key paths. If a component has other missing or broken files, a quick repair might not repair them.	A full repair discovers every Windows Installer application that needs repair while a quick repair might not.
Method for performing the repair	Use a policy.	Use a policy or a task.

See "Repairing Windows Installer applications" on page 194.

Repairing Windows Installer applications

You can proactively identify and repair broken Windows Installer applications on managed computers even before the user encounters a problem. These repairs can save time for both you and the user.

You can use a policy or a task to repair Windows Installer applications on managed computers.

See "About Windows Installer repair" on page 193.

Table 15-2 Process for repairing Windows Installer applications

Step	Action	Description
Step 1	Configure a policy or create a task.	Configure a Windows Installer Repair policy to check and repair Windows Installer applications on a recurring basis.
		See "Configuring a Windows Installer Repair policy" on page 195.
		Create a Windows Installer Repair task to repair a specific application.
		See "Creating a task in Software Management Solution" on page 142.
		See "Windows Installer Repair settings" on page 196.
Step 2	(Optional, task only) Change the task settings.	Every task inherits the default settings that control how it runs. You can override the default settings for a particular task.
		See "Advanced options for tasks in Software Management Solution" on page 70.
		You cannot change the settings for a Windows Installer Repair policy.
Step 3	(Task only) Schedule the task and select the delivery destinations.	Your options for scheduling the task are as follows:
		■ Run the task now. This option runs the task as soon as possible, unless it must wait for a maintenance window.
		■ Schedule the task to run at a specific time.
		See "Scheduling a task and selecting computers in Software Management Solution" on page 144.
		This additional step is not necessary for the policy because you schedule it as part of its configuration.
Step 4	View the Application Management reports that identify broken elements.	These reports display the Windows Installer applications that had broken elements during a specified time range. The reports also identify the element that is broken. If an application could not be repaired, the **Software Resources - Current Broken Elements** report displays details about why the repair failed.
		Use these reports to help you resolve broken Windows Installer applications. These reports are listed under the Software reports.
		See "Running a Software Management Solution report" on page 83.

Configuring a Windows Installer Repair policy

You can repair Windows Installer applications on managed computers by configuring a Windows Installer Repair policy. Typically, you use a policy to check

and repair Windows Installer applications on a recurring basis. Configuring the policy is a step in the process for repairing Windows Installer applications.

See "Repairing Windows Installer applications" on page 194.

After you configure the policy, it runs as scheduled on the specified computers or for the specified users. Whenever the policy discovers a broken application, it initiates a repair. If you schedule the policy to repeat, it can continue to check and repair the applications.

You can clone a Windows Installer Repair policy to create policies with different schedules for different computers. Use the context menu to clone a policy.

See "About Windows Installer repair" on page 193.

To configure a Windows Installer Repair policy

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

2   In the left pane, under **Settings**, click **Software > Application Management > Windows**, and then click one of the following options:

■   **Windows Installer Full Repair**

■   **Windows Installer Quick Repair**

See "Types of Windows Installer repairs" on page 193.

3   In the right pane, under **Schedule**, specify the schedule for the policy.

To run this policy on a recurring basis, under **Schedule**, click **No repeat** and then, in the **Repeat Schedule** dialog box, select the repeat interval.

For more information, see the topics about specifying a policy schedule in the *Symantec Management Platform Help*.

4   Under **Applied to**, specify the computers or users to which the policy applies.

For more information, see the topics about applying a policy to targets, computers, resources, and users in the *Symantec Management Platform Help*.

5   Turn on the policy.

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

6   Click **Save changes**.

Windows Installer Repair settings

This section lets you define or edit the details of a Windows Installer Repair task, including the software to repair.

See "About Windows Installer repair" on page 193.

See "Creating a task in Software Management Solution" on page 142.

When you edit a Windows Installer Repair task, the **Task Status** section appears beneath the **Windows Installer Repair Settings** section on the page. Under the **Task Status** section, you can schedule the task, select the destination computers, and view the status of the task.

See "Scheduling a task and selecting computers in Software Management Solution" on page 144.

Table 15-3   Windows Installer Repair settings

Option	Description
Name When you edit a task, this option is not labeled. In the upper left of the task page, you can click the existing name to edit it.	Identifies this task in any list of tasks throughout the product. Make the name descriptive enough for others to easily identify this task and what it does. Follow your organization's standards for naming tasks, if any.
Description When you edit a task, this option is not labeled. In the upper left of the task page, you can click the existing description to edit it.	Provides further information about this task. Do not include critical information in the description because it is not intended to appear in all the lists that contain the name.
All Windows Installer applications	Repairs all Windows Installer applications.
Selected Windows Installer application	Repairs the selected Windows Installer application.
Advanced	Lets you change the settings that control how this task runs. See "Advanced options for tasks in Software Management Solution" on page 70.

See "Creating a task in Software Management Solution" on page 142.

See "Editing a task in Software Management Solution" on page 143.

About source path updates for Windows Installer applications

On managed computers, you can update the source paths of Windows Installer applications with resilient source paths.

When a Windows Installer application is broken, Windows Installer can repair or modify it, but only if the original installation file is accessible. When Windows Installer tries to modify or repair an application, it uses the application's source path to access the installation file. This source path is based on the application's package code. Without resilient source paths, if the installation file is no longer available, the modification or repair fails. With resilient source paths, Windows Installer can look for the installation file on a set of package servers that you designate.

For example, the software delivery policies and tasks in Software Management Solution typically install packages from a package server. If that package server becomes unavailable, a Windows Installer application that was installed from that server cannot be repaired. To avoid this problem, update the application's source paths to point to additional servers from which the installation file can be accessed.

You can perform resilient source path updates of Windows Installer applications with a policy or a task as follows:

Policy
: Use a policy as your primary means to update the source paths of Windows Installer applications. A policy can update the source paths of existing applications, but also the source paths of the applications that are installed in the future. To include the applications that are not yet installed, schedule the policy to run repeatedly.

  A Source Path Update policy updates all the Windows Installer applications that are installed on the client computer.

Task
: Use a task when you need to update the source path of a specific application and the update needs to be done immediately. For example, a Windows Installer repair might fail because the server that distributed the application is out of service. You can create a task to update the source path for that application.

  A Source Path Update task can update a specific application or all the Windows Installer applications that are installed on the client computer.

See "Updating the source paths of Windows Installer applications" on page 199.

The Software Management Solution agent must be installed on the client computers for you to update source paths.

See "Installing the Software Management Solution agent" on page 38.

See "About managing Windows Installer applications" on page 192.

Updating the source paths of Windows Installer applications

You can update the source paths of Windows Installer applications with resilient source paths. The updated source paths point to the package servers that you designate. If an application needs modification or repair, Windows Installer can access the needed installation file from one of these servers.

You can use a policy or a task to perform resilient source path updates of Windows Installer applications on managed computers.

See "About source path updates for Windows Installer applications" on page 198.

Table 15-4   Process for updating source paths for Windows Installer applications

Step	Action	Description
Step 1	Configure a policy or create a task to update the source paths of Windows Installer applications.	A Source Path Update policy or task adds resilient source paths to Windows Installer applications on managed computers. See "Configuring a Source Path Update policy" on page 200. See "Creating a task in Software Management Solution" on page 142. You can also create a Source Path Update task from a software resource in the Software Catalog. If you create the task from a software resource, you select the computers that the task applies to and the task runs immediately.
Step 2	(Optional, task only) Change the task settings.	Every task inherits the default settings that control how it runs. You can override the default settings for a particular task. See "Advanced options for tasks in Software Management Solution" on page 70. You cannot change the settings for a Source Path Update policy.

| | Table 15-4 | Process for updating source paths for Windows Installer applications *(continued)* |

Step	Action	Description
Step 3	(Task only) Schedule the task and select the delivery destinations.	Your options for scheduling the task are as follows: ■ Run the task now. This option runs the task as soon as possible, unless it must wait for a maintenance window. ■ Schedule the task to run at a specific time. See "Scheduling a task and selecting computers in Software Management Solution" on page 144. This additional step is not necessary for the policy because you schedule it as part of its configuration.
Step 4	View the **Software Resources - Inaccessible Source Paths** report.	This report lists the computers that had Windows Installer applications with inaccessible source paths during the most recent scan. Use this report to identify the changes that you need to make to resolve inaccessible source path problems. This report is one of the Application Management reports that is listed under the Software reports. See "Running a Software Management Solution report" on page 83.

Configuring a Source Path Update policy

You can update the source paths of Windows Installer applications with resilient source paths by configuring a Source Path Update policy. Configuring the policy is a step in the process of updating the source paths of Windows Installer applications.

See "Updating the source paths of Windows Installer applications" on page 199.

After you configure the policy, it runs as scheduled on the specified computers or for the specified users. If you schedule the policy to repeat, it can continue to check and update the source paths.

See "About source path updates for Windows Installer applications" on page 198.

To configure a Source Path Update policy

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

2   In the left pane, under **Settings**, click **Software > Application Management > Windows > Source Path Update**.

3   In the right pane, on the **Source Path Update** page, under **Settings**, specify the package servers to use as follows:

First Server to Use	Lets you select the first server to use as a source path. You can click **Any Server** or you can select a specific server from the list. The package server that you select must be accessible to the computers that are specified in the policy.
	To optimize bandwidth, select specific package servers to serve as the source paths for Windows Installer applications. Servers between the first and last are used in order of response speed.
	If you do not select specific package servers, the update begins with the fastest-responding server and works toward the slowest. It then ends with the Notification Server computer.
Last Server to Use	Lets you select the last server to use as a source path. You can click **Any Server** or you can select a specific server from the list. The package server that you select must be accessible to the computers that are specified in the policy.

4   In **Maximum Number of Servers** type the maximum number of servers to use for the source path update.

5   Under **Schedule**, specify the schedule for the policy.

To run this policy on a recurring basis, under **Schedule**, click **No repeat** and then, in the **Repeat Schedule** dialog box, select the repeat interval.

For more information, see the topics about specifying a policy schedule in the *Symantec Management Platform Help*.

6   Under **Applied to**, select the computers or users to which the policy applies.

For more information, see the topics about specifying the targets of a policy or task in the *Symantec Management Platform Help*.

7   Turn on the policy.

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

8   Click **Save changes**.

Configuration settings for Source Path Update tasks

(Windows only)

This section lets you define or edit the details of a Source Path Update task, including the software to update and the servers to use.

See "About source path updates for Windows Installer applications" on page 198.

See "Creating a task in Software Management Solution" on page 142.

When you edit a Source Path Update task, the **Task Status** section appears beneath the **Configuration settings** section on the page. Under the **Task Status** section, you can schedule the task, select the destination computers, and view the status of the task.

See "Scheduling a task and selecting computers in Software Management Solution" on page 144.

Table 15-5   Configuration settings for Source Path Update tasks

Option	Description
Name When you edit a task, this option is not labeled. In the upper left of the task page, you can click the existing name to edit it.	Identifies this task in any list of tasks throughout the product. Make the name descriptive enough for others to easily identify this task and what it does. Follow your organization's standards for naming tasks, if any.
Description When you edit a task, this option is not labeled. In the upper left of the task page, you can click the existing description to edit it.	Provides further information about this task. Do not include critical information in the description because it is not intended to appear in all the lists that contain the name.
All Windows Installer applications	Updates the source paths for all Windows Installer applications.
Selected Windows Installer application	Updates the source paths for a specific Windows Installer application. Click the **Select Software** link to the right of this option to select the software resource to update.

Table 15-5   Configuration settings for Source Path Update tasks *(continued)*

Option	Description
First Server to Use	Lets you select the first server to use as a source path. You can click **Any Server** or you can select a specific server from the list. The package server that you select must be accessible to the computers that are specified in the policy.
	To optimize bandwidth, select specific package servers to serve as the source paths for Windows Installer applications. Servers between the first and last are used in order of response speed.
	If you do not select specific package servers, the update begins with the fastest-responding server and works toward the slowest. It then ends with the Notification Server computer.
Last Server to Use	Lets you select the last server to use as a source path. You can click **Any Server** or you can select a specific server from the list. The package server that you select must be accessible to the computers that are specified in the policy.
Maximum Number of Servers	Lets you type the maximum number of servers to use for the source path update.
Advanced	Lets you change the settings that control how this task runs.
	See "Advanced options for tasks in Software Management Solution" on page 70.

See "Creating a task in Software Management Solution" on page 142.

See "Editing a task in Software Management Solution" on page 143.

About the Application Management agent

The policies and the tasks that perform Windows Installer repairs or source path updates use the Application Management agent. When these tasks or these policies run on managed computers, they install the agent if it is not already installed. The Application Management agent works with Windows Installer to help you manage Windows Installer applications.

See "About managing Windows Installer applications" on page 192.

The Application Management agent also gathers data about Windows Installer applications on managed computers. You can view this data on the Application

Management reports that are listed under the Software reports. Create your own policies and tasks only if the predefined policies and tasks do not meet your needs.

See "Running a Software Management Solution report" on page 83.

A software resource for the Application Management agent is created in the Software Catalog when Software Management Solution is installed. You can use this software resource to create your own policies and tasks to repair Windows Installer applications or to update their source paths.

See "Creating customized Windows Installer policies and tasks" on page 204.

You can determine where the Application Management agent is installed. Create a Targeted Software Inventory policy for the Application Management agent's software resource so you can look for the agent on selected client computers.

For more information, see the topics about Targeted Software Inventory in the *Inventory Solution Help*.

Creating customized Windows Installer policies and tasks

A software resource for the Application Management agent is created in the Software Catalog when Software Management Solution is installed. You can use this software resource to create your own policies and tasks to repair Windows Installer applications or to update their source paths. Create your own policies and tasks only if the predefined policies and tasks do not meet your needs.

See "About the Application Management agent" on page 203.

Table 15-6   Process for creating and customizing Windows Installer policies and tasks

Step	Action	Description
Step 1	Create a customized command line for the Application Management agent package in the Software Catalog.	You can either edit an existing command line or create a new command line. See "Command-line options for the Application Management agent" on page 205. For more information, see the topics about adding and editing command lines in the *Symantec Management Platform Help*.

Table 15-6   Process for creating and customizing Windows Installer policies and
                  tasks *(continued)*

Step	Action	Description
Step 2	Deliver the Application Management agent with the customized command line.	You can use Quick Delivery or Managed Software Delivery to deliver the agent. In Managed Software Delivery, you can create the command line when you create the policy. See "Creating a Managed Software Delivery policy with the Managed Software Delivery wizard" on page 106. See "Creating a Quick Delivery task with the Quick Delivery wizard" on page 134.

Command-line options for the Application Management agent

A software resource for the Application Management agent is created in the Software Catalog when Software Management Solution is installed. You can use this software resource to create your own policies and tasks to repair Windows Installer applications or to update their source paths. You deliver the agent with a command line that runs the agent according to your specifications. You use the Application Management agent command-line options to create the command line.

See "Creating customized Windows Installer policies and tasks" on page 204.

See "About the Application Management agent" on page 203.

For more information, see the topics about creating a command line in the *Symantec Management Platform Help*.

The executable file for the Application Management agent is Aexmsiagent.exe. The command lines must use the following format:

`Aexmsiagent.exe /option parameter`

The command-line options for the Application Management agent adhere to the following standards:

- They can be standalone options or they can take parameters.

- They are not case sensitive.

- They can use environment variables.

■ If they use GUIDs, the GUIDS must be formatted as follows:
{8E1FC9E1-8ACC-4e1c-9D6C-F217C0223B7D}

Table 15-7 Command-line options for the Application Management agent

Option	Description and parameters
/?	Displays a help dialog box.
/AddSourcePath	Adds a source path to the list of valid sources for the specified product. If another source in the set was used to install the product, the new source is not used unless the current source is unavailable. This option takes the following parameters: ■ *ProductID* The GUID of the product to add the source path to. ■ *User* The user name of the user whose product installation is modified. For all users, type **all**. For a local user, type the user name in one of the following formats: ***domain\user name*** ***computer name\user name***. ■ *Path* The source path to add to the list of valid sources for the specified product. ■ *ClearSourceList* Specify **Yes** or **True** to clear all other source paths from the source list and then add this source path as the only entry in the list. Type **No** or **False** to append this source path to the source list.
/Collect	Runs the Inventory Collector and sends Windows Installer information to the Notification Server computer if the Altiris Agent is running on the computer.
/ExcludeComponents *IDs*	Excludes the specified components. For *IDs*, type a semicolon-delimited list of the component names or GUIDs. Excluding components from the processing reduces the agent's run time.
/ExcludeProducts *IDs*	Excludes the specified products. For *IDs*, type a semicolon-delimited list of the product names or GUIDs. Excluding products from the processing reduces the agent's run time.

Table 15-7   Command-line options for the Application Management agent
(continued)

Option	Description and parameters
`/first=`*Computer Name*	Specifies the first package server that Windows Installer should check for source files during an update of source paths for an application. For *Computer Name*, type the computer name of the package server to check. This option can be used with the following options: ■ `/nbest` ■ `/last` ■ `/UpdateSourcePaths`
`/ICFilePath` *file path*	Specifies an alternate Inventory Collector program, where *file path* is the program's full path and file name. After the Application Management agent creates its output, it invokes the Inventory Collector to process the output. The inventory collector prepares the output for loading into the Configuration Management Database. By default, the agent assumes that the Inventory Collector program is in the same directory as the agent. The Inventory Collector program is AeXNSInvCollector.exe.
`/IncludeComponents` *IDs*	Processes only the specified components. For *IDs*, type a semicolon-delimited list of the component names or GUIDs. Limiting the components that are processed reduces the agent's run time.
`/IncludeProducts` *IDs*	Processes only the specified products. For *IDs*, type a semicolon-delimited list of the product names or GUIDs. Limiting the products that are processed reduces the agent's run time.
`/last=`*Computer Name*	Specifies the last package server that Windows Installer should check for source files during an update of source paths for an application. For *Computer Name*, type the computer name of the package server to check. This option can be used with the following options: ■ `/nbest` ■ `/first` ■ `/UpdateSourcePaths`
`/LFile` *file name*	When logging is enabled, log messages are written to Aexmsiagent.log by default. Use this option to specify an alternate log file, where *file name* is the path name and file name. If a path is not specified, the file is written to the current executable directory. This option is used with `/Log`.

	Table 15-7	Command-line options for the Application Management agent *(continued)*

Option	Description and parameters
/LLevel	When logging is enabled, log messages contain only errors and warning by default. Use this option to specify the types of messages to log.
	This option is used with /Log.
	This option takes one or more of the following parameters:
	■ all Log all messages ■ I Log information level messages ■ w Log warning level messages ■ e Log error level messages ■ d Log debug messages
	Do not separate the parameters with spaces or other characters. For example, the following command logs error and information level messages:
	Aexmsiagent.exe /Log /LLevel ei
/Log	Enables logging to disk. The default log file is Aexmsiagent.log.
/Lsize *x*	Sets the maximum number of bytes that a log file can reach before it is backed up and a new log file is started. For *x*, type the number of bytes to allow.
	The default maximum size is 1,024,000. The minimum size that is allowed is 2,048. Any size less than that is set to 2,048.
/nbest=*number*	Specifies the number of package servers that Windows Installer should check for source files during an update of source paths for an application. For *number*, type the number of servers to check. Leave this option blank for an unlimited number of package servers.
	This option can be used with the following options:
	■ /first ■ /last ■ /UpdateSourcePaths
/NoDeepScan	Scans only the component's key file instead of performing a deep scan on the component's resources (files, shortcuts, and registry entries).
	See "Types of Windows Installer repairs" on page 193.

Option	Description and parameters
`/NoShortcuts`	Prevents the agent from trying to verify (deep scan) shortcuts during its scan.
`/Output format`	Specifies the type of output the agent produces. For *format*, type **xml** because the output must be in XML format.

`/Repair`	Specifies whether a component should be repaired, where the *options* parameter is one or more characters that represent the component's state. If the agent finds a component in one of the specified states, the agent immediately tries to repair the component. The agent then reports on the status of the repair.
	
	This option takes one or more of the following parameters:
	
	■ `All`
	  Repair items in any of the possible states
	■ `a`
	  Repair absent (missing) items
	■ `b`
	  Repair broken items
	■ `c`
	  Repair corrupted items
	■ `I`
	  Repair incomplete items
	
	Do not separate the parameters with spaces or other characters. For example, the following command repairs any features or components in an absent state or a corrupted state:
	
	`Aexmsiagent.exe /Repair ac`

`/RepairTO seconds`	Specifies the time that the Application Management agent waits for Windows Installer to complete a repair before the agent terminates it. For *seconds*, type the number of seconds to wait. The default value is 300 seconds.
`/Sleep x`	Specifies the number of milliseconds that the agent should wait each time the throttle threshold is reached. This option reduces the load on the CPU at run time. For *x*, type the number of milliseconds to wait. The default value is 150. This option is used with the `/Throttle` option to modify the performance of the agent.
`/SystemLevelScan`	Scans the products that are installed per-machine, and ignores the specific user values.

| Table 15-7 | Command-line options for the Application Management agent *(continued)* |

Option	Description and parameters
/Throttle *x*	Specifies the number of items to process before the throttle threshold is reached. For *x*, type the number of items to process. The default value is 20.
	When the threshold is reached, the agent waits the number of milliseconds specified by the /Sleep option and then proceeds. Because feature objects and component objects are the most numerous and the most common, they are used for the throttle count "item."
/UI	Displays a user interface on the user's computer. The interface displays details about each Windows Installer application and lets the user selectively scan and repair broken applications.
/UpdateSourcePaths	Updates the source paths for all applications.
	This option can be used with the following options:
	■ /first ■ /last ■ /nbest
/Visible	Displays any errors that occur while the agent runs.

Managing virtual applications

This chapter includes the following topics:

About managing virtual applications

Software virtualization lets you install Windows-based applications into virtual software layers.

See "About software virtualization" on page 212.

Virtual software layers facilitate the management of software on client computers as follows:

You avoid conflicts between applications.	A virtual application always uses the correct files and registry settings and does not modify the operating system or interfere with other applications. You can even install two versions of the same application on the same computer.
You can repair broken applications quickly.	If an application is broken, you can quickly reset its layer to restore the application to its original installed state. When an application's layer is reset, other applications that are installed on the computer cannot be damaged.
You can easily roll back to an earlier version.	When you install a new version of an application, you can deactivate the earlier version. If the new version causes problems, you can easily deactivate it and activate the earlier version.

Software Management Solution lets you perform the following virtualization actions:

- Virtualize applications during a Managed Software Delivery installation.
  See "Methods for virtualizing software" on page 219.
- Deliver and manage virtual layers with any delivery policy or task in Software Management Solution.
  See "Methods for installing and managing virtual software" on page 221.

About software virtualization

Software virtualization lets you create virtual software layers. These layers consist of one or more Windows-based applications or sets of data. A virtual software layer contains all the files and registry settings of the application or the set of data.

Software virtualization requires that a licensed version of the Software Virtualization agent is installed on the client computers.

See "Installing the Software Virtualization agent" on page 47.

When you install a virtual software layer on a computer, the contents of the layer are placed in a protected folder on the hard drive. This protected folder is referred to as the redirection area. The files and registry settings of a layer are placed in subfolders in the redirection area. When you activate a layer on a computer, its contents are layered over the base file system and registry. The contents of the layer appear where they would be if they were installed with a normal installation.

For example, if you install a virtual software layer for Firefox, its files are placed in a subdirectory of C:\fslrdr. After you activate the layer for Firefox, the filter driver displays the files for Firefox in C:\Program Files.

To accomplish this virtualization, software virtualization uses a file system filter driver. This filter driver intercepts requests to the file system and the registry and redirects the requests to the active layer. The filter driver aggregates the real file system and the virtual file system into one view for the user. This filter driver is the main component of the Software Virtualization agent.

Because software virtualization uses redirection, it can maintain discrete settings and file versions for different applications on a single computer. When you use software virtualization, a required version of a file is never overwritten and the problem of conflicting DLL files is eliminated.

See "Managing virtual applications" on page 217.

See "About virtual software archive files" on page 214.

See "About preventing the loss of virtual application data" on page 215.

See "About exclude entries for virtual software layers" on page 215.

See "About data layers" on page 217.

About the applications that you can virtualize

(Windows only)

Use the following guidelines to determine what you can and cannot virtualize:

What you can virtualize — Most Windows-based applications can be virtualized, including the following types of applications:

- Office applications
- Databases
- Internet browsers except for Internet Explorer
- Media
  Spyware utilities

Virtual applications function normally, and all configuration options are available to the user.

What you cannot virtualize	You cannot virtualize the following applications or files:

- Windows operating system components including Internet Explorer
- Windows operating system patches
- Drivers
- Applications that have dedicated drivers
  For example, client firewalls.
- All management agents including antivirus software, security scanners, encryption agents, or any agent that is used in the Symantec Management Platform
- Data files that you plan to encrypt
- The diagnostic utilities or recovery utilities that run in safe mode
  Software virtualization does not run in safe mode.

See "About managing virtual applications" on page 211.

See "Methods for virtualizing software" on page 219.

About virtual software archive files

A virtual software archive (VSA) file is a portable virtual software layer, which installs one or more Windows-based applications or sets of data.

See "About managing virtual applications" on page 211.

You can use either of the following tools to repackage an application's installation file to create a VSA file:

- Wise Package Studio 7.0 or later

- Software Virtualization Solution or its new version, which is called Symantec Workspace Virtualization.

You can create a software resource for a VSA file in the Software Catalog. When you create the software resource, you can add the VSA file to the Software Library. In the Software Catalog, you can edit the software resource. For example, you can define associations and additional command lines. The **VSA Command Line Builder** makes it easy to create syntactically-correct command lines for the software resource of a VSA file.

For more information, see the topics about the Software Catalog and software resources in the *Symantec Management Platform Help*.

After you create the software resource for a VSA file in the Software Catalog, you can use any delivery method to deliver it. You can also deliver a VSA file with a Software Virtualization task.

See "Methods for delivering software" on page 88.

See "Installing and managing a virtual software layer with a Software Virtualization task" on page 225.

When you deliver a VSA file, the Software Virtualization agent installs it to create a virtual software layer. After the layer is created and activated, its files and registry settings become visible. If the layer contains an application, the application functions as if it were not in a layer.

See "About software virtualization" on page 212.

About preventing the loss of virtual application data

(Windows only)

If a virtual application saves data in the virtual software layer, the data is lost when the layer is reset. To prevent the loss of application data, ensure that the application data is not saved in the application's layer.

See "About managing virtual applications" on page 211.

The application data is not saved in the application's layer in the following situations:

■ When the data is excluded with an exclude entry.
  An exclude entry excludes files from a layer and saves them in the base file system instead.
  See "About exclude entries for virtual software layers" on page 215.

■ When the data is saved in a data layer.
  You can create and deploy data layers to capture application data. When a data layer captures data from a virtual application, it is excluded from the application's layer.
  See "About data layers" on page 217.

■ When the data is not saved locally.
  For example, if a virtual application creates data and the data is saved on a network share, the data is excluded from the application's layer.

See "About software virtualization" on page 212.

About exclude entries for virtual software layers

(Windows only)

Exclude entries prevent the loss of data that a virtual application creates or modifies.

See "About preventing the loss of virtual application data" on page 215.

When a virtual application creates or modifies application data, the data files can be saved in the application layer. If the layer is reset, the files are lost. An exclude entry excludes files from a layer and saves them in the base file system instead. An exclude entry can exclude a file type or a directory. If an exclude entry excludes a directory, it can also exclude its subdirectories.

Exclude extries can be created with the following products:

- Any WiseScript product such as WiseScript Editor or WiseScript Package Editor. The **Set SVS Exclude Entry** script action can create exclude entries on client computers.

- Software Virtualization Solution or its new version, which is called Symantec Workspace Virtualization.

For more information about exclude entries, see the respective product's documentation.

Table 16-1   Types of exclude entries

Type	Description
Layer exclude entry	Redirects the files from a specific layer to the base file system.
	For example, a virtual software layer for Microsoft Word can have a layer exclude for the following file types: DOC, RTF, TXT. When Word saves a file with any of these file types, the file is saved in the base file system and not in the layer.
	Note: When you use Managed Software Delivery to virtualize software during installation, the resulting layer has no layer exclude entries.
	See "Virtualizing software during installation" on page 220.
Global exclude entry	Redirects the files for every virtual software layer on a computer to the base file system. For example, a computer can have a global exclude for PDF files. If a layer creates PDF files, the files are excluded from the layer and saved in the base file system.
	By default, when the Software Virtualization agent is installed on a managed computer, global excludes are created for the My Documents and the Desktop directories.

A data layer takes precedence over an exclude entry. If a data layer contains the same data that an exclude entry excludes, the data is saved in the data layer.

See "About data layers" on page 217.

See "About software virtualization" on page 212.

About data layers

(Windows only)

A data layer stores data that would otherwise be written to an application layer or the base file system. You can use a data layer to prevent the loss of data that a virtual application creates or modifies. You can use one or more data layers on a computer.

See "About preventing the loss of virtual application data" on page 215.

You can create data layers in either of the following products:

■ Virtual Package Editor in Wise Package Studio 7.0 or later

■ Software Virtualization Solution or its new version, which is called Symantec Workspace Virtualization.

See "About software virtualization" on page 212.

Managing virtual applications

You can use software virtualization to facilitate the management of most Windows-based software on client computers.

See "About software virtualization" on page 212.

See "About managing virtual applications" on page 211.

Software virtualization requires that a licensed version of the Software Virtualization agent is installed on the client computers.

See "Installing the Software Virtualization agent" on page 47.

| Table 16-2 | | Process for managing virtual applications |

Step	Action	Description
Step 1	Virtualize the software.	The simplest way to virtualize software is to perform the virtualization during installation. See "Methods for virtualizing software" on page 219. See "About the applications that you can virtualize" on page 213. Additional options for virtualizing software are as follows: ■ Repackage an application into a virtual software archive (VSA) file, which is a portable virtual software layer. ■ Import an existing VSA file into the Software Catalog to create a software resource. For more information, see the topics about importing a package to create a software resource in the *Symantec Management Platform Help*.
Step 2	Install the software into a virtual software layer.	You can install the software into a virtual layer on the client computer at the same time that you virtualize the software. See "Virtualizing software during installation" on page 220. You also can use any delivery method to install a VSA file as a new layer and activate it on the client computer. See "Methods for installing and managing virtual software" on page 221.
Step 3	Manage the software that is installed in virtual software layers.	You can create a policy or task that executes a command line for a specific virtual software layer. When the layer command line runs on a managed computer, it performs an action on the layer. For example, if a virtual application is broken, you can create a task that executes a command line to reset the application's layer. The application is quickly restored to its original installed state. See "Methods for installing and managing virtual software" on page 221. See "Actions that you can perform on a virtual software layer" on page 223.
Step 4	View the Virtualized Software Resources reports.	You can use the reports to monitor the state of virtual applications. These reports are listed under the Software reports. See "Running a Software Management Solution report" on page 83.

Methods for virtualizing software

Software virtualization is the creation of virtual software layers. A virtual software layer contains all the files and registry settings of one or more Windows-based applications or sets of data.

See "Managing virtual applications" on page 217.

See "About the applications that you can virtualize" on page 213.

Warning: If a virtual application is reset, it is possible to lose the data that the application creates or modifies. Before you use virtual applications, make sure that you understand how to prevent the loss of application data.

See "About preventing the loss of virtual application data" on page 215.

Table 16-3 Methods for virtualizing software

Method	Description
Virtualize the software during installation	Lets you deliver the vendor's installation file. For example, you can deliver an MSI or EXE. The installation file is virtualized when it is installed. This method is only available with Managed Software Delivery.
	We recommend this method for the following reasons:
	■ It uses the installation file that the vendor created so that you do not have to repackage the installation.
	■ It preserves any logic that the vendor might have added to the installation. For example, an installation might contain logic to install a different DLL file depending on the computer's operating system. If you repackage the software, this logic is lost. A repackaged installation contains the DLL file for only the operating system on which the installation was repackaged.
	See "Virtualizing software during installation" on page 220.

Table 16-3	Methods for virtualizing software *(continued)*

Method	Description
Virtualize the software before installation	This method requires that you repackage the installation file to create a virtual software archive file. A virtual software archive (VSA) file is a portable virtual software layer, which installs one or more Windows-based applications or sets of data.
	Use a tool other than Software Management Solution to perform this step.
	See "About virtual software archive files" on page 214.
	See "Methods for delivering software" on page 88.

Virtualizing software during installation

(Windows only)

When you deliver Windows-based software with a Managed Software Delivery policy, you can select an option to virtualize the software when it is installed. You should virtualize software if it conflicts with other software that could be installed on the same computer. When you virtualize software, you avoid conflicts between that application and other applications.

See "About managing virtual applications" on page 211.

When you select the option to virtualize software during installation, the Managed Software Delivery policy installs the software as follows:

If the Software Virtualization agent is installed on the client computer	The policy performs the following actions:
	■ Deactivates any active layers that are on the client computer.
	■ Installs the software into a new layer. You can specify the layer name in the Managed Software Delivery policy. If you do not provide a layer name, the layer name defaults to the installation file name plus the command-line name.
	■ Reactivates any layers that it deactivated.

If the Software Virtualization agent is not installed on the client computer	The policy installs the software normally.

See "Managing virtual applications" on page 217.

Warning: If a virtual application is reset, it is possible to lose the data that the application creates or modifies. Before you use virtual applications, make sure you understand how to prevent the loss of application data.

See "About preventing the loss of virtual application data" on page 215.

To virtualize software during installation

1   In the **Symantec Management Console**, begin the creation of a Managed Software Delivery policy for the software to be virtualized.

Create the policy in one of the following ways:

- With the Managed Software Delivery wizard
  See "Creating a Managed Software Delivery policy with the Managed Software Delivery wizard" on page 106.

- Without the Managed Software Delivery wizard
  See "Creating a Managed Software Delivery policy" on page 110.

2   In the policy, check **Install this policy's software into a virtual software layer**.

Depending on how you create the policy, this check box appears in one of the following places:

- In the Managed Software Delivery wizard, this check box appears on the **Select software resource** page.
  If the software resource has any defined conflicts with other software resources, those conflicts are listed with this option. Conflict associations between software resources are defined in the Software Catalog.
  For more information, see the topics about defining associations for software resources in the *Symantec Management Platform Help*.

- On the policy's edit page, this check box appears in the **Policy/Rules Actions** section, under **User interaction**.

3   Complete the policy.

See "Performing an advanced software delivery" on page 104.

Methods for installing and managing virtual software

(Windows only)

You can use any delivery task or policy in Software Management Solution to install software into a virtual layer on a client computer. You can use the same methods to manage the layer after it is installed.

The task or policy installs and manages the layer by running a command line that performs actions on the layer.

See "Actions that you can perform on a virtual software layer" on page 223.

Table 16-4   Methods for installing and managing virtual software

Method	Description
Software Virtualization task	Lets you install a virtual software archive (VSA) file to a managed computer and create a new virtual software layer. It also lets you manage any virtual software layer regardless of how the layer was created. Each action requires a separate task, including the installation. You can also add a Software Virtualization task to a job or a Managed Software Delivery policy to perform more complex management tasks. See "Installing and managing a virtual software layer with a Software Virtualization task" on page 225.
Quick Delivery task Package Delivery task	Lets you install a virtual software archive (VSA) file to a managed computer and create a new virtual software layer. It also lets you manage a virtual software layer that was created by installing a virtual software archive file. Each action requires a separate task, including the installation. You can also create a Quick Delivery task or a Package Delivery task and add it to a Managed Software Delivery policy. See "Installing and managing a virtual software layer with a Quick Delivery or Package Delivery task" on page 228.
Managed Software Delivery policy	Lets you perform more complex management tasks. A Managed Software Delivery policy can create and manage new virtual software layers and it can manage existing layers. See "Installing and managing a virtual software layer with a Managed Software Delivery policy" on page 230. You can manage multiple virtual software layers at the same time. For example, you can create a policy that installs a new version of an application into a layer and then deactivates the earlier version. To do so, you can add multiple Software Virtualization tasks, Quick Delivery tasks, or Package Delivery tasks to a Managed Software Delivery policy. See "Delivering multiple software resources and tasks sequentially" on page 126. If you need to manage a single virtual software layer, we recommend that you use one of the other methods.

Actions that you can perform on a virtual software layer

(Windows only)

After you install Windows-based software into a virtual software layer on client computers, you can manage the layer. To do so, you run a command line that performs actions on the layer.

See "Methods for installing and managing virtual software" on page 221.

Table 16-5   Actions that you can perform on a virtual software layer

Action	Description
Activate	Activates a virtual software layer that was installed on a managed computer. When a layer is activated, its contents become visible to the user. If the layer contains an application, the application is fully functional.
Deactivate	Deactivates a virtual software layer that was installed on a managed computer. When a layer is deactivated, it is hidden from the user but is still on the computer.
	If a process from the layer is running, this action fails unless you also select an option to force the operation to complete.
Deactivate and Delete	Deactivates and deletes a virtual software layer that was installed on a managed computer. Before you can delete some applications, you must first deactivate them. For example, you must deactivate Yahoo! Messenger before you can delete it. This action is not available with a Software Virtualization task.
Delete	Deletes a virtual software layer that was installed on a managed computer. This action removes the layer and all of its contents.
Import	Imports (installs) a virtual software archive (VSA) file to a managed computer and creates a new virtual software layer. After you install the VSA file, you must activate the layer to make it functional.
	See "About virtual software archive files" on page 214.

Table 16-5   Actions that you can perform on a virtual software layer *(continued)*

Action	Description
Import and Activate	Imports a VSA file onto a managed computer, creates a new virtual software layer, and activates the layer.
	This action is not available in a Software Virtualization task.
	See "About virtual software archive files" on page 214.
Reset	Resets a virtual software layer to its original installed state.
	Warning: When a layer is reset, it is possible to lose the data that the application creates or modifies.
	See "About preventing the loss of virtual application data" on page 215.
Reset and Activate	Resets a virtual software layer to its original installed state and activates the layer.
	Warning: When a layer is reset, it is possible to lose the data that the application creates or modifies.
	See "About preventing the loss of virtual application data" on page 215.
	This action is not available in a Software Virtualization task.
Reset and Deactivate	Resets a virtual software layer to its original installed state and deactivates the layer. Before you can deactivate some applications that are in a bad state, you must first reset them.
	Warning: When a layer is reset, it is possible to lose the data that the application creates or modifies.
	See "About preventing the loss of virtual application data" on page 215.
	This action is not available in a Software Virtualization task.
Set active on startup	Configures a virtual software layer to be activated when a computer starts. If a layer is not activated on startup, a user can access it only if they can activate it manually.
	This action is not available in a Software Virtualization task.

Table 16-5   Actions that you can perform on a virtual software layer *(continued)*

Action	Description
Set not active on startup	Configures a virtual software layer not to be activated when a computer starts. If a layer is not activated on startup, a user can access it only if they can activate it manually. You might perform this action if a user seldom uses a layer and the layer takes a significant amount of time to activate.
	This action is not available in a Software Virtualization task.

Installing and managing a virtual software layer with a Software Virtualization task

(Windows only)

You can create a Software Virtualization task to deliver and install a virtual software archive (VSA) file on managed computers. You can also use a Software Virtualization task to manage any virtual software layer regardless of how the layer was created.

A Software Virtualization task contains a command line for the specified virtual software layer. When the task runs on a client computer, it executes the command line that performs an action on the layer. Each action requires a separate task, including the installation.

See "Actions that you can perform on a virtual software layer" on page 223.

Table 16-6   Process for managing a virtual software layer with a Software Virtualization task

Step	Action	Description
Step 1	Create a Software Virtualization task.	When you create the task, you select the command to perform and the layer on which to perform the command.
		If you install (import) a layer, you must select a VSA file. If you perform any other command, you can specify any existing layer.
		See "Creating a task in Software Management Solution" on page 142.
		See "Software Virtualization settings" on page 226.
Step 2	(Optional) Change the task settings.	Every task inherits the default settings that control how the task runs. You can override the default settings for a particular task.
		See "Advanced options for tasks in Software Management Solution" on page 70.

| | **Table 16-6** | Process for managing a virtual software layer with a Software Virtualization task *(continued)* |

Step	Action	Description
Step 3	Schedule the task and select the delivery destinations.	Define the schedule and the delivery destinations every time you run the task. Your options for scheduling the task are as follows: ■ Run the task now. This option runs the task as soon as possible, unless it must wait for a maintenance window. ■ Schedule the task to run at a specific time. See "Scheduling a task and selecting computers in Software Management Solution" on page 144.
Step 4	View the Virtualized Software Resources reports.	You can use the reports to monitor the state of virtual applications. These reports are listed under the Software reports. See "Running a Software Management Solution report" on page 83.

See "Managing virtual applications" on page 217.

Software Virtualization settings

(Windows only)

This section lets you define or edit the details of a Software Virtualization task, including the layer that it manages.

See "About managing virtual applications" on page 211.

When you edit a Software Virtualization task, the **Task Status** section appears beneath the **Software virtualization settings** section on the page. Under the **Task Status** section, you can schedule the task, select the destination computers, and view the status of the task.

See "Scheduling a task and selecting computers in Software Management Solution" on page 144.

Table 16-7   Software virtualization settings

Option	Description
Name When you edit a task, this option is not labeled. In the upper left of the task page, you can click the existing name to edit it.	Identifies this task in any list of tasks throughout the product. Because the description does not always appear, make the name descriptive enough for other administrators to easily identify this task.
Description When you edit a task, this option is not labeled. In the upper left of the task page, you can click the existing description to edit it.	Lets you type a description to further identify this task and make it more recognizable. Do not include critical information in the description because it is not intended to appear in all the lists that contain the name.
Software virtualization command	Lets you select the command for the action you want to perform. See "Actions that you can perform on a virtual software layer" on page 223.
Layer name	Lets you define the layer on which to perform the command. Type the name of the layer exactly as it appears on the managed computer. The name is not case sensitive.
File name	Lets you specify the virtual software archive (VSA) file to import. You must type the full path and name of the .VSA file as it appears on the managed computer. You can use a UNC path. This option is enabled for the **Import** command only. See "About virtual software archive files" on page 214.
Force this operation to complete	Lets you force the task to run when it might otherwise fail. For example, a Software Virtualization task fails if a process from the layer is running on the client computer. When you install a layer, if the layer is already on the client computer and you do not check this check box, the task fails. If you check this check box, the task proceeds and replaces the existing layer with the new layer.

Table 16-7   Software virtualization settings *(continued)*

Option	Description
Advanced	Lets you change the settings that control how this task runs. See "Advanced options for tasks in Software Management Solution" on page 70.

See "Creating a task in Software Management Solution" on page 142.

See "Editing a task in Software Management Solution" on page 143.

Installing and managing a virtual software layer with a Quick Delivery or Package Delivery task

(Windows only)

You can create a Quick Delivery or Package Delivery task to deliver and install a virtual software archive (VSA) file on managed computers. You can also use these tasks to manage a virtual software layer that was created by installing a virtual software archive file. If the software was virtualized during a Managed Software Delivery installation, then you must use a Software Virtualization task to manage the layer.

See "Installing and managing a virtual software layer with a Software Virtualization task" on page 225.

A Quick Delivery or Package Delivery task contains a command line for the specified VSA file. When the task runs on a client computer, it executes the command line that performs an action on the layer. Each action requires a separate task, including the installation.

Table 16-8   Process for installing and managing a virtual software layer with a Quick Delivery or Package Delivery task

Step	Action	Description
Step 1	Create a Quick Delivery task or a Package Delivery task.	The options for creating the task are as follows: ■ Use the **Quick Delivery** wizard. See "Creating a Quick Delivery task with the Quick Delivery wizard" on page 134. ■ Create a Quick Delivery task without the wizard. See "Creating a task in Software Management Solution" on page 142. See "Software settings for Quick Delivery tasks" on page 135. ■ Create a Package Delivery task. See "Creating a task in Software Management Solution" on page 142. See "Package settings for Package Delivery tasks" on page 139.
Step 2	In the task, specify the software to install or manage.	Select the software resource that represents the VSA file to install or manage. If you plan to manage an existing layer, select the software resource that contains the VSA file that was installed to create the layer. In a Package Delivery task, you can also specify a VSA package that is not assigned to a software resource.
Step 3	In the task, specify the action to perform.	Select a command line that specifies the action to perform. For example, you can install (import) the layer or you can deactivate an existing layer. See "Actions that you can perform on a virtual software layer" on page 223. In a Package Delivery task, if you selected a VSA file that does not have predefined command lines, you can type a valid command line.
Step 4	(Optional) Change the task settings.	Every task inherits the default settings that control how the task runs. You can override the default settings for a particular task. See "Advanced options for tasks in Software Management Solution" on page 70.

	Table 16-8	Process for installing and managing a virtual software layer with a Quick Delivery or Package Delivery task *(continued)*

Step	Action	Description

Step 5	Schedule the task and select the delivery destinations.	Define the schedule and the delivery destinations every time you run the task.
		
		Your options for scheduling the task are as follows:
		
		■ Run the task now.
		    This option runs the task as soon as possible, unless it must wait for a maintenance window.
		■ Schedule the task to run at a specific time.
		    See "Scheduling a task and selecting computers in Software Management Solution" on page 144.

Step 6	View the Virtualized Software Resources reports.	You can use the reports to monitor the state of virtual applications. These reports are listed under the Software reports. See "Running a Software Management Solution report" on page 83.

See "Managing virtual applications" on page 217.

Installing and managing a virtual software layer with a Managed Software Delivery policy

(Windows only)

You can create Managed Software Delivery policies to create and manage new virtual software layers or manage existing layers on client computers.

A Managed Software Delivery policy lets you perform complex layer management tasks.

For example, you can create a Managed Software Delivery policy that manages virtual software layers as follows:

■ Installs a new version of an application into a virtual software layer and then deactivates or deletes the earlier version.

■ Deactivates one version of an application and activates another version.

If you need to manage a single virtual software layer, use a Software Virtualization task, a Quick Delivery task, or a Package Delivery task.

See "Methods for installing and managing virtual software" on page 221.

Table 16-9   Process for managing virtual software layers with a Managed Software Delivery policy

Step	Action
Step 1	Create one or more Software Virtualization tasks or Quick Delivery tasks that manage virtual software layers. See "Installing and managing a virtual software layer with a Software Virtualization task" on page 225. See "Installing and managing a virtual software layer with a Quick Delivery or Package Delivery task" on page 228.
Step 2	Create a Managed Software Delivery policy that manages a virtual software layer in one of the following ways: ■ Installs a software resource into a virtual software layer. ■ Manages a virtual software layer that was created by installing a virtual software archive (VSA) file. See "Creating a Managed Software Delivery policy with the Managed Software Delivery wizard" on page 106. See "Creating a Managed Software Delivery policy" on page 110.
Step 3	Add the Software Virtualization tasks or Quick Delivery tasks to the Managed Software Delivery policy. See "Delivering multiple software resources and tasks sequentially" on page 126.

Index

W