Symantec™ System Recovery 2013 R2 Management Solution Administrator's Guide

Symantec™ System Recovery 2013 R2 Management Solution Administrator's Guide

Documentation version: 2014

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's 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

Chapter 1

Introducing Symantec™ System Recovery 2013 R2 Management Solution

This chapter includes the following topics:

About Symantec System Recovery 2013 R2 Management Solution

Symantec System Recovery 2013 R2 Management Solution provides the enterprise-level backup management tasks for server and desktop protection.

You can centrally monitor the recovery point status of Windows and Linux servers, desktops, and laptops across your organization, all from the Symantec Management Console. From the product's Home page, you can easily view the computers that are protected, including backup status. Using the power of Symantec System Recovery, you can also perform remote system and drive recovery of Windows computers (Linux computers must be recovered locally).

See "What's new in Symantec System Recovery 2013 R2 Management Solution" on page 14.

What's new in Symantec System Recovery 2013 R2 Management Solution

Symantec System Recovery 2013 R2 Management Solution includes the following enhancements and new features:

Table 1-1 What's new in Symantec System Recovery 2013 R2 Management Solution

Feature	Description
Symantec Management Platform 7.5 supported	Symantec System Recovery 2013 R2 Management Solution now only supports Symantec Management Platform 7.5. Installation of Symantec System Recovery 2013 R2 Management Solution on 64-bit operating system is only supported with Symantec Management Platform 7.5.
Generate LightsOut Restore package	Symantec System Recovery 2013 R2 Management Solution provides a link to the Symantec System Recovery Disk creation utility installer. Using this utility, you can create both 32-bit and 64-bit recovery disks. You can use the recovery disks to restore any computer. The Symantec System Recovery 2013 R2 Management Solution console now lets you create an LightsOut Restore package, which was earlier available through the Symantec Installation manager (SIM). To create the LightsOut Restore package, you need to upload the Symantec System Recovery Disks that are created. After the created Symantec System Recovery Disks are uploaded, the LightsOut Restore package is generated on the Management Solution server and can be deployed to managed nodes.
Supports Windows 8, Windows 8.1, Windows Server 2012, and Windows Server 2012 R2 for managed clients	Symantec System Recovery 2013 R2 Management Solution now supports the Windows 8, Windows 8.1, Windows Server 2012, and Windows Server 2012 R2 operating systems for managed clients.

Table 1-1 What's new in Symantec System Recovery 2013 R2 Management Solution *(continued)*

Feature	Description
Symantec Management Platform (SMP) 7.0 and 7.1 are no longer supported	Starting with 2013 R2, Symantec System Recovery 2013 R2 Management Solution has removed the support for Symantec Management Platform 7.0. Installation of Symantec System Recovery 2013 R2 Management Solution on 32-bit operating system (SMP 7.0) is not supported. Starting with 2013 R2, Symantec System Recovery 2013 R2 Management Solution has removed the support for Symantec Management Platform 7.1. Installation of Symantec System Recovery 2013 R2 Management Solution on 64-bit operating system (SMP 7.1) is not supported.
pcAnywhere is no longer supported	Starting with 2013 R2, Symantec System Recovery 2013 R2 Management Solution has removed the support for pcAnywhere.

Components of Symantec System Recovery 2013 R2 Management Solution

An installation of Symantec System Recovery 2013 R2 Management Solution consists of several main components for managing recovery points on client computers.

See "How Symantec System Recovery 2013 R2 Management Solution works" on page 17.

Table 1-2 Components of Symantec System Recovery 2013 R2 Management Solution

Component	Description
Symantec System Recovery 2013 R2 Management Solution	Lets you remotely run and manage backup policies and recovery on client computers from a central location. See "About the Symantec System Recovery 2013 R2 Management Solution Home page" on page 27.

Table 1-2 Components of Symantec System Recovery 2013 R2 Management Solution *(continued)*

Component	Description
Symantec System Recovery 2013 R2 Management Solution configuration file	Adds and configures the following items at the time of installation: ■ Database configuration files on the SQL database that Notification Server uses. The database stores recovery point history, client computer information, backup history, recovery point information, and configuration details. ■ Symantec System Recovery Plug-in install file. Symantec System Recovery 2013 R2 Management Solution already comes with a software delivery policy for Symantec System Recovery 2013 R2 that you can deploy to resource targets. You can also create your own Symantec System Recovery Plug-in software delivery policies by editing the packages that are already provided in the solution. Or, you can create new Symantec System Recovery Plug-in packages. ■ A folder where you can store your own command files that you run before or after data capture, or after recovery point creation.
Symantec System Recovery 2013 R2 Management Solution Web pages	Installs the Web pages that the solution uses.

Table 1-2 Components of Symantec System Recovery 2013 R2 Management Solution *(continued)*

Component	Description
Symantec System Recovery Plug-in	Publishes a variety of event information to Symantec Management Console (by way of Notification Server), such as the following: ■ A list of recovery points and their storage locations. ■ Backups that are assigned to the computer. ■ Symantec System Recovery version. ■ Any configuration changes that are made to the computer. The Symantec System Recovery Plug-in is a necessary component of Symantec System Recovery. It must be installed on each computer that has backups you want to manage. A computer is considered to be managed by Symantec System Recovery 2013 R2 Management Solution when the Symantec System Recovery Plug-in is installed on it. See "Installing the Symantec System Recovery Plug-in on computers" on page 35.
Microsoft IIS virtual directory path	References the Web folder of your solution installation path.

How Symantec System Recovery 2013 R2 Management Solution works

In Symantec System Recovery 2013 R2 Management Solution, backup policies are submitted through Symantec Management Console and stored in the database. Client computers pull the backup policies down from Notification Server and process them. Administrators run Symantec Management Console from Notification Server, or from a remote system. After policies are created, the Symantec System Recovery 2013 R2 Management Solution components on the server process them. All interaction to the Symantec System Recovery 2013 R2 Management Solution system, such as submitting policies and viewing results can be done through the console.

Through the console, you can create a one-time backup task, or use the schedule policy to create recurring daily backups. You can also delete recovery points, or even recover a computer.

Through Symantec Management Console functions, client computers are grouped together into resource targets to simplify the backup process. On the portal page of the solution, you can track and troubleshoot all of the computers whose backups you manage. You can view the backup status and statistics by computer filters such as backup failures, and deleted recovery point task status.

After a backup policy has been processed, the results are stored in the database.

See "What you can do with Symantec System Recovery 2013 R2 Management Solution" on page 18.

What you can do with Symantec System Recovery 2013 R2 Management Solution

Symantec System Recovery 2013 R2 Management Solution lets you work from a remote location to back up and recover Windows-based computers. You can also back up Linux-based computers and recover them locally on a computer using Symantec System Recovery Linux Edition. For more information, see the *Symantec System Recovery 2013 R2 User's Guide Linux Edition.*

Table 1-3 What you can do with Symantec System Recovery 2013 R2 Management Solution

Task	Description
Generate LightsOut Restore package	Lets you generate the LightsOut Restore package by creating ISOs using the Symantec System Recovery Disk Creation Utility and uploading them on the Management Solution server. After the LightsOut Restore Package is generated, you can configure and install LightsOut Restore 2013 R2 on client computers. See "Generating the LightsOut Restore package in Symantec System Recovery 2013 R2 Management Solution" on page 48.
Define backup policies and tasks and recovery point storage locations	Lets you do the following: ■ Define daily, weekly, monthly, or quarterly backup policies, and assign them to one or more resource targets. ■ Create full independent recovery points or recovery point sets with incrementals. ■ Define recovery point destinations on a network share or on a local drive on the client computer. See "Creating a basic backup policy" on page 89. See "Creating an advanced backup policy" on page 105.

Table 1-3 What you can do with Symantec System Recovery 2013 R2 Management Solution *(continued)*

Task	Description
Remotely recover one drive, multiple drives, or an entire computer (Windows-based)	Lets you do the following: ■ Remotely recover a data drive on a managed client computer. See "Recovering a drive" on page 180. ■ Use LightsOut Restore to recover a system drive on a managed client computer that you can restart. See "Recovering a remote computer" on page 183.
Deploy command files on Windows-based computer	Lets you do the following: ■ Deploy a command files package from Notification Server directly to client computers. The files are run during a particular stage in the recovery point creation process. ■ Specify a folder on a network share where managed client computers can run command files during a particular stage in the recovery point creation process. See "About running command files during a backup" on page 112. See "Deploying the command files package to client computers for use during a backup" on page 115.
Remotely delete recovery points	Lets you do the following: ■ Delete entire recovery point sets. See "Deleting a recovery point set" on page 155. ■ Delete recovery points within a set. See "Deleting recovery points within a set" on page 156.
Administer server, desktop, and laptop computers	Lets you do the following: ■ Troubleshoot and resolve backup policies remotely. ■ Run various predefined reports on managed computers. ■ Manage Symantec System Recovery licenses on resource targets. ■ Monitor the overall status of recovery points for an entire network of Windows computers. See "Viewing reports" on page 212. See "About managing Symantec System Recovery license policies" on page 77.

Chapter 2

Installing Symantec System Recovery 2013 R2 Management Solution

This chapter includes the following topics:

About upgrading from Symantec System Recovery 2013 Management Solution to Symantec System Recovery 2013 R2 Management Solution

When you upgrade, the installation program uninstalls Symantec System Recovery 2013 Management Solution. However, all the configurations, policies, tasks, and recovery points are preserved.

To upgrade Symantec System Recovery 2013 Management Solution to Symantec System Recovery 2013 R2 Management Solution, run the Symantec System Recovery 2013 R2 Management Solution installation program.

See “Installing Symantec System Recovery 2013 R2 Management Solution ” on page 21.

Post-upgrade tasks

After you upgrade Symantec System Recovery 2013 Management Solution to Symantec System Recovery 2013 R2 Management Solution, you must perform the following tasks:

- Install the Symantec Management Agent on the client computers. You can skip this task if the latest supported version of Symantec Management Agent is already installed on the client computers.
  See "Installing the Symantec Management Agent on client computers" on page 34.
- Install the Symantec System Recovery Plug-in on the client computers.
  See "Installing the Symantec System Recovery Plug-in on computers" on page 35.
- Install Symantec System Recovery 2013 R2 on the client computers. You can skip this task if you do not want to upgrade the client computers to Symantec System Recovery 2013 R2.
  See "Installing Symantec System Recovery 2013 R2 or Symantec System Recovery 2013 R2 Linux Edition on client computers" on page 39.

Installing Symantec System Recovery 2013 R2 Management Solution

Symantec System Recovery 2013 R2 is already included as a software delivery policy with Symantec System Recovery 2013 R2 Management Solution.

See the product documentation for Symantec System Recovery 2013 R2 or Symantec System Recovery 2013 R2 Linux Edition for complete system requirements.

You may intend to define your own software delivery policies for Symantec System Recovery 2013 or Symantec System Recovery 2011. In such cases, the system requirements vary depending on the package contents.

Symantec System Recovery 2013 R2 Management Solution supports up to 20,000 installations of Symantec System Recovery for each installation of the solution on a Notification Server. However, network performance varies greatly among organizations. The total number of supported installations of Symantec System Recovery may be more or less for your network. Network performance should be monitored to ensure that installations of Symantec System Recovery are not extended beyond the capacity and capability of your network.

You use the Symantec Installation Manager to install Symantec System Recovery 2013 R2 Management Solution on the Notification Server computer. The Symantec

Installation Manager checks for the required software and hardware resources, updates registry settings, and then copies the required files to the hard disk.

For detailed installation instructions, please refer to the *Symantec Management Platform Installation Guide*.

System requirements for Symantec System Recovery 2013 R2 Management Solution

The computer on which you install and use Symantec System Recovery 2013 R2 Management Solution must meet the following minimum system requirements.

Table 2-1 Minimum system requirements for 64-bit operating systems

Component	Requirements
Processor	Dual Processor Dual Core with 2.53 GHz or faster **Note:** An Intel Itanium 2 processor is required for Windows Server 2008 R2 for Itanium-Based Systems.
RAM	4 GB
Available disk space	20 GB or more
Operating system	Microsoft Windows Server 2008 R2, Enterprise Edition, or Standard Edition
Database	Express, Standard, and Enterprise editions of the following SQL servers are supported: ■ Microsoft SQL Server 2005 SP4 only ■ Microsoft SQL Server 2008 SP2 onwards ■ Microsoft SQL Server 2012 **Note:** Symantec recommends that you install Microsoft SQL Server and Symantec System Recovery 2013 R2 Management Solution on separate computers to avoid computer performance issues.
Software	The following must be installed on the computer on which you want to install Symantec System Recovery 2013 R2 Management Solution: ■ Microsoft Silverlight 3.0 or later ■ Symantec Installation Manager 7.5 ■ Symantec Management Platform 7.5 HF 6 **Note:** Installation of Symantec System Recovery 2013 R2 Management Solution is not supported on encrypted file systems. **Note:** Symantec System Recovery 2013 R2 Management Solution does not support Symantec Management Platform 7.5 SP1.

Table 2-1 Minimum system requirements for 64-bit operating systems *(continued)*

Component	Requirements
Internet access	High-speed Internet access is recommended at the computer where you install Symantec System Recovery 2013 R2 Management Solution.

Symantec also recommends that you familiarize yourself with the Symantec Management Platform by reviewing the *Symantec Management Platform Installation Guide*.

The Symantec Management Platform requires a Microsoft SQL Server database. The SQL Server database can be installed on the same computer as the Symantec Management Platform or on a remote computer. Symantec recommends that you install the SQL Server database on a remote computer to avoid computer performance issues.

See "Preparing to manage the backups of client computers" on page 32.

To install the Symantec System Recovery 2013 R2 Management Solution

1. Log on to your Notification Server computer by using either the Administrator account or an account with administrator privileges.
2. Click **Start > All Programs > Symantec > Symantec Installation Manager > Symantec Installation Manager**.
3. Click **Install new products**.
4. On the **Install New Products** panel, in the **Filter** drop-down list, select **None**.
5. Select the following products:
   - Symantec System Recovery 2013 R2 Management Solution
   - Symantec System Recovery 2013 R2 Installer
   - Symantec System Recovery 2013 R2 Linux Management Solution (only required if you intend to back up Linux-based computers)
   - Symantec Management Platform

   The Symantec Installation Manager may automatically select additional software components to complete the installation.
6. Click **Review selected products**.
7. In the **Selected Products and Features** panel, review the list of selected products, and then click **Next**.

8 On the **End User License Agreement** panel, read the End User License Agreement , and then click **I accept the terms in the license agreements**, and then click **Next**.

The Symantec Installation Manager runs an installation readiness check to make sure that your computer meets all requirements. The results of the installation readiness check appear in the **Install Readiness Check** panel.

9 On the **Install Readiness Check** panel, install any required software before you continue the installation.

Where applicable, a link appears in the **Install Readiness Check** panel that lets you install the missing software from within the **Symantec Installation Manager** panel. If a link does not appear, you must exit the installation. Then you must install the missing software component, and then start the Symantec System Recovery 2013 R2 Management Solution installation again.

The following options appear in the **Install Readiness Check** panel.

Check mark	The requirements and the recommendations are met.
Exclamation point	The requirement is met. You can continue with the installation. However, there are some recommendations to consider.
X	The requirement is not met. You cannot continue with the installation until the requirement is met. Click the associated link for additional information or to install the required product. After you make changes to your computer, click **Check install readiness again** to recheck your system. You may be required to restart your computer after the required software is installed.

When all the requirements are met in the **Install Readiness Check** panel, you can continue with the installation.

10 Click **Next**.

11 On the **Notification Server Configuration** panel, type the appropriate information to complete the panel, and then click **Next**.

12 On the **Contact Information** panel, type the appropriate information to complete the panel, and then click **Next**.

13 On the **Review Installation Details** panel, review the installation information, and then click **Begin install**.

14 On the **Installation** panel, click **Finish** to launch the Symantec Management Console.

See "About the Symantec System Recovery 2013 R2 Management Solution Home page" on page 27.

See "Installing the Symantec System Recovery Plug-in on computers" on page 35.

See "Creating a basic backup policy" on page 89.

Uninstalling Symantec System Recovery 2013 R2 Management Solution

You can uninstall Symantec System Recovery 2013 R2 Management Solution from the computer on which Notification Server is installed. The uninstallation program removes the files and registry settings that were set up or copied onto the computer's hard disk during installation. The uninstallation program also removes the policies and tasks that were setup or created while using Symantec System Recovery Management Solution.

When you uninstall the solution, Symantec System Recovery is not uninstalled from any managed client computers that you added to the console.

To uninstall Symantec System Recovery 2013 R2 Management Solution

1 Log on to your computer by using either the Administrator account or an account with administrator privileges.

2 On the computer where Notification Server is installed, click **Start > All Programs > Symantec > Symantec Installation Manager > Symantec Installation Manager**.

3 Select **Symantec System Recovery 2013 R2 Management Solution** in the **Installed products** list.

4 Click **Uninstall**.

5 Click **Yes**.

Chapter 3

Getting started with Symantec System Recovery 2013 R2 Management Solution

This chapter includes the following topics:

- Uninstalling Symantec System Recovery-related products and components from client computers
- Generating the LightsOut Restore package in Symantec System Recovery 2013 R2 Management Solution
- Configuring and installing LightsOut Restore 2013 R2 on client computers
- Configuring and installing LightsOut Restore 2013 on client computers
- Configuring and installing LightsOut Restore 2011 on client computers
- Uninstalling LightsOut Restore from client computers
- Updating the settings of a package
- Uninstalling Symantec System Recovery-related products from the Symantec Management Platform
- Adding or removing recovery point passwords
- About managing recovery point destinations
- Configuring a Dedicated Offsite Copy task
- About viewing filters
- About organizational views
- About managing Symantec System Recovery license policies

About the Symantec System Recovery 2013 R2 Management Solution Home page

The **Home** page provides a visual overall status of servers and desktop computers. Those computers may or may not have an installation of Symantec System Recovery on them. Actual data regarding computer incidents populates this page.

Note: The computers must have Symantec System Recovery Plug-in and Symantec System Recovery installed to show up on the **Home** page.

You can edit the **Home** page by adding or deleting Web parts. You can add or delete Web parts from other solutions or Symantec System Recovery 2013 R2 Management Solution. You can also add or delete the Web parts that already come with the Symantec Management Console.

For information about using Symantec Management Console, click the Help icon in the console.

See "Starting Symantec System Recovery 2013 R2 Management Solution" on page 31.

Web parts for the Home page

The following table describes the product's Web parts you can delete from or add to the **Home** page.

Table 3-1 Web parts for the Symantec System Recovery 2013 R2 Management Solution Home page

Web part	Description
Alerts and Failures	Displays a table of various types of failures and alerts that you can act on or resolve by clicking the associated hyperlink.

Table 3-1 Web parts for the Symantec System Recovery 2013 R2 Management Solution Home page *(continued)*

Web part	Description
Backup Status	Filters the backup status results by collection. Client computer status types include the following: ■ **Backed up** Indicates the number of managed client computers that have made a recovery point of all drives in the last 30 days. And, the client computers have not missed the last scheduled backup. **Note:** The drives must be set to report full status. Client computers are considered "backed up" without having an assigned backup policy. This status is true as long as one or more recovery points have been created within the last 30 days. A backed-up drive can be fully recovered. ■ **Needs Attention** Indicates the number of managed client computers that have a backup policy assigned but the policy has not run for a long time. Or, it has missed the last scheduled backup (meaning that existing recovery points are probably old). A client computer drive that needs attention can be recovered. However, if the recovery points are old, the recovery points may not contain the latest versions of files or folders. ■ **At Risk** Indicates the number of managed client computers that have no recovery points available for the reported drives. A client computer that is at risk can be recovered if the volumes are set to back up. For example, suppose you have a C:\, D:\, and E:\ volume on a client computer, but only a backup of C:\ exists. While Symantec System Recovery 2013 R2 Management Solution shows the client computer at risk, you can still recover the C:\ volume. ■ **Not Reporting** Indicates the number of managed client computers that have not reported back to the Symantec System Recovery 2013 R2 Management Solution server. The computers must report within a set time interval regardless of whether or not any policies are assigned to them. Sometimes this error is caused from network connectivity issues. For example, the computer is turned off or is not connected to the network.

Table 3-1 Web parts for the Symantec System Recovery 2013 R2 Management Solution Home page *(continued)*

Web part	Description
Computer Statistics	Displays a summary of all of the managed client computers that have a supported version of Symantec System Recovery installed. Servers and desktops sort this information. You can click **Desktops or Servers** in the legend to open a detailed view of the managed client computers within that group.
Destination Storage	Displays a table summary of all defined local and network destinations for recovery points. The table displays the destination type and path, among other things.
Failures	Displays a line chart that shows the number of managed client computers that have backup failures within one or more collections. Backup failures can be caused if you run out of hard disk space at the recovery point storage location. Or, a backup that is unable to connect to the specified recovery point storage location (usually a non-local storage location). Click **Details** to review a list of client computers with backup failures.
Getting Started	Displays the hyperlinked tasks to perform following a new installation of Symantec System Recovery 2013 R2 Management Solution. It also includes a link to Help that lists the common tasks that you can perform, such as how to create a backup policy.
License status	Shows the proportions of licenses for managed client computers. You can filter license status results by collection. License status types include the following: ■ **Licensed** Indicates the number of managed client computers that have a current license assigned to them. ■ **Not Licensed** Indicates the number of client computers on which an expired trial version of Symantec System Recovery is installed or on which no license was activated. ■ **Trial License** Indicates the number of managed client computers that have a trial version of Symantec System Recovery installed. You can click a license status in the legend to open a detailed view of the client computers within that status.

Table 3-1 Web parts for the Symantec System Recovery 2013 R2 Management Solution Home page *(continued)*

Web part	Description
Operating system Statistics	Displays a summary of all of the managed client computers that have a supported version of Symantec System Recovery installed. The information is sorted according to Windows version. You can click an operating system in the legend to open a detailed view of the managed client computers within that group.
ThreatCon Response Level	Indicates the current ThreatCon level as identified by Symantec's early warning security threat system. When Symantec identifies various threats, the ThreatCon team adjusts the threat level. This adjustment gives people and systems adequate warning to protect data and systems against attack. The following ThreatCon levels may appear: ■ **Level 1** No discernable security threats exist. ■ **Level 2** Security threats can occur, although no specific threats have been known to occur. ■ **Level 3** An isolated security threat is in progress. ■ **Level 4** Extreme global security threats are in progress.

Starting Symantec System Recovery 2013 R2 Management Solution

You can start Symantec System Recovery 2013 R2 Management Solution using several different methods.

See "About the Symantec System Recovery 2013 R2 Management Solution Home page" on page 27.

To start Symantec System Recovery 2013 R2 Management Solution

1 Do one of the following:

- On the computer where Notification Server is installed, on the Windows taskbar, click **Start > All Programs > Symantec > Solutions > Symantec System Recovery 2013 R2 Management Solution**.

- On the computer where Notification Server is installed, on the Windows taskbar, click **Start > All Programs > Symantec > Symantec Management Console**.
  In the Symantec Management Console, on the **Home** menu, click **Backup and Recovery > Symantec System Recovery 2013 R2 Management Solution**.
- On any computer on the network, open a Web browser and enter the following URL:
  http://<server_name>/Altiris/Console/
  In the Symantec Management Console, on the **Home** menu, click **Backup and Recovery > Symantec System Recovery 2013 R2 Management Solution**.

2 In the right pane of the **Home** page, click the arrow in the title bar of a Web part to display or hide the results.

Sending feedback to Symantec

Please take a moment to share your feedback and comments with Symantec regarding Symantec System Recovery 2013 R2 Management Solution.

To send feedback

1 In the Symantec Management Console, on the toolbar, click **Settings > Console > Views**.

2 In the left pane, in the Symantec System Recovery 2013 R2 Management Solution tree, click **Tell Symantec What You Think**.

3 In the right pane, click **Send feedback to Symantec**, and then follow the on-screen instructions.

4 When you are finished, click **OK**.

See "About the Symantec System Recovery 2013 R2 Management Solution Home page" on page 27.

Preparing to manage the backups of client computers

Before you can begin to manage backups of computers on a network or a remote location, you must first ensure that the following configurations occur. Certain components must be installed to the resource targets you want.

Table 3-2 Preparing to manage the backups of client computers

Step	Description
Step 1	Discover computers on the network. See "Discovering client computers on the network" on page 33.
Step 2	Install the Symantec Management Agent. See "Installing the Symantec Management Agent on client computers" on page 34.
Step 3	Install the Symantec System Recovery Plug-in or the Symantec System Recovery Linux Edition Plug-in. See "Installing the Symantec System Recovery Plug-in on computers" on page 35.
Step 4	Install Symantec System Recovery 2013 R2, Symantec System Recovery 2013 R2 Linux Edition, or LightsOut Restore 2013 R2. See "Installing Symantec System Recovery 2013 R2 or Symantec System Recovery 2013 R2 Linux Edition on client computers" on page 39. See "Configuring and installing LightsOut Restore 2013 R2 on client computers" on page 50.
Step 5	Create Symantec System Recovery Disk (ISO) and generate the LightsOut Restore Package in Symantec System Recovery 2013 R2 Management Solution. See "Generating the LightsOut Restore package in Symantec System Recovery 2013 R2 Management Solution" on page 48.
Step 6	Define and assign backup policies to resource targets. See "Creating a basic backup policy" on page 89.

Discovering client computers on the network

Before you can manage the backups of client computers on the network, you must first discover the client computers. You can discover computers in an Active Directory domain and select specific computers or an entire Active Directory domain. Or, you can discover computers in a network domain and select specific computers or an entire network domain.

After you discover the computers, you can install the Symantec Management Agent on them.

The amount of time that is required to discover computers varies depending on the number of computers that are involved.

See "Installing the Symantec Management Agent on client computers" on page 34.

See "Preparing to manage the backups of client computers" on page 32.

To discover client computers on the network

- Do one of the following:

To discover client computers by importing them from Active Directory	Do the following: ■ On the **Home** tab, in the **Getting Started** Web Part, click **Active Directory Import**. ■ On the **Microsoft Active Directory Import** page, in the **Resource Import Rules** table, select the rule to import computer resources. ■ On the **Resource Import Rules** toolbar, click the run import rule icon to run the rule.
To discover client computers in a domain	Do the following: ■ On the **Home** tab, in the **Getting Started** Web Part, click **Domain Discovery**. ■ On the **Domain Membership/WINS Import** page, select a domain to search. ■ Click **Discover Now**.

Installing the Symantec Management Agent on client computers

After you discover the computers whose backups you want to manage on the network, you must install the Symantec Management Agent on those computers.

The amount of time that is required to install the Symantec Management Agent can vary. It depends on the number of computers on which you want to install the agent.

See "Installing the Symantec System Recovery Plug-in on computers" on page 35.

See "Preparing to manage the backups of client computers" on page 32.

To install the Symantec Management Agent on client computers

1. On the **Home** tab, in the **Getting Started** Web Part, click **Install the Symantec Management Agent**.
2. Do one of the following:

To install the Symantec Management Agent on computers where Symantec System Recovery for Windows runs	Do the following: ■ Select one or more computers. ■ On the **Install Symantec Management Agent** tab, click **Installation Settings**. ■ In the **Symantec Management Agent Installation Options** panel, select the options you want to apply to the agent. ■ Click **OK**. ■ Click **Install Symantec Management Agent**. Review the installation options and make changes if necessary. ■ Click **Proceed with Install**.
To install the Symantec Management Agent on computers where Symantec System Recovery 2013 R2 Linux Edition runs	Do the following: ■ Select one or more computers. ■ On the **Install Symantec Management Agent for UNIX, Linux and Mac** tab, click **Installation Settings**. ■ In the **Install Settings** panel, set the options you want to apply to the agent as found in the **Connection and Authentication** tab and the **Agent Settings** tab. ■ Click **OK**. ■ Click **Install the Symantec Management Agent**. ■ Click **OK** to proceed with the installation.

Installing the Symantec System Recovery Plug-in on computers

Using Symantec Management Platform policies, you can install the Symantec System Recovery Plug-in or the Symantec System Recovery Linux Edition Plug-in

to computers on your network. You can also use policies to upgrade (excludes the Symantec System Recovery Linux Edition) and uninstall the plug-in.

See "Uninstalling the Symantec System Recovery Plug-in on computers" on page 38.

Note: To use rollout policies, the Symantec Management Agent must be installed on the computers that you want to manage. You should already have a working knowledge of policies, packages, programs, and resource targets.

The amount of time that is required to install Symantec System Recovery can vary. It depends on the number of computers on which you want to install it.

See "Preparing to manage the backups of client computers" on page 32.

The following table describes the Symantec System Recovery Plug-in policies that are included with your installation of Symantec System Recovery 2013 R2 Management Solution.

Table 3-3 Predefined Symantec System Recovery Plug-in policies

Symantec System Recovery Plug-in policy	Description
Symantec System Recovery Plug-in **Symantec System Recovery Linux Edition Plug-in**	A software delivery policy that is installed on resource targets with no Symantec System Recovery Plug-in installed. You can also use the uninstall program with the software delivery policy to uninstall the plug-in. The Symantec System Recovery Plug-in lets you run tasks from Notification Server on the client computer. This plug-in policy also gathers information from the plug-in itself (such as backup definitions, changes to back up policies or **Independent Backup** tasks, and backup status). That information is published back to Notification Server. The Symantec System Recovery Plug-in accepts and applies backup configuration changes from Notification Server.
Symantec System Recovery Plug-in Upgrade	A software delivery policy that upgrades the previously installed Symantec System Recovery Plug-in on the resource targets that require an upgrade to the plug-in.

Table 3-3 Predefined Symantec System Recovery Plug-in policies *(continued)*

Symantec System Recovery Plug-in policy	Description
Symantec System Recovery Plug-in Uninstall **Symantec System Recovery Linux Edition Plug-in Uninstall**	A software delivery policy that uninstalls the previously installed Symantec System Recovery Plug-in on resource targets with the plug-in.

To install the Symantec System Recovery Plug-in on client computers

1 Do one of the following:

To install the Symantec System Recovery for Windows Plug-in	Do the following: ■ On the Symantec System Recovery 2013 R2 Management Solution **Packages and Policies** tab, in the **Install Policies** list in the left pane, under **Agent Plug-in**, click **Symantec System Recovery**.
To install the Symantec System Recovery Linux Edition Plug-in	Do the following: ■ On the Symantec System Recovery 2013 R2 Management Solution **Packages and Policies** tab, in the **Install Policies** list in the left pane, under **Agent Plug-in**, click **Install Plug-in for Symantec System Recovery Linux**.

2 Near the upper-right corner of the right pane, make sure **On** is selected from the list to enable the software delivery policy.

3 Set the deployment options.

Program name	Identifies the name of the program that you want to run.
Enable Verbose Reporting of Status Events	Sends the plug-in status events to the Notification Server computer.
Applied to	Identifies the resource target to which you want the software task applied.
Package multicast	Lets you uncheck (default) this option if you want to enable package multicast when the Symantec Management Agent's multicast option is disabled.
Schedule	Runs the software task either at a specific start time, or at specified start, end, and duration times. You can specify as many schedules as you need. You can also have any number of schedules active at once.

4 Click **Save changes**.

Uninstalling the Symantec System Recovery Plug-in on computers

Using Symantec Management Platform policies, you can upgrade or uninstall the Symantec System Recovery Plug-in on computers on your network. (Excludes the Symantec System Recovery Linux Edition.)

To uninstall the Symantec System Recovery Plug-in from client computers

1 Do one of the following:

To uninstall the Symantec System Recovery for Windows Plug-in	Do the following: ■ On the Symantec System Recovery 2013 R2 Management Solution **Packages and Policies** tab, in the **Uninstall Policies** list in the left pane, under **Agent Plug-in**, click **Plug-in for Symantec System Recovery Uninstall**.

To uninstall the Symantec System Recovery Linux Edition Plug-in	Do the following: ■ On the Symantec System Recovery 2013 R2 Management Solution **Packages and Policies** tab, in the **Uninstall Policies** list in the left pane, under **Agent Plug-in**, click **Plug-in for Symantec System Recovery for Linux Uninstall**.

2 Near the upper-right corner of the right pane, make sure **On** is selected from the list to enable the software delivery policy.

3 Set the deployment options.

Program name	Identifies the name of the program that you want to run.
Enable Verbose Reporting of Status Events	Sends the plug-in status events to the Notification Server computer.
Applied to	Identifies the resource target to which you want the software task applied.
Package multicast	Lets you uncheck (default) this option if you want to enable package multicast when the Symantec Management Agent's multicast option is disabled.
Schedule	Runs the software task either at a specific start time, or at specified start, end, and duration times. You can specify as many schedules as you need. You can also have any number of schedules active at once.

4 Click **Save changes**.

Installing Symantec System Recovery 2013 R2 or Symantec System Recovery 2013 R2 Linux Edition on client computers

You can deploy Symantec System Recovery 2013 R2 or Symantec System Recovery 2013 R2 Linux Edition software delivery packages to computers. You can also choose to install Symantec System Recovery with a user interface. The user interface lets users interact with the software from the desktop of the client computer.

For complete system requirements, see the *Symantec System Recovery 2013 R2 User's Guide* (includes LightsOut Restore), or the *Symantec System Recovery 2013 R2 User's Guide Linux Edition*.

Note: Symantec System Recovery 2013 R2 Management Solution does not support recovery of Linux-based computers. You must recover Linux-based computers on the local computer. For more information about using Symantec System Recovery Linux Edition locally on a computer, see the *Symantec System Recovery 2013 R2 User's Guide Linux Edition*.

Note: Following the installation of Symantec System Recovery 2013 R2 for Windows, the client computer is automatically restarted. The restart is necessary to ensure that the necessary Symantec System Recovery services are started and running. A restart is not necessary following the installation of Symantec System Recovery 2013 R2 Linux Edition.

To review the installation's log file, check the C:\Windows\Temp folder.

See "Installing Symantec System Recovery 2011 on client computers" on page 44.

To install Symantec System Recovery 2013 R2 or Symantec System Recovery 2013 R2 Linux Edition on client computers

1. Do one of the following:
   - You may have chosen to install the **Symantec System Recovery 2013 R2 or Symantec System Recovery 2013 R2 Package** at the time you installed Symantec System Recovery 2013 R2 Management Solution. Or, you may have chosen to install the **Symantec System Recovery 2013 R2 or Symantec System Recovery 2013 R2 Linux Edition Package** at the time you installed Symantec System Recovery 2013 R2 Management Solution. In either case, go to step 3.
   - You may have chosen not to install the **Symantec System Recovery 2013 R2 or Symantec System Recovery 2013 R2 Package** at the time you installed Symantec System Recovery 2013 R2 Management Solution. Or, you may have chosen to not install the **Symantec System Recovery 2013 R2 or Symantec System Recovery 2013 R2 Linux Edition Package** at the time you installed Symantec System Recovery 2013 R2 Management Solution. In either case, continue to the next step.
2. Use the Symantec Installation Manager to install the **Symantec System Recovery 2013 R2 package** or the **Symantec System Recovery 2013 R2 Linux Edition package**.
3. Do one of the following:

To install Symantec System Recovery 2013 R2 that includes a user interface that is accessible from the desktop on client computers	Do one of the following: ■ On the Symantec System Recovery 2013 R2 Management Solution **Packages and Policies** tab, in the **Install Policies** list in the left pane, under **Symantec System Recovery > 2013 R2 > Install With User Interface**, click either **Install With Telemetry** or **Install Without Telemetry**. **Note:** The telemetry feature collects and transmits installation results and non-personal usage information to Symantec for reporting purposes. Symantec recommends that you install Symantec System Recovery with the telemetry feature.
To install Symantec System Recovery 2013 R2 that does not include a user interface on the desktop of client computers	Do the following: ■ On the Symantec System Recovery 2013 R2 Management Solution **Packages and Policies** tab, in the **Install Policies** list in the left pane, under **Symantec System Recovery > 2013 R2 > Install Without Interface**, click either **Install With Telemetry Interface** or **Install Without Telemetry**. **Note:** The telemetry feature collects and transmits installation results and non-personal usage information to Symantec for reporting purposes. Symantec recommends that you install Symantec System Recovery with the telemetry feature.
To install Symantec System Recovery 2013 R2 Linux Edition	Do the following: ■ On the Symantec System Recovery 2013 R2 Management Solution **Packages and Policies** tab, in the **Install Policies** list in the left pane, under **Symantec System Recovery Linux Edition > 2013 R2**, click **Install Without User Interface**.

4 Near the upper-right corner of the right pane, click **On** to enable the software delivery policy.

5 Set the deployment options.

Program name	Identifies the name of the program that you want to run.
Enable Verbose Reporting of Status Events	Sends the plug-in status events to the Notification Server computer.
Applied to	Identifies the resource target to which you want the software task applied.
Package multicast	Lets you uncheck (default) this option if you want to enable package multicast when the Symantec Management Agent's multicast option is disabled.
Schedule	Runs the software task either at a specific start time, or at specified start, end, and duration times. You can specify as many schedules as you need. You can also have any number of schedules active at once.

6 Click **Save changes**.

Installing Symantec System Recovery 2013 on client computers

You can deploy the Symantec System Recovery 2013 software delivery packages to client computers. You can also choose to install it with a user interface. The user interface lets you interact with the software from the desktop of the client computer.

For complete information about system requirements, see the *Symantec System Recovery User's Guide* (includes LightsOut Restore), or the *Symantec System Recovery User's Guide Linux Edition*.

Note: Symantec System Recovery 2013 R2 Management Solution does not support the recovery of Linux-based computers. You must recover Linux-based computers on the local computer. For more information about using Symantec System Recovery Linux Edition, see the *Symantec System Recovery User's Guide Linux Edition*.

To install Symantec System Recovery 2013 on client computers

1. Insert the Symantec System Recovery 2013 product CD into the media drive of the client computer.
2. Browse to the root of the Symantec System Recovery Disk CD.
3. Copy the contents of the SSR32 folder and paste them to the default package location that is local to the computer on which Notification Server is installed.

   The default location is `C:\Program Files\Altiris\Symantec System Recovery Management Solution\Web\SoftwareDelivery\SSR\11.0\Install`.
4. Copy the contents of the SSR64 folder and paste them to the default package location that is local to the computer on which Notification Server is installed.

   The default location is `C:\Program Files\Altiris\Symantec System Recovery Management Solution\Web\SoftwareDelivery\SSR\11.0\Installx64`.
5. From the left pane of the Symantec System Recovery 2013 R2 Management Solution **Packages and Policies** tab, expand the **Update Packages** list.
6. Under **Symantec System Recovery > 2013 >** click **Install Without User Interface Package** or **Install With User Interface Package**, select required package.
7. In the bottom of the right pane, click **Update Distribution Points** to make the Notification Server computer aware of the package location that you added.
8. Do one of the following:

To install Symantec System Recovery 2013 that includes a user interface that is accessible from the desktop on client computers	Do the following: ■ On the Symantec System Recovery 2013 R2 Management Solution **Packages and Policies** tab, expand the **Install Policies** list in the left pane. ■ Under **Symantec System Recovery > 2013**, click **Install With User Interface**.
To install Symantec System Recovery 2013 that does not include a user interface on the desktop of client computers	Do the following: ■ On the Symantec System Recovery 2013 R2 Management Solution **Packages and Policies** tab, expand the **Install Policies** list in the left pane. ■ Under **Symantec System Recovery > 2013**, click **Install Without User Interface**.

9 On the upper-right corner of the right pane, click **On** to enable the software delivery policy.

10 Set the deployment options.

Program name	Identifies the name of the program that you want to run.
Enable Verbose Reporting of Status Events	Sends the plug-in status events to the Notification Server computer.
Applied to	Identifies the resource target to which you want the software task applied.
Package multicast	Lets you uncheck (default) this option if you want to enable package multicast when the Symantec Management Agent's multicast option is disabled.
Schedule	Runs the software task either at a specific start time, or at specified start, end, and duration times. You can specify as many schedules as you need. You can also have any number of schedules active at once.

11 Click **Save changes**.

To review the installation log file, look in the C:\Windows\Temp folder.

Installing Symantec System Recovery 2011 on client computers

You can deploy Symantec System Recovery 2011 software delivery packages to computers. You can also choose to install Symantec System Recovery with a user interface. The user interface lets users interact with the software from the desktop of the client computer.

For complete system requirements, see the *Symantec System Recovery User's Guide* (includes LightsOut Restore), or the *Symantec System Recovery User's Guide Linux Edition*.

Note: Symantec System Recovery 2013 R2 Management Solution does not support recovery of Linux-based computers. You must recover Linux-based computers on the local computer. For more information about using Symantec System Recovery Linux Edition locally on a computer, see the *Symantec System Recovery User's Guide Linux Edition*.

To review the installation's log file, check the C:\Windows\Temp folder.

See "Installing Symantec System Recovery 2013 R2 or Symantec System Recovery 2013 R2 Linux Edition on client computers" on page 39.

To install Symantec System Recovery 2011 on client computers

1. Insert the Symantec System Recovery 2011 product CD into the media drive of the Notification Server computer.
2. Browse to the root of the Symantec System Recovery CD.
3. Copy and paste the Install folder to the default package location that is local to the computer on which Notification Server is installed.

   The default location is `C:\Program Files\Altiris\Symantec System Recovery Management Solution\Web\SoftwareDelivery\SSR\11.0\`. If you copy the Install folder from Symantec System Recovery product CD, paste it to the 10.0 folder .
4. On the Symantec System Recovery 2013 R2 Management Solution **Packages and Policies** tab, in the left pane, expand the **Update Packages** list.
5. Under **Symantec System Recovery > 2011** click **Install Without User Interface Package** or **Install With User Interface Package**.
6. In the bottom of right pane, click **Update Distribution Points** to make the Notification Server computer aware of the package location that you added.
7. Do one of the following:

To install Symantec System Recovery 2011 that includes a user interface that is accessible from the desktop on client computers	Do the following: ■ On the Symantec System Recovery 2013 R2 Management Solution **Packages and Policies** tab, expand the **Install Policies** list in the left pane. ■ Under **Symantec System Recovery > 2011**, click **Install With User Interface**.
To install Symantec System Recovery 2011 that does not include a user interface on the desktop of client computers	Do the following: ■ On the Symantec System Recovery 2013 R2 Management Solution **Packages and Policies** tab, expand the **Install Policies** list in the left pane. ■ Under **Symantec System Recovery > 2011**, click **Install Without User Interface**.

8 On the upper-right corner of the right pane, click **On** to enable the software delivery policy.

9 Set the deployment options.

Program name	Identifies the name of the program that you want to run.
Enable Verbose Reporting of Status Events	Sends the plug-in status events to the Notification Server computer.
Applied to	Identifies the resource target to which you want the software task applied.
Package multicast	Lets you uncheck (default) this option if you want to enable package multicast when the Symantec Management Agent's multicast option is disabled.
Schedule	Runs the software task either at a specific start time, or at specified start, end, and duration times. You can specify as many schedules as you need. You can also have any number of schedules active at once.

10 Click **Save changes**.

To review the installation log file, look in the C:\Windows\Temp folder.

Uninstalling Symantec System Recovery-related products and components from client computers

You can use uninstall policies in Symantec System Recovery 2013 R2 Management Solution to remove the following items from client computers:

- Symantec System Recovery 2013 R2
- Symantec System Recovery 2013 R2 or 2013 Linux Edition Plug-in
- Symantec System Recovery 2013 R2, 2013, or 2011
- Backup Exec System Recovery 2010
- Symantec System Recovery 2013 R2, 2013, or 2011 Linux Edition
- LightsOut Restore 2013 R2, 2013 or 2011

See “Uninstalling Symantec System Recovery-related products and components from client computers” on page 46.

See "Installing Symantec System Recovery 2013 R2 or Symantec System Recovery 2013 R2 Linux Edition on client computers" on page 39.

To uninstall Symantec System Recovery or Symantec System Recovery Linux Edition from client computers

1 Do one of the following:

To uninstall the Symantec System Recovery	Do the following: ■ On the Symantec System Recovery 2013 R2 Management Solution **Packages and Policies** tab, in the **Uninstall Policies** list in the left pane, under **Symantec System Recovery**, click **2013 R2 Uninstall**. To uninstall Symantec System Recovery 2013 Management Solution, click **2013 Uninstall**. To uninstall Symantec System Recovery 2011 Management Solution, click **2011 Uninstall**. Similarly, to uninstall Backup Exec System Recovery 2010, click **2010 Uninstall** under **Backup Exec System Recovery**.
To uninstall the Symantec System Recovery Linux Edition	Do the following: ■ On the Symantec System Recovery 2013 R2 Management Solution **Packages and Policies** tab, in the **Uninstall Policies** list in the left pane, under **Symantec System Recovery Linux Edition**, click **2013 R2 Uninstall**. To uninstall Symantec System Recovery 2013 Linux Edition, click **2013 Uninstall**. To uninstall Symantec System Recovery 2011 Linux Edition, click **2011 Uninstall**.

2 Near the upper-right corner of the right pane, make sure **On** is selected from the list to enable the software delivery policy.

3 Set the deployment options.

Program name	Identifies the name of the program that you want to run.
Enable Verbose Reporting of Status Events	Sends the plug-in status events to the Notification Server computer.
Applied to	Identifies the resource target to which you want the software task applied.
Package multicast	Lets you uncheck (default) this option if you want to enable package multicast when the Symantec Management Agent's multicast option is disabled.
Schedule	Runs the software task either at a specific start time, or at specified start, end, and duration times. You can specify as many schedules as you need. You can also have any number of schedules active at once.

4 Click **Save changes**.

Generating the LightsOut Restore package in Symantec System Recovery 2013 R2 Management Solution

As Microsoft does not allow redistribution of WinPE, starting from Symantec System Recovery 2013 R2 Management Solution, Symantec no longer provides the LightsOut Restore package in advance. You can now generate the LightsOut Restore package by creating ISOs using the Symantec System Recovery Disk Creation Utility and uploading them on the Management Solution server.

When you install Symantec System Recovery 2013 R2 Management Solution, the Symantec System Recovery Disk Creation Utility is extracted and is available for download on the Management Solution Server.

Note: Starting with Symantec System Recovery 2013 R2 Management Solution, the LightsOut Restore option is no longer available on the Symantec Installation Manager as before.

To generate the LightsOut Restore package

1. On the **Home** tab, in the **Getting Started** Web Part, click **Create Symantec System Recovery Disk (ISO) and generate LightsOut Restore Package**.
2. On the **Create Symantec System Recovery Disk (ISO) and generate LightsOut Restore Package** panel, click the **here** link to download and install the Symantec System Recovery Disk Creation Utility.

   When you install this utility a limited version of the Symantec System Recovery 2013 R2 is installed on your computer.

   Note: You must restart your computer after the Symantec System Recovery Disk Creation Utility is downloaded and installed. An Internet connection is a must to create the Symantec System Recovery Disk.

   ---

3. Do one of the following:
   - Click **Run** to start the installation.
     The Symantec System Recovery Disk Creation Utility is saved to a temporary location on your computer.
   - Click **Save** to save the installer on the default downloads location of your computer.
   - Click **Save As** and browse to select a location on your computer to save the installer.
   - Click **Save and Run** to save the installer and begin the installation.

   After the installation is complete, your computer restarts and the **Create Symantec System Recovery Disk Wizard (Management Solution Mode)** is displayed.
4. Using the **Create Symantec System Recovery Disk Wizard (Management Solution Mode)**, create both 32-bit and 64-bit Symantec System Recovery Disks (ISOs).

   To learn more about how to create a Symantec System Recovery Disk, click the Help icon on the **Create Symantec System Recovery Disk Wizard (Management Solution Mode)**.
5. Open the Symantec System Recovery 2013 R2 Management Solution console and navigate to the **Create Symantec System Recovery Disk (ISO) and Generate LightsOut Restore Package** page.
6. Select the **Symantec System Recovery Disk (ISOs) to generate the LightsOut Restore package on the server** check box.

7 Click **Browse** to select both the 32-bit and 64-bit Symantec System Recovery Disks that you created.

8 Click the **Generate LightsOut Restore Package** option.

The LightsOut Restore package that is generated is saved on the Management Solution server.

9 Use the **Install Without User Interface** policy in the **Packages and Policies** tab to deploy the LightsOut Restore package on the managed nodes.

The Symantec System Recovery Disk (ISOs) are also stored on the Management Solution server at the following location:

`C:\Program Files\Altiris\Symantec System Recovery Management Solution\Web\SoftwareDelivery\LOR\11.1\ISO`.

Note: If the managed client has a Windows 2003 operating system, create the Symantec System Recovery Disk ISOs using Windows ADK for Windows 8.0. Perform steps 1 to 9 separately for a Windows 2003 computer.

Note: If the LightsOut Restore package fails to generate, the logs with the failed information are available at the following location: `Start\All Programs\Symantec\Diagnostics\Altiris Log Viewer`.

After the LightsOut Restore Package is generated you can configure and install LightsOut Restore 2013 R2 on client computers.

See "Configuring and installing LightsOut Restore 2013 R2 on client computers" on page 50.

Configuring and installing LightsOut Restore 2013 R2 on client computers

You must generate the LightsOut Restore package before you configure and install LightsOut Restore 2013 R2 on client computers.

You can configure how LightsOut Restore runs on the resource targets that you want to protect. The configuration settings are applied to the Symantec Recovery Environment on each computer's local file system. The configuration also creates an entry in the **Windows boot** menu that you use to boot into the recovery environment.

Note: The LightsOut Restore feature requires a minimum of 1.5 GB of memory on the client computer to run properly.

To review the installation log file, look in the C:\Windows\Temp folder.

See "Uninstalling LightsOut Restore from client computers" on page 57.

To configure and install LightsOut Restore 2013 R2 on client computers

1. Generate a LightsOut Restore package.

   See "Generating the LightsOut Restore package in Symantec System Recovery 2013 R2 Management Solution" on page 48.

2. Do one of the following:

   - On the Symantec System Recovery 2013 Management Solution or Symantec System Recovery 2013 R2 Management Solution **Packages and Policies** tab, expand the **Install Policies** list in the left pane.
   - Under **LightsOut Restore**, under **2013 R2**, click **Configure Policy**.

3 In the right pane, set the configuration options.

Use the default language that is specified in Symantec Recovery Disk (English)	Indicates that English is used as the display language in the recovery environment.
Choose language	Lets you select the display language that you prefer to use in the recovery environment.
Time Zone	Runs the recovery environment in the specified time zone.
Keyboard layout	Lets you specify keyboard layout to use while in the recovery environment.
Time to display boot menu	Specifies (in seconds) how long the boot menu should display on the managed client computer. The default is 10 seconds.
Boot menu label	Creates a text label that is displayed in the **Windows boot** menu. You can select the label to boot into the recovery environment.
Automatically start network services	Starts the network services automatically when you recover the computer through LightsOut Restore.
Dynamic IP address	Connects to a network without the need for additional network configuration. You can use this option if you know a DHCP server is available on the network at the time you restore.
Static IP address	Connects to a network with a particular network adapter and specific address settings. You should use this option if you are sure that there is no DHCP server (or the DHCP server is not available) when you recover. **Note:** The **DNS Server Address** field is optional.

4 Click **Install Without User Interface**.

5 On the upper-right corner of the right pane, click **On** to enable **Install Without User Interface**.

6 Set the deployment options.

Program name	Identifies the name of the program that you want to run.
Enable Verbose Reporting of Status Events	Sends the plug-in status events to the Notification Server computer.
Applied to	Identifies the resource target to which you want the software task applied.
Package multicast	Lets you uncheck (default) this option if you want to enable package multicast when the Symantec Management Agent's multicast option is disabled.
Schedule	Runs the software task either at a specific start time, or at specified start, end, and duration times. You can specify as many schedules as you need. You can also have any number of schedules active at once.

7 Click **Save changes**.

Configuring and installing LightsOut Restore 2013 on client computers

To install LightsOut Restore 2013 you must use the Symantec System Recovery Disk that you have created.

See "Installing Symantec System Recovery 2013 on client computers" on page 42.

See "Uninstalling LightsOut Restore from client computers" on page 57.

You can configure how LightsOut Restore runs on the resource targets that you want to protect. The configuration settings are applied to the Symantec Recovery Environment on each computer's local file system. The configuration also creates an entry in the **Windows boot** menu that you use to boot into the recovery environment.

Note: The LightsOut Restore feature requires a minimum of 1.5 GB of memory on the client computer to run properly.

You can configure and install LightsOut Restore 2013 on client computers using the 32-bit or 64-bit Symantec System Recovery Disk of Symantec System Recovery 2013.

To review the installation log file, look in the C:\Windows\Temp folder.

To configure and install LightsOut Restore 2013 on client computers

1. Insert the 32-bit or 64-bit Symantec System Recovery Disk into the media drive of the Notification Server computer.
2. Browse to the root of the Symantec System Recovery Disk CD.
3. Copy the contents to the default package location that is local to the computer on which Notification Server is installed.

   The default location is for the 32-bit package is `C:\Program Files\Altiris\Backup Exec Retrieve Management Solution\Web\SoftwareDelivery\LOR\11.0\INSTALL`.

   The default location is for the 64-bit package is `C:\Program Files\Altiris\Backup Exec Retrieve Management Solution\Web\SoftwareDelivery\LOR\11.0\INSTALLx64`.
4. On Symantec System Recovery 2013 R2 Management Solution under the **Packages and Policies** tab, in the left pane, expand the **Update Packages** list.
5. Under **LightsOut Restore > 2013 >** click **Install Without User Interface Package**.
6. On the lower-right pane, click **Update Distribution Points** to make the Notification Server computer aware of the package location that you added.
7. Click **Save changes**.

Configuring and installing LightsOut Restore 2011 on client computers

To install LightsOut Restore 2011 you must use the Symantec System Recovery Disk that you have created.

You can configure how LightsOut Restore runs on the resource targets that you want to protect. The configuration settings are applied to the Symantec Recovery Environment on each computer's local file system. The configuration also creates an entry in the **Windows boot** menu that you use to boot into the recovery environment.

Note: The LightsOut Restore feature requires a minimum of 1.5 GB of memory on the client computer to run properly.

To review the installation log file, look in the C:\Windows\Temp folder.

See "Installing Symantec System Recovery 2011 on client computers" on page 44.

See "Uninstalling LightsOut Restore from client computers" on page 57.

To configure and install LightsOut Restore 2011 on client computers

1. Copy LightsOut Restore from Symantec Recovery Disk to the default package location on the Notification Server computer by doing the following:
   - Mount the Symantec Recovery Disk ISO file.
     Or, if you burned the Symantec Recovery Disk ISO file to media, insert the CD into the media drive. The media drive should be with the computer on which Notification Server is installed.
   - Browse to the root of the CD.
   - Copy the entire contents of the CD to the default package location that is local to the computer on which Notification Server is installed.
     You can view the path to the package location in the **Packages and Policies** tab of the Symantec System Recovery 2013 R2 Management Solution. In the left pane, double-click **Update Packages**. In the right pane, click the **Package** tab. The package location is identified in the **Package location** text box.
     The default location for LightsOut Restore 2011 is the following:
     C:\Program Files\Altiris\Symantec System Recovery Management Solution\web\softwaredelivery\lor\10.0\
2. On the Symantec System Recovery 2013 R2 Management Solution **Packages and Policies** tab, expand the **Install Policies** list in the left pane.
3. Under **LightsOut Restore**, under **2011**, click **Configure Policy**.

4 In the right pane, set the configuration options.

Use the default language that is specified in Symantec Recovery Disk (English)	Indicates that English is used as the display language in the recovery environment.
Choose language	Lets you select the display language that you prefer to use in the recovery environment.
Time Zone	Runs the recovery environment in the specified time zone.
Keyboard layout	Lets you specify keyboard layout to use while in the recovery environment.
Time to display boot menu	Specifies (in seconds) how long the boot menu should display on the managed client computer. The default is 10 seconds.
Boot menu label	Creates a text label that is displayed in the **Windows boot** menu. You can select the label to boot into the recovery environment.
Automatically start network services	Starts the network services automatically when you recover the computer through LightsOut Restore.
Dynamic IP address	Connects to a network without the need for additional network configuration. You can use this option if you know a DHCP server is available on the network at the time you restore.
Static IP address	Connects to a network with a particular network adapter and specific address settings. You should use this option if you are sure that there is no DHCP server (or the DHCP server is not available) when you recover.

5 Click **Install Without User Interface Package**.

6 Near the upper-right corner of the right pane, click **On** to enable **Install Without User Interface**.

7 Set the deployment options.

Program name	Identifies the name of the program that you want to run.
Enable Verbose Reporting of Status Events	Sends the plug-in status events to the Notification Server computer.
Applied to	Identifies the resource target to which you want the software task applied.
Package multicast	Lets you uncheck (default) this option if you want to enable package multicast when the Symantec Management Agent's multicast option is disabled.
Schedule	Runs the software task either at a specific start time, or at specified start, end, and duration times. You can specify as many schedules as you need. You can also have any number of schedules active at once.

8 Click **Save changes**.

Uninstalling LightsOut Restore from client computers

You can uninstall LightsOut Restore 2013 R2, 2013, or 2011 on client computers.

See "Configuring and installing LightsOut Restore 2013 R2 on client computers" on page 50.

See "Configuring and installing LightsOut Restore 2011 on client computers" on page 54.

To uninstall LightsOut Restore from client computers

1 On the Symantec System Recovery 2013 R2 Management Solution **Packages and Policies** tab, in the **Uninstall Policies** list, click the LightsOut Restore version that you want to uninstall.

2 Near the upper-right corner of the right pane, make sure **On** is selected from the list to enable the software delivery policy.

3 Set the deployment options.

Program name	Identifies the name of the program that you want to run.
Enable Verbose Reporting of Status Events	Sends the plug-in status events to the Notification Server computer.
Applied to	Identifies the resource target to which you want the software task applied.
Package multicast	Lets you uncheck (default) this option if you want to enable package multicast when the Symantec Management Agent's multicast option is disabled.
Schedule	Runs the software task either at a specific start time, or at specified start, end, and duration times. You can specify as many schedules as you need. You can also have any number of schedules active at once.

4 Click **Save changes**.

Updating the settings of a package

The various packages that are available in Symantec System Recovery 2013 R2 Management Solution are already predefined with the proper settings. Therefore, you should update the settings only if necessary.

The distribution points for a package are the locations at which the package is stored, such as package servers or UNC source locations. Information about each package is contained in an XML file that is stored with the package. This information must be updated each time you edit the settings in a package. Notification Server and package servers use this information to provide the appropriate files when a managed computer requests the package. The package information is updated on a schedule, but you can perform a manual update when appropriate. For example, if you have changed a package, you can manually update the distribution points for the package. Doing so updates the package information on all of its distribution points immediately.

To update the settings of a package

1 On the Symantec System Recovery 2013 R2 Management Solution **Packages and Policies** tab, expand the **Update Packages** list in the left pane.

2 In the left pane, click a package name whose settings you want to change.

3 In the right pane, edit the settings under each tab name.

Package tab settings

Name	Indicates the package name.
Description	Lets you add a user-friendly description of the package.
Publisher	Indicates the package publisher.
Language	Indicates the package language.
Version	Indicates the package version.
Package Source	Indicates the location from which to access the package source files: ■ **Package does not contain source files** The package is a command line that is sent to the target computer. For example, a call to a utility such as `Chkdsk.exe`. The package contains no source files. ■ **Access Package from a local directory in the Notification Server computer** The package is stored in a local directory on the Notification Server computer. ■ **Access Package from existing UNC** The package is stored on a UNC source path and is downloaded through HTTP using the appropriate distribution point credential. ■ **Access Package from a URL** The package is accessed through an anonymous URL that points to the appropriate UNC source location.
Package Location	Indicates the location at which the package is stored. This location can be a local directory on the Notification Server computer. Or, it can be a UNC path or a URL location depending on the package source option that is specified.
Package files will be deleted from the client computer if unused for	Lets you specify the length of time after which an unused package is deleted from a managed computer. The following options are available: ■ **Never Delete** ■ **0 Days (delete immediately)** ■ **1, 2, 3 days, 1, 2 weeks, 1 month, 1 year**

Programs tab settings

Name	Indicates the program name. This field contains a drop-down list of programs that the package contains. The other settings on this tab apply to the selected program. This field is required.
Description	Lets you add a user-friendly description of the selected program. This field is optional.
Command Line	Indicates the command line to run the program, including switches and parameters if applicable. The command-line entry must be in the same location or path as the package. This field is required.
Working Directory	Indicates the directory where the files are temporarily stored during deployment by the program. If no directory is specified here, the system temp directory is used.
Success Codes **Failure Codes**	Determined by the exit code that is returned when an application ends. Applications can define their own exit codes for success and failures. However, a zero value is used for success and a non-zero value for failure. These fields are optional.
Estimated Disk Space	Indicates the estimated amount of disk space that the program requires to run on the target computer. The Symantec Management Agent ensures that at least one physical drive with the specified space is available before the program runs. This field is optional.
Estimated Run Time	Indicates the estimated time in minutes that the program requires to run on the target computer. This field is optional.
Terminate After	Indicates the timeout period, after which the program is terminated (as a failure) if it has not finished running. If this field is left blank or set to zero, the program terminates after 360 minutes.

After Running Lets you specify the action that is performed when the program finishes running:

- **No action required**
- **Restart computer**
- **Log off user**

Starting window Indicates the status of the command window that runs the program on a managed computer:

- **Normal**
- **Hidden**
- **Minimized**
- **Maximized**

Run with rights Lets you select the rights with which the program runs on the target computer:

- **System account**
- **Logged in user**
- **Specified user**
  If you select this option, you need to specify the user domain.

Program can run Lets you specify the conditions under which the program can run:

- **Whether or not a user is logged on**
- **Only when a user is logged on**
- **Only when no user is logged on**

User Input Required Specifies that the program brings up a user interface that may require user input to complete the process.

This field is valid only when the **Only when a user is logged on** option is selected in the **Program can run** field.

Minimum connection speed

Specifies the minimum connection speed for software delivery programs to be executed. Before the program runs, the connection speed from the Symantec Management Agent to Notification Server is tested. If the connection speed is less than the specified minimum speed, the program does not run.

The options are as follows:

- **No network connection required**
  No default minimum connection speed.
- **1, 2, 5, 10, 50, 100, 256, 512 KB/sec, or 1 MB/sec**
  The minimum connection speed.

Note: This setting applies to package execution, not to package download. The package must already be downloaded.

Package Servers tab settings

Package Destination Location on Package Servers

Lets you assign the package to a specific directory on the package servers instead of the default directory. You only need to specify a directory if you do not want to use the default location. Specify a UNC path.

If nothing is specified here, the default location is used:

installation_path\Symantec\Symantec Management Agent\Agents\SoftwareManagement\Software Delivery*package_GUID*\cache

Assign packages to Specifies the package servers to which the package is assigned.

The options are as follows:

- **All Package Servers**
  Assigns the package to all package servers.
- **Package Servers Individually**
  Assigns the package to selected package servers.
- **Package Servers by Site**
  Assigns a site to packages from a list of configured sites in the **Site Maintenance** configuration page. When a site is assigned to a package, all package servers within the selected site host the package.
- **Package Servers Automatically with manual prestaging**
  Occurs when a task that requires the package is assigned to a resource target. All the computers that the resource target identifies requires the package. The package is assigned to all of the sites that are associated with those computers. The package is downloaded to all the package servers that are in those sites.
  This option also lets you manually assign packages to additional sites if necessary.

Advanced tab settings

Agent display name Identifies the package name to be displayed on the Symantec Management Agent. This name can be different than the package name that is specified on the **Package** tab.

This setting lets you supply a package name that makes sense to the user . The name that is specified on the **Package** tab may make sense only to an administrator.

Agent display description Lets you supply a package description that tells the user what the package does on the managed computer. This description can be different than the package description that is specified on the **Package** tab.

Enable verbose reporting of Package Status events	Lets you enable the sending of package status events to Notification Server. Disabling events for the package prevents Symantec Management Agents from sending AeX SWD Package events to Notification Server. The Notification Server computer Event Capture settings in the Global Symantec Management Agent Settings policy take precedence to the **Enable Verbose Reporting** feature. Events are sent only if they are enabled in the Global Symantec Management Agent Settings policy. The following types of AeX SWD Package events are not sent if package events are disabled: ■ New Package ■ Package Updated ■ Package To Be Removed ■ Package Removed ■ Unable To Check Package ■ Insufficient Disk To Download Package ■ Download Complete ■ Package Download Blocked
Use alternate download destination on client	If this option is enabled, package files are delivered to managed computers at the specified alternate destination. When the task executes, package files are copied to the new location. The Symantec Management Agent never deletes copied package files. They are copied each time the task runs. Therefore, if the task is running on a recurring schedule, the files are copied repeatedly. This process may be useful to ensure that the user of a managed computer does not delete a required file. If this option is not enabled, the default location is used: *installation_path*\Symantec\Symantec Management Agent\Agents\SoftwareManagement\SoftwareDelivery*package_GUID*cache

4 When you are finished making changes to the package, click **Update Distribution Points**.

5 Click **Save Changes** to confirm the new settings.

Uninstalling Symantec System Recovery-related products from the Symantec Management Platform

You can uninstall Symantec System Recovery 2013 R2 Management Solution or Symantec System Recovery-related products from the Symantec Management Platform by using Symantec Installation Manager. If you uninstall the Symantec System Recovery 2013 R2 Management Solution, the solution and any other related installed Symantec System Recovery products are also uninstalled.

You may choose to uninstall Symantec System Recovery 2013 R2 Management Solution. If so, be aware that the following items are not uninstalled from any managed client computers that you added to the console:

- Symantec System Recovery
- Symantec System Recovery Plug-in
- LightsOut Restore

To uninstall Symantec System Recovery and related components from client computers, you must use the Symantec System Recovery 2013 R2 Management Solution. Therefore, you should run the uninstall policies for the following products and components, in the following order:

- Run the LightsOut Restore Uninstall policy
- Run the Symantec System Recovery or the Symantec System Recovery Linux Edition Uninstall policy
- Run the Symantec System Recovery Plug-in or the Symantec System Recovery Linux Edition Plug-in Uninstall policy

See "Uninstalling Symantec System Recovery-related products and components from client computers" on page 46.

Following the uninstallation of these items, you can use Symantec Installation Manager to uninstall Symantec System Recovery 2013 R2 Management Solution.

To uninstall Symantec System Recovery-related products from the Symantec Management Platform

1. Start Symantec Installation Manager.
2. In the **Installed Products** page, select the Symantec System Recovery 2013 R2 Management Solution product to uninstall.

3 Click **Uninstall**, and then click **Yes** to confirm the removal of the product.

The product is uninstalled from the Symantec Management Platform. The solution no longer appears in the console and all entries in the database are deleted.

4 On the **Uninstallation Complete** page, click **Finish**.

Adding or removing recovery point passwords

For each backup policy or **Independent Backup** task that you create, you can optionally assign a password to the resulting recovery point for added security. Over time, the number of different passwords that you use can accumulate. This situation can make it difficult to remember which password to use for a given task. For example, with a **Convert to Virtual** task you use multiple recovery points that may each have different passwords assigned to them. In such cases, you can use the password store to add all potential passwords that you have used.

Any password that you assign to a backup policy or an **Independent Backup** task is also added to the password store.

Adding recovery point passwords to the password store

You can add recovery point passwords to the password store to aid in the recovery or conversion of multiple password-protected recovery points.

Any password that you assign to a backup policy or an **Independent Backup** task is also added to the password store.

To add recovery point passwords to the password store

1 On the Symantec System Recovery 2013 R2 Management Solution **Packages and Policies** tab, expand the **Password Management** list in the left pane.

2 Click **Password Store**.

3 In the right pane, in the **Password** field, type a password that you have used in a backup policy or an **Independent Backup** task.

4 Click **Add**.

5 Repeat steps 3 and 4 for each password that you have used.

6 Click **OK** when you are done.

Removing all recovery point passwords from the password store

You can remove all recovery point passwords from the password store.

To remove all recovery point passwords from the password store

1. On the Symantec System Recovery 2013 R2 Management Solution **Packages and Policies** tab, expand the **Password Management** list in the left pane.
2. Click **Manage Password**.
3. In the right pane, click **Clear password store**.
4. Click **OK**.

About managing recovery point destinations

You can define destinations where you want to store recovery points that managed computers create.

By defining recovery point destinations separate from backup policies and computers, you can see how many computers have backed up to a given destination. You can view this information in the **Destination** Web Part, on the **Home** page. You can also optimize the network load balance during a backup.

When you specify a local folder path as a recovery point destination, the path corresponds to the drive that is found on the client computer. It is not the path on the computer where the Symantec Management Console runs.

See "Creating default recovery point destinations" on page 68.

You can change an existing recovery point destination's network credentials. The change takes effect when the existing connection on the client computer is closed (usually by restarting).

To edit the destination path, you must define a new destination.

See "Editing network credentials for a recovery point destination " on page 70.

You can delete previously-defined destinations no longer used.

Note: Before you delete a recovery point destination, edit any backup policies that use the recovery point destination to specify a new destination. You cannot delete a recovery point destination that existing recovery points reference.

See "Deleting recovery point destinations" on page 71.

You can also assign a computer the task of copying recovery point sets from a recovery point destination to an Offsite Copy destination.

See "Configuring a Dedicated Offsite Copy task" on page 71.

Creating default recovery point destinations

You can define destinations where you want to store recovery points that client computers create. The destination must be accessible by the client computer that you back up.

See "About managing recovery point destinations" on page 67.

See "About Offsite Copy" on page 100.

See "Configuring a Dedicated Offsite Copy task" on page 71.

To create default recovery point destinations

1. On the Symantec System Recovery 2013 R2 Management Solution **Manage Tasks** tab, expand the **Destinations** area in the left pane.
2. In the left pane, in the **Destinations** tree, select a destination type.
3. On the toolbar in the middle pane, click **Create**.
4. Depending on the destination type you selected in the left pane, do one of the following:

If you selected **Local**	On the **Backup Destinations** panel, type a local folder path. The local folder path you specify is relative to the managed client computer. It is not the folder path on the computer where you run Symantec Management Console. You can also use the specified local path as an off-site destination by selecting it from the **Off-site** drop-down list in a backup policy. USB is not supported as an off-site location.
If you selected **Network Shares**	On the **Backup Destinations** panel, do the following: ■ Type a UNC path to a network share. Make sure double backslash characters (\\) precede the UNC path. Or, type the IP address path to a network share. Make sure double backslash characters (\\) precede the IP address path. ■ In the **Network credentials** group box, type the domain\user_name (or workgroup\user_name). Type the password for logging on to the network storage location. You can also use the specified network share as an off-site destination by selecting it from the **Off-site** drop-down list in a backup policy.

If you selected **FTP**

On the **Backup Destinations** panel, type an FTP path that you can use with the **Offsite Copy** option in a backup policy.

You can also use the specified FTP path as an off-site destination by selecting it from the **Off-site** drop-down list in a backup policy.

If you selected **ESX**

On the **ESX Server** panel, do the following:

- Type the name of the VMware ESX server or the server's IP address.
- In the **ESX server credentials** group box, type a valid administrator user name that has sufficient rights.
- Type a valid password to the server.
- In the **Upload Locations** area, specify the path to the folder where the virtual disk files are written. Use the **Add**, **Remove**, and **Edit** options to configure the upload folder path you want.
- In the **Import Locations** area, specify the path to the folder where you want to import virtual disk files.

  The folder that you select must be different than the upload location folder.

  Use the **Add**, **Remove**, and **Edit** options to configure the import folder path you want.

The virtual disk files are transferred to an ESX server through a Secure Shell (SSH) and secure file transfer protocol (SFTP). You might need to change the settings on the ESX server. For more information, see your ESX server documentation.

If you selected **Linux**

In the **Backup Destinations** panel, type a Linux-based path name to a destination directory. For absolute path names, make sure a single forward slash character (/) precedes the path.

You do not need to specify a user name and password for a Linux-based destination

ESX Server Location options

ESX Server Name or Address

Specifies the name of the server or the server's IP address.

Note: The virtual disk files are transferred to an ESX server through a Secure Shell (SSH) and secure file transfer protocol (SFTP). You might need to change the settings on the ESX server. For more information, see your ESX server documentation.

ESX Server credentials	Specifies a valid administrator name that has sufficient rights and a valid password to the server.
Create ESX Server	Lets you add the defined ESX Server whose name or address and credentials you have specified.
Upload Location	Lets you specify the path to the folder where the virtual disk files are written. Use the **Add**, **Remove**, and **Edit** options to configure the upload folder path you want.
Import Location	Specifies the path to the folder where you want to import virtual disk files. **Note:** The folder that you select must be different than the upload location folder. Use the **Add**, **Remove**, and **Edit** options to configure the import folder path you want.

5 Click **Apply**.

Editing network credentials for a recovery point destination

You can change an existing recovery point destination's network credentials for a network share, FTP, or ESX path. The change takes effect when the existing connection on the client computer is closed (usually by restarting).

You cannot edit the destination to a local, network share, FTP, or Linux path. Instead, you must create a new destination.

See "About managing recovery point destinations" on page 67.

See "Creating default recovery point destinations" on page 68.

To edit network credentials for a recovery point destination

1 On the Symantec System Recovery 2013 R2 Management Solution **Manage Tasks** tab, expand the **Destinations** area in the left pane.

2 In the left pane, click the **Destinations** tree.

3 In the table, in the middle pane, select a network share, FTP, or ESX path with network credentials you want to edit.

4 On the toolbar in the middle pane, click **Edit**.

You cannot edit the destination to a local, network share, FTP, or Linux path. Instead, you must create a new destination.

5 In the **Network credentials** group box, type the new user name and password to the destination.

6 Click **Save changes**.

Deleting recovery point destinations

You can delete previously-defined destinations no longer used.

See "Editing a backup policy" on page 130.

See "About managing recovery point destinations" on page 67.

Note: Before you delete a recovery point destination, edit any backup policies that use the recovery point destination to specify a new destination. You cannot delete a recovery point destination that existing recovery points reference.

To delete recovery point destinations

1 In the Symantec System Recovery 2013 R2 Management Solution **Manage Tasks** tab, expand the **Destinations** list in the left pane.

2 In the left pane, click **Destinations**.

3 In the middle pane, in the table, select a destination path that you want to delete.

4 In the middle pane, on the toolbar, click **Delete**.

Configuring a Dedicated Offsite Copy task

You can assign a computer the task of copying recovery point sets from a recovery point destination to a dedicated Offsite Copy location. Configuring such a task is very efficient and powerful. Unlike specifying an Offsite Copy destination within a backup policy that may go to many computers, you use the system resources of one dedicated computer. That one dedicated computer processes an entire Offsite Copy task.

See "About Offsite Copy" on page 100.

See "About managing recovery point destinations" on page 67.

To configure a Dedicated Offsite Copy task

1. On the Symantec System Recovery 2013 R2 Management Solution **Monitor Tasks** tab, right-click **Symantec System Recovery Tasks**, and then click **New > Task**.
2. In the **Client Tasks** tree, click **Symantec System Recovery Tasks > Dedicated Offsite Copy**.
3. On the **Create New Task** page, in the right pane, type a name for the task.
4. Select the computer that you want to dedicate to the Offsite Copy task.
5. Do one of the following:
   - Click **Copy all recovery point sets**.
   - Select **Copy recovery point sets created by this computer**, and then select the computer that you want from the drop-down list.
   - Select **Copy recovery point sets that have recovery points created in the last**, and then specify the number of days in the text field.
   - Click **Specific recovery point sets**, and then select a recovery point set based on the date it was created.
6. Do one of the following:

To use an existing destination	In the **Offsite Destination** drop-down list, select the destination where you want the recover point sets to be copied.
To create a new destination	Select **Create new destination**, and then specify a local folder path or a UNC path to a network share. If you typed a UNC path, you must specify the necessary user name and password credentials. Click **Add Destination**.

7 Click **OK**.

8 In the **Task Status** field for your dedicated Offsite Copy task, do one of the following:

To run the task as soon as possible	Click **New Schedule**. Click **Now** or click **Schedule** at the bottom of the panel to run the task as soon as possible.
To schedule a time to run the task	Click **New Schedule**. Click **Schedule**. Specify the date and time to run the task. Click **Schedule** at the bottom of the panel.

About viewing filters

Symantec System Recovery 2013 R2 Management Solution includes numerous predefined filters that you can use to roll out Symantec System Recovery policies to client computers.

The following table describes a few of the predefined filters that are installed with Symantec System Recovery 2013 R2 Management Solution.

Table 3-4 Predefined filters

Filter	Description
Backup Policy	Lists the computers in which the backup policy is successfully deployed.
License Status	Includes the following license status filters: ■ **Licensed Symantec System Recovery computers** Lists the managed client computers that have a current license assigned to them. ■ **Trial licensed Symantec System Recovery computers** Lists the managed client computers that have a trial version of Symantec System Recovery installed. ■ **Unlicensed Symantec System Recovery computers** Lists the number of managed client computers on which an expired trial version of Symantec System Recovery is installed.

Table 3-4 Predefined filters *(continued)*

Filter	Description
Linux	Includes the following Linux filters: ■ Computers with Symantec System Recovery 2013 R2 installed ■ Red Hat Enterprise Linux Server 5 with Symantec System Recovery Plug-in installed ■ Red Hat Enterprise Linux Server 6 with Symantec System Recovery Plug-in installed ■ SUSE Linux Enterprise Server 10 with Symantec System Recovery Plug-in installed ■ SUSE Linux Enterprise Server 11 with Symantec System Recovery Plug-in installed
All computers with Symantec System Recovery installed	Lists the managed client computers that have Symantec System Recovery 2013 R2 or 2011, Backup Exec System Recovery 2010, or Symantec System Recovery 2013 R2 Linux Edition installed.
Windows computers with LightsOut Restore installed	Lists the managed Windows client computers that have LightsOut Restore 2013 R2 installed.

When you are in the **Manage Tasks** tab of Symantec System Recovery 2013 R2 Management Solution, you can filter the displayed results in the table. You use the **Filter results** bar in the middle pane. You can also add the filtered results path to the **Favorites** area in the left pane on the **Manage Tasks** tab. Adding filter paths to **Favorites** can help you save time by letting you get to specific data quickly.

See "Viewing Symantec System Recovery 2013 R2 Management Solution filters" on page 74.

See "Viewing the filters and policies that are assigned to a client computer" on page 75.

See "Adding a filtered results path in the Manage Tasks tab to Favorites" on page 76.

Viewing Symantec System Recovery 2013 R2 Management Solution filters

You can view a variety of predefined Symantec System Recovery 2013 R2 Management Solution filters.

See "About viewing filters" on page 73.

To view Symantec System Recovery 2013 R2 Management Solution filters

1. In the Symantec Management Console, on the toolbar, click **Manage > Filters**.
2. In the **Filters** tree, click **Computer Filters > Symantec System Recovery Filters**.
3. In the left pane, select a filter name to view all the computers in the right pane that are currently assigned to that filter.

Viewing the filters and policies that are assigned to a client computer

You can use the **Resource Manager** in the console to view the following information:

- Filters that a computer is a member of.
- Policies that have been applied to a computer.

See "About viewing filters" on page 73.

To view the filters and policies that are assigned to a client computer from the Symantec Management Console

1. In the Symantec Management Console, on the toolbar, click **Manage > Filters**.
2. On the **Filters** tree, click **Computer Filters > Symantec System Recovery Filters**, and then select a filter.
3. In the right pane of the console, double-click a computer name to open it in the Resource Manager.
4. On the **Summaries** menu, do one of the following:
   - To view the filters for which the managed client computer is a member, click **Filter Summary**.
   - To view the policies that are applied to the managed client computer, click **Policy Summary**.

To view the filters and policies that are assigned to a client computer from Symantec System Recovery 2013 R2 Management Solution

1. On the Symantec System Recovery 2013 R2 Management Solution **Manage Tasks** tab, expand the **Computers** list in the left pane.
2. In the left pane, under the **Computers** heading, do one of the following:
   - Click **Select Organizational Views**, and then select a computer group name.
   - Click **Computers**.
     If necessary, in the middle pane, use the **Filter results** bar to refine the list of computers.

- Expand the **Computers** tree and select a predefined filter name.

3. In the middle pane, in the table, select a computer name, and then click **Resource Manager** on the toolbar.
4. On the **Summaries** menu, do one of the following:
   - To view the filters for which the managed client computer is a member, click **Filter Summary**.
   - To view the policies that are applied to the managed client computer, click **Policy Summary**.

Adding a filtered results path in the Manage Tasks tab to Favorites

You can add filtered results paths in the **Manage Tasks** tab to the **Favorites** area in the left pane for convenience and faster access.

To add filtered results in the Manage Tasks tab to the Favorites area

1. On the Symantec System Recovery 2013 R2 Management Solution **Manage Tasks** tab, in the left pane, select any specific filter.
2. On the **Filter results** bar in the middle pane, select a field.
3. Continue selecting the filters you want to further refine the displayed results in the table.
4. Click the star icon to the right of the filter path.
5. Type a name that you want to give to the filtered results path.
6. Click **OK** to add the filtered results path to the **Favorites** area in the left pane.

About organizational views

An organizational view is a hierarchical grouping of resources (as organizational groups) that reflects a real-world structure, or view of your organization. For example, you may create organizational views to group your resources by geographical location, or by department, or by network structure.

The custom organizational views that you created using Symantec Management Platform are available in Symantec System Recovery 2013 R2 Management Solution. When you are in the **Manage Tasks** tab, you can use these organization views to filter the list of client computers.

Note: You cannot create organizational views from the Symantec System Recovery 2013 R2 Management Solution. The organizational views can be created from Symantec Management Platform only. For more information about organizational views, see the *Symantec Management Platform Administrator's Guide*.

See "Filtering the list of client computers using organizational views" on page 77.

Filtering the list of client computers using organizational views

You can select the organizational views to filter the list of client computers.

To filter the list of client computers using organizational views

1. On the Symantec System Recovery 2011 Management Solution **Manage Tasks** tab, in the left pane, click **Computers > Select Organizational Views**.
2. In the **Select Organizational Views** dialog box, select the appropriate organizational view.
3. Click **OK**.

See "About organizational views" on page 76.

About managing Symantec System Recovery license policies

You can add or delete Symantec System Recovery license policies. When you add a license policy, the license key information is stored in the Symantec System Recovery 2013 R2 Management Solution database.

When you delete license policies, the license is removed from the computer and the license information is removed from the database.

After you add a license policy, you can assign it to resource targets with an unlicensed version or trial version of Symantec System Recovery installed.

See "Adding Symantec System Recovery license policies" on page 79.

See "Deleting Symantec System Recovery license policies" on page 79.

You can assign or unassign Symantec System Recovery licenses to resource targets.

After you add a license policy, you can assign it to resource targets. The resource targets should have an unlicensed version or trial version of Symantec System Recovery installed. When you assign licenses, you activate Symantec System Recovery on the client computers and remove the 60-day trial.

Unassigning licenses from client computers returns Symantec System Recovery to a 60-day trial version. If you choose to delay installation of the license, all features in Symantec System Recovery remain enabled during a 60-day grace period. The grace period begins the first time you send a policy or a task to the managed client computer where Symantec System Recovery is installed.

You can unassign licenses from resource targets by using any one of the following methods:

- Remove the resource targets that are associated with the policy.
  Symantec System Recovery returns to a trial version on the affected resource targets.
- Delete the license policy.
  When you delete a license policy, the license is removed from the associated resource targets and the license file information is removed from the database. The policy is also removed from the License policy tree in the console.
- Disable the license policy.
  Removes the license policy entirely from assigned resource targets. The license file information remains in the Symantec System Recovery 2013 R2 Management Solution database.

See "Adding Symantec System Recovery license policies" on page 79.

See "Unassigning Symantec System Recovery licenses from client computers" on page 80.

You can review the license status of Symantec System Recovery on computers by using the Symantec System Recovery 2013 R2 Management Solution **Home** tab.

A computer is considered managed by Symantec System Recovery 2013 R2 Management Solution when the following is installed:

- The Symantec Management Agent.
- The Symantec System Recovery Plug-in.
- Symantec System Recovery.

The following table describes the different license status information that is available:

Table 3-5 Symantec System Recovery license status

Symantec System Recovery license status	Description
Licensed	The number of computers that have a current license assigned.

Table 3-5 Symantec System Recovery license status *(continued)*

Symantec System Recovery license status	Description
Not licensed	The number of computers on which an expired trial version of Symantec System Recovery is installed or on which no license was activated.
Trial licensed	The number of computers that have a trial version of Symantec System Recovery installed.

See "Checking the license status of Symantec System Recovery on client computers" on page 81.

Adding Symantec System Recovery license policies

You can add Symantec System Recovery license policies. For each license policy that you add, it is automatically enabled (turned on).

See "Deleting Symantec System Recovery license policies" on page 79.

See "About managing Symantec System Recovery license policies" on page 77.

To add Symantec System Recovery license policies

1. On the Symantec System Recovery 2013 R2 Management Solution **Manage Tasks** tab, expand the **Configuration Policies** list in the left pane.
2. In the left pane, under **Client Configuration Policies**, click **All Client Licenses**.
3. In the middle pane, on the toolbar, click **Create**.
4. In the **Licenses** panel, type the name that you want to associate with the Symantec System Recovery license policy.
5. Enter a valid Symantec System Recovery license key.
6. Click **Save changes**.

   You may need to click **Refresh** on the table filter toolbar to see the changes.

Deleting Symantec System Recovery license policies

You can delete Symantec System Recovery license policies.

See "Adding Symantec System Recovery license policies" on page 79.

See "About managing Symantec System Recovery license policies" on page 77.

To delete Symantec System Recovery license policies

1. On the Symantec System Recovery 2013 R2 Management Solution **Manage Tasks** tab, expand the **Configuration Policies** list in the left pane.
2. In the left pane, under **Client Configuration Policies**, click **All Client Licenses**.
3. In the middle pane, select a license policy that you want to delete.
4. On the table's toolbar, click **Delete**.
5. Click **OK** to confirm the deletion.

   You may need to click **Refresh** on the table filter toolbar to see the changes.

Assigning Symantec System Recovery licenses to client computers

You can assign Symantec System Recovery licenses to computers.

See "Unassigning Symantec System Recovery licenses from client computers" on page 80.

See "About managing Symantec System Recovery license policies" on page 77.

To assign Symantec System Recovery licenses to client computers

1. On the Symantec System Recovery 2013 R2 Management Solution **Manage Tasks** tab, expand the **Configuration Policies** list in the left pane.
2. In the left pane, under **Client Configuration Policies**, click **All Client Licenses**.
3. In the middle pane, select the name of the Symantec System Recovery license policy that you want to assign to computers.
4. In the table, check the **Enabled** column to make sure that the selected license policy is on.

   If the policy is off, click **Enable** on the table toolbar.
5. In the table toolbar, click **Assign**.
6. In the **Assign** panel, select the computer groups to which you want the policy applied.
7. Click **OK**.

   You may need to click **Refresh** on the table filter toolbar to see the changes.

Unassigning Symantec System Recovery licenses from client computers

You can unassign Symantec System Recovery licenses from computers.

See "Assigning Symantec System Recovery licenses to client computers" on page 80.

See "About managing Symantec System Recovery license policies" on page 77.

To unassign Symantec System Recovery licenses from client computers

1. On the Symantec System Recovery 2013 R2 Management Solution **Manage Tasks** tab, expand the **Configuration Policies** list in the left pane.
2. In the left pane, under **Client Configuration Policies**, click **All Client Licenses**.
3. In the table in the middle pane, select the name of a license policy that you want to unassign from computer groups.
4. Do one of the following:
   - On the table's toolbar, click **Delete**, and then click **OK**.
   - On the tables's toolbar, click **Disable**.

   You may need to click **Refresh** on the table filter toolbar to see the changes.

Checking the license status of Symantec System Recovery on client computers

You can review the license status of Symantec System Recovery on computers by using the Symantec System Recovery 2013 R2 Management Solution portal.

A computer is considered managed by Symantec System Recovery 2013 R2 Management Solution when the following is installed:

- The Symantec Management Agent.
- The Symantec System Recovery Plug-in.
- Symantec System Recovery.

See "About managing Symantec System Recovery license policies" on page 77.

To check the license status of Symantec System Recovery on client computers

1. On the Symantec System Recovery 2013 R2 Management Solution **Home** tab, in the upper-right corner, click **Edit**.
2. In the left pane, in the **Web Parts** tree, click **Symantec System Recovery 2013 R2 Management Solution**.
3. Select **License Status**.

4 Click **Add** to add license status to the list of Web parts that are displayed on the Symantec System Recovery **Home** page.

If **Add** is dimmed (unavailable), the Web Part is already added to the Symantec System Recovery 2013 R2 Management Solution **Home** tab.

5 Click **Apply** to return to the **Home** tab.

6 Do one of the following:

To view license status from the **License Status** Web Part	On the Symantec System Recovery 2013 R2 Management Solution **Home** tab, in the **License Status** Web Part, click **Licensed**, **Not Licensed**, or **Trial License**.
To view license status from the **Computers** filter, in the **Alerts and Failures** folder on the **Manage Tasks** tab	Do the following: ■ On the Symantec System Recovery 2013 R2 Management Solution **Manage Tasks** tab, expand the **Computers** list in the left pane. ■ Double-click **Alerts and Failures**. ■ Select a license status near the bottom of the list. You can further refine the displayed results by using the **Filter results** bar in the right pane. There must be two or more rows in the table to enable the **Filter results** bar. You can add the filtered results path to the **Favorites** area in the left pane. You click the star icon on the right side of the Filter results bar. Type a name for the Favorite, and then click **OK**.

Chapter 4

Managing backups

This chapter includes the following topics:

About backup policies

You can create backup policies to automate the creation of recovery points by using a daily, weekly, or monthly schedule. This method is useful if you want to create recovery points of managed client computers during off-hours when you are not present. Or, if you want to create a recovery point set without interrupting the normal

flow of work. If you create a recovery point set, you can also specify that certain events, like logging on or off of a computer, create incremental recovery points

By default, file names for scheduled independent recovery points or recovery point sets are appended with 001.v2i, 002.v2i, and so forth. File names for incremental recovery points within a recovery point set are appended with _i001.iv2i, _i002.iv2i, and so forth. For example, if your base recovery point were called C_Drive001.v2i, the first incremental recovery point would be called C_Drive001_i001.iv2i.

The name of the computer (where the backup occurs) is always appended to the recovery point file name.

Each backup policy that you create is added to the Backup Policies tree of the product.

You implement a backup policy by doing the following:

- Create a backup policy.
  You specify what to back up, the backup destination where the resulting recovery points are stored, and when to run the backup (scheduled or manually).
- Deploy a backup policy to one or more computer collections.

You can also specify the compression levels of recovery points, enable encryption and password protection, and search engine support for Google and Backup Exec Retrieve. Many other options are available that let you customize each backup according to your business needs.

The client computer must be turned on to create a recovery point at the scheduled time. However, Symantec Management Console does not need to be open for the backup to take place. Also, a remote user does not need to be logged on to the managed client computer. However, Windows must be started on the computer.

To verify that a backup completed as scheduled, you can use the Symantec System Recovery 2013 R2 Management Solution portal page to check backup status information. Or, you can review the Recovery Points report in the Reports folder of the Symantec System Recovery 2013 R2 Management Solution tree.

Note: Symantec System Recovery 2013 R2 Management Solution supports the recovery point files that are saved directly to a network hard disk or to a local hard disk on the client computer (including USB or FireWire drives). Symantec System Recovery 2013 R2 Management Solution does not support saving recovery point files directly to CD or DVD.

See “Creating a basic backup policy” on page 89.

You can also set advanced backup options for an existing backup policy. For example, you can specify the compression level of recovery points or run command files when a backup policy begins on client computers.

See “Creating an advanced backup policy” on page 105.

You can back up databases.

See “About backing up VSS-aware databases” on page 219.

See “About backing up non-VSS-aware databases” on page 221.

See “Recovery point sets and independent recovery points in backup policies” on page 85.

See “Tips for creating recovery points” on page 87.

See “About backing up dual-boot systems” on page 88.

Recovery point sets and independent recovery points in backup policies

The following table describes the advantages and disadvantages of scheduled independent recovery points or recovery point sets as part of your backup policy.

Warning: The full recovery point and all associated incremental recovery points that make up the recovery point set must be kept together in the same folder. If there are missing files, the recovery point becomes invalid and you cannot restore the data.

Table 4-1 Types of scheduled recovery points

Type	Description
Recovery point set	Consider the following when you create recovery point sets. ■ A recovery point set is the same as an Independent recovery point except that it also has incremental tracking enabled for the selected drive. ■ This type of backup creates a base recovery point. Additional recovery points are created but save only the hard disk sectors that have changed since the creation of the base recovery point or the previous incremental recovery point. ■ Incremental recovery points are created faster than the first (base) recovery point and use less storage space than an independent recovery point. ■ Recovery point sets are ideal when you combine them with a schedule. ■ When you restore to a given point in time, the full recovery point plus all the incrementals up to that point in time are used for the restore. For example, suppose you have a full recovery point with eight incremental recovery points. You decide to restore the fourth incremental that was taken. When you restore, the full recovery point and the first four incrementals are used to restore the computer. ■ You can free hard drive space by deleting outdated recovery points and incremental recovery points.

Table 4-1 Types of scheduled recovery points *(continued)*

Type	Description
Independent recovery point	Consider the following when you create independent recovery points. ■ An independent recovery point creates a complete, independent copy of the entire selected drive. ■ An independent recovery point is not associated with incremental recovery points or recovery point sets in any way. As such, independent recovery points stand on their own and are usually a less complicated method for protecting your computer than recovery point sets. You can create an independent recovery point of a drive (using a one-time backup) even if that drive is tracked with a recovery point set. See "Creating an independent backup task" on page 118. See "Deploying an existing backup policy as soon as possible" on page 128. ■ This backup type typically requires more storage space on a hard disk than a recovery point set.

See "About backup policies" on page 83.

Tips for creating recovery points

The following information may help when you create recovery points:

- Because Notification Server works with a database, you should back up the server on a regular basis.
- Symantec Management Console does not need to be open for a scheduled backup to start or run. Therefore, after you create a backup policy and assign it to resource targets, you can exit the console. The client computer that you manage, however, must be turned on and Windows must be started. To verify that the creation of a recovery point is in progress, check the **Status** tab of a selected backup policy. To verify that a recovery point was made, you can review the information on the Symantec System Recovery 2013 R2 Management Solution portal page.

- All backup policies are saved in the Symantec System Recovery 2013 R2 Management Solution database so that you can edit or run them later.
- Store recovery points to a network share or to a hard disk on the managed client computer other than the primary hard disk C. This practice helps ensure that you can recover the system in the event that the client's primary hard disk fails.
- Avoid the need to run a disk defragmentation program on the managed client computer during the creation of recovery points. Doing so significantly increases the time it takes to create the recovery point, and it may cause unexpected system resource issues on the client computer.
- If you have two or more drives that are dependent on each other, or they are used as a group by a program like a database service, include both drives in the same backup policy. Back up multiple drives simultaneously by selecting two or more drives in the **Create New Backup Policy** Web page.
- Include multiple drives in the same backup policy to reduce the total number of backups that must be run.
- Avoid storing recovery points on the Symantec System Recovery 2013 R2 Management Solution computer. As the number or size of recovery points grows, you have less disk space available for regular server use. When you save recovery points to a separate drive or a network location, this problem is eliminated. Also, if you decide to store recovery points on the client computer, store them to a secondary hard disk. Avoid storing them on the primary hard disk C. This practice helps ensure that you can recover the system in the event that the client's primary hard disk fails.

See “About backup policies” on page 83.

About backing up dual-boot systems

You can back up dual-boot systems. You can also back up computers with more than one operating system, even if you have drives (partitions) that are hidden within the operating system where you run the software.

When you run a backup, everything on the drive is included in the recovery point so that you can start your computer later if you restore it. An exception is if you back up a bootstrapped operating system. In such cases, you must back up and then restore every drive with operating system boot information. This kind of restore allows your computer to boot in the same way from a restored system as it did from the original configuration.

Note: You should not create incremental recovery points of shared data drives. This applies ifSymantec System Recovery is installed on both operating systems, and they are both set to manage the shared drive.

You may encounter issues if you try to use Symantec System Recovery LightsOut Restore or Symantec System Recovery Restore Anyware on a dual boot system.

See "About backup policies" on page 83.

Creating a basic backup policy

You can automate the creation of recovery points with a daily, weekly, or monthly schedule. If you create a recovery point set, you can also specify that certain events, like logging on or off a computer, create incremental recovery points.

When a backup runs, each snapshot is stored on your computer as a recovery point. You can use the recovery point to restore your computer to the point in time when you created the snapshot.

Note: Symantec recommends that you enable AES encryption for the recovery points so that only users with passwords can mount the files.

See "About backup policies" on page 83.

See "Creating an advanced backup policy" on page 105.

See "Editing a backup policy" on page 130.

See "Editing the schedule of a backup policy" on page 139.

To create a basic backup policy

1. On the Symantec System Recovery 2013 R2 Management Solution **Manage** tab, in the left pane, expand the **Backup Policies** list in the left pane.
2. Select the type of recovery point that you want the backup policy to create, and then click **New > Backup Policy**.

   See "Recovery point sets and independent recovery points in backup policies" on page 85.
3. On the **Backup Policies** panel, in the **Name** text field, type a descriptive name for the new backup policy.
4. In the **Drives** field, click the hyperlink.

5 On the **Backup Policy Drives** panel, set the drive option you want, and then click **Apply**.

All drives on selected computers	Lets you define a backup policy for two or more computers. You should select this option to protect all drives (including hidden or unmounted), that exist on the client computers.
By Drive	Lets you select the drives that you want to back up on the selected client computers. If you chose to create a recovery point set, hidden drives are not displayed in the **By Drive** list. Sometimes a selected drive letter is not available for backing up on a particular client computer. The drive has been deleted or the entire hard disk has been removed from the client computer since Symantec System Recovery was installed. In such cases, when the recovery point is created, it does not include the drive.

6 In the **Schedule** field, click the hyperlink.

7 On the **Backup Policy Schedule** panel, set the schedule options you want, and then click **Apply**.

The available scheduling options depend on the recovery point type that you selected.

Backup Policy Schedule tab options for a recovery point set

Schedule	Lets you select the days and a start time for when the backup should run.
Start time (24 hour format)	Lets you customize the start time of the backup .
Sun Mon Tue Wed Thu Fri Sat	Lets you customize the days of the week for the backup to run. The default is to run the backup Monday through Friday.
Run more than once per day	Lets you run the backup more than once a day to protect the data that you edit or change frequently.
Time between backups	Lets you specify the maximum time that should occur between backups.
Number of times	Lets you specify the number of times per day that the backup should run.

Automatically optimize

Lets you select how often optimization should occur for the backup destination to manage the used disk space.

You can choose from the following options:

- **Never**
  Indicates that no deletion of incremental recovery points is performed.
- **Every four hours**
  Indicates that a deletion of incremental recovery points that are four hours old (or older) is performed every four hours. Also, after the first incremental of the day is taken, all incremental files from two days previous are consolidated to a single file.
- **Every twelve hours**
  Indicates that a deletion of incremental recovery points that are 12 hours old (or older) is performed every 12 hours. Also, after the first incremental of the day is taken, all incremental files from two days previous are consolidated to a single file.

Distribute strategy randomly across (minutes)

Indicates that the policy is distributed randomly across a specified number of minutes (0-1440) to all the computers that are assigned to the policy. This option applies if you save recovery points to a network destination.

For example, suppose you want to distribute a backup policy in 60 minutes to 120 computers. Each of the 120 computers would randomly choose a time within the 60 minutes, before or after the scheduled start time, to start the backup.

This option helps to run not the policy at the same start time for all computers, which can cause a denial of service condition on the network, the recovery point destination, or both.

Start a new recovery point set

Lets you select how frequently a new recovery point set should be started.

Your options for starting new recovery point set (base) include the following:

- **Weekly**
  Creates a new recovery point set on the first scheduled or manual backup of the week.
- **Monthly**
  Creates a new recovery point set on the first scheduled or manual backup of the month.
- **Quarterly**
  Creates a new recovery point set on the first scheduled or manual backup every three months from the date when you selected this option.
- **Yearly**
  Creates a new recovery point set on the first scheduled or manual backup of the year, once a year, on the date that you selected for this option.
- **Custom**
  Lets you set specific weekly or monthly options for starting a new recovery point set.

Custom

Lets you customize the start time, and the days of the week or month to run the backup.

Note: If you choose to archive recovery points, consider creating recovery point sets more frequently to keep the size of your recovery point sets smaller.

Backup Policy Triggers tab options for a recovery point set

Any application is installed

Indicates that an incremental recovery point is created at the time users begin to install a software application on their computer.

Specified applications are launched

Indicates that an incremental recovery point is created at the time users run a specified software application on their computer.

Any user logs on to the computer

Indicates that an incremental recovery point is created when users log on to Windows on their computer.

Any user logs off from the computer	Indicates that an incremental recovery point is created at the moment users log off from Windows on their computer (but does not turn off Windows).
Data added to the drive exceeds	Indicates that an incremental recovery point is created when the added data on a drive exceeds an amount (in megabytes) that you specify.

Backup Policy ThreatCon tab options for a recovery point set

Do Not Monitor - Disable	Lets you turn off monitoring of ThreatCon levels for the selected backup policy. **Note:** Level 1 of Symantec ThreatCon indicates that there are no discernable security threats. Because level 1 suggests no threats, it is not an option.
Level 2	Security threats can occur, although no specific threats have been known to occur.
Level 3	An isolated security threat is in progress.
Level 4	Extreme global security threats are in progress.

Backup Policy Schedule options for an independent recovery point

Automatically create a recovery point

Lets you specify a weekly or monthly backup schedule.

The scheduling options include the following:

- **Weekly**
  Creates a new, independent recovery point on each day of the week that you check, and at the specified time. When you create independent recovery points one or more times per week, large amounts of disk storage space may be required.
- **Monthly**
  Creates a new, independent recovery point on each day of the month that you check, and at the specified time.
- **No Schedule**
  Saves all of the backup policy settings except a schedule. You can later deploy the backup policy at your convenience by assigning a schedule to the policy.

You can also create a single independent recovery point once, with no schedule.

See "Creating an independent backup task" on page 118.

Start time (24 hour format)

Lets you customize the start time of the backup .

Days of the week

Lets you customize the days of the week for the backup policy to run.

Days of the month

Lets you customize the days of the month for the backup policy to run.

Distribute strategy randomly across (minutes)

Indicates that the policy is distributed randomly across a specified number of minutes (0-1440) to all the computers that are assigned to the policy. This option applies if you save recovery points to a network destination.

For example, suppose you want to distribute a backup policy in 60 minutes to 120 computers. Each of the 120 computers would randomly choose a time within the 60 minutes, before or after the scheduled start time, to start the backup.

This option helps to not run the policy at the same start time for all computers, which can cause a denial of service condition on the network, the recovery point destination, or both.

8 On the **Backup Policies** panel, do one of the following:

- On the **Destination** list, select a local target folder.
- Click **Define destination**. On the **Backup Destination** panel, set the options you want, and then click **Apply**.
  When you click Define Destination and select a network destination to save the recovery points, the backup is not encrypted.

Note: Symantec recommends that you use AES encryption when you define a backup to prevent unauthorized access to the files.

Enter a folder relative to the managed computers	Indicates the location where you want to store the recovery points, relative to the managed computers.
Browse	Lets you browse to locate a destination that you want to use, relative to the managed computers. You must have create, read, and write privileges at the specified location. If there is insufficient space at the destination where the recovery point is stored, the policy fails and an error is reported on the Symantec System Recovery 2013 R2 Management Solution **Home** tab.
User name	Lets you specify the user name to a destination folder that is located in a network path.
Password	Lets you specify the password to a destination that is located in a network path.
Confirm password	Lets you retype the password for confirmation.

See "About managing recovery point destinations" on page 67.

9 Optionally, select **Create subfolder for each computer** if you want to create new subfolders on the network share that serves as the backup destination.

The new subfolders are given the same names as each client computer that is backed up. For example, suppose you have two client computers. One is named "CathyReadLaptop" and the other is named "MyLaptop". The new subfolders are named \CathyReadLaptop and \MyLaptop.

10 Optionally, if you want to make copies of your recovery points to store at a remote location for added backup protection, do one of the following:

- In the **Offsite Copy** list, select an off-site destination.

- In the **Offsite Copy** list area, click **Define Destination**. Specify the path to an external drive, a network server, or an FTP server, and then click **Apply**.

All drives on selected computers	Lets you define a backup policy for two or more computers. You should select this option to protect all drives (including hidden or unmounted), that exist on the client computers.
By Drive	Lets you select the drives that you want to back up on the selected client computers. If you chose to create a recovery point set, hidden drives are not displayed in the **By Drive** list. Sometimes a selected drive letter is not available for backing up on a particular client computer. The drive has been deleted or the entire hard disk has been removed from the client computer since Symantec System Recovery was installed. In such cases, when the recovery point is created, it does not include the drive.

See "About Offsite Copy" on page 100.

11 In the **Enable password protection** panel, enter the following information.

Enable password protection	Sets a password and enables AES encryption on the recovery point when it is created. This check box is selected by default.
Password	Lets you specify a password for the backup. Passwords can include standard characters. Passwords cannot include extended characters, or symbols. (Use characters with an ASCII value of 128 or lower.) You must type this password before you restore a backup or view the contents of the recovery point.
Confirm password	Lets you retype the password for confirmation.

AES encryption

Encrypts recovery point data to add another level of protection to your recovery points.

Note: If the **Use Password** check box is selected, you must define AES encryption.

Choose from the following encryption levels:

- **Standard 128-bit (8+ character password)**
- **Medium 192-bit (16+ character password)**
- **High 256-bit (32+ character password)**

You may have older backup policies created using Symantec System Recovery 2013 Management Solution or Symantec System Recovery 2011 Management Solution, where password protection was not enabled. If you edit the older policies using Symantec System Recovery 2013 R2 Management Solution, the AES Encryption field displays **None**. You need to select one of the options in the list to enable AES encryption.

While higher strengths require longer passwords, the result is greater security for your data.

Note: When you create a backup policy, the password that you enter in this option is also automatically added to the recovery point password store.

See "Creating an advanced backup policy" on page 105.

See "Adding or removing recovery point passwords" on page 66.

See "Creating an independent backup task" on page 118.

See "Editing a backup policy" on page 130.

See "Editing the schedule of a backup policy" on page 139.

12 Click **Save changes**.

13 In the middle pane, click **Apply** on the toolbar.

14 Select the targets to which you want the policy to be applied, and then click **OK**.

You can also click **Unapply** on the toolbar in the middle pane to remove the policy from selected targets.

About recovery points stored on a network destination

You can choose to store recovery points on a selected network destination. To do this, you need to specify the UNC path (\\server\share\folder) to the folder on the network where you want to store the recovery points. Alternatively, you can browse to the appropriate network share.

Table 4-2 Recovery point options stored on a network destination

Option	Description
Enter a folder relative to the managed computers	Indicates the location where you want to store the recovery points, relative to the managed computers.
Browse	Lets you browse to locate a destination that you want to use, relative to the managed computers. You must have create, read, and write privileges at the specified location. If there is insufficient space at the destination where the recovery point is stored, the policy fails and an error is reported on the Symantec System Recovery 2013 R2 Management Solution **Home** tab.
User name	Lets you specify the user name to a destination folder that is located in a network path.
Password	Lets you specify the password to a destination that is located in a network path.
Confirm password	Lets you retype the password for confirmation.

See "About recovery points stored in a local folder on the client computer" on page 99.

See "Creating default recovery point destinations" on page 68.

You also have the option to create a subfolder (selected by default) for each computer's recovery points at the network destination. If you clear this option, all recovery points for all computers that are assigned to the backup policy are stored at the root of the network destination.

See "About managing recovery point destinations" on page 67.

Recovery point file names are unique and include the name of the computer. You can use the same network storage location for multiple computers or for groups of computers that you have created in the console.

The user name that you enter needs a read or write access to the network folders where the recovery points are stored. The product uses this logon information to access the network when you create a recovery point.

Note: You should avoid storing recovery points on the Symantec System Recovery 2013 R2 Management Solution computer. As the number or size of backups grows, you have less disk space available for regular server use. When you save recovery points to a separate drive or a network location, the problem is eliminated. Also, if you decide to store recovery points on the client computer, store them to a secondary hard disk and not on the C drive. This practice helps ensure that you can recover the system in the event that the client's primary hard disk fails.

About recovery points stored in a local folder on the client computer

You can store recovery points locally by specifying a drive and folder (for example, E:\Data_RPoints\) on the hard drive of the client computer. Recovery points that are stored on the local hard drive of the managed client computer are accessed only by that computer.

Table 4-3

Option	Description
Enter a folder relative to the managed computers	Indicates the location where you want to store the recovery points, relative to the managed computers.
Browse	Lets you browse to locate a destination that you want to use, relative to the managed computers. You must have create, read, and write privileges at the specified location. If there is insufficient space at the destination where the recovery point is stored, the policy fails and an error is reported on the Symantec System Recovery 2013 R2 Management Solution **Home** tab.
User name	Lets you specify the user name to a destination folder that is located in a network path.
Password	Lets you specify the password to a destination that is located in a network path.
Confirm password	Lets you retype the password for confirmation.

See "About recovery points stored on a network destination" on page 98.

See "Creating default recovery point destinations" on page 68.

Warning: Saving recovery points to a network share or to a secondary hard disk on the client computer is highly recommended.

While you can save recovery points to the same drive that you are backing up, it is not recommended for the following reasons:

- If the computer suffers a catastrophic failure, such as the failure of a primary hard drive, you cannot restore the recovery point you need. Such occurrences can happen even if you save the recovery point to a different drive on the same hard disk.
- As the number or size of recovery points grows, you have less disk space available for regular use.
- The recovery point itself is included in subsequent recovery points of the drive. As a result, the size of recovery points increases exponentially over time.

Recovery points are stored on the computer itself, not on the computer where you run the Symantec System Recovery 2013 R2 Management Solution console.

About Offsite Copy

Backing up data to a secondary hard disk is a critical first step to protect your information assets. To make certain your data is safe, you can use the Offsite Copy feature when you create a backup policy to copy the latest recovery points. You can have them copied to an external storage device, a network share, or to a remote FTP server.

Regardless of the copy method you use, Offsite Copy provides a crucial level of redundancy that required if your office becomes inaccessible. Offsite Copy can double your data protection by ensuring that you have a remote copy.

See “Creating default recovery point destinations” on page 68.

The following are three different methods you can use to configure the Offsite Copy feature in Symantec System Recovery 2013 R2 Management Solution:

- You can configure a task to use a computer that is dedicated to Offsite Copy. This is the most efficient way to use the Offsite Copy feature.
  See “Configuring a Dedicated Offsite Copy task” on page 71.
- You can create a backup policy and specify an Offsite Copy destination as part of that policy.
  See “Creating a basic backup policy” on page 89.
- You can edit an existing backup policy and specify an Offsite Copy destination as part of that policy.
  See “Editing a backup policy” on page 130.

When you enable Offsite Copy through a backup policy, you specify up to two off-site destinations. After the backup policy finishes creating recovery points, Offsite

Copy verifies that the off-site destinations are available. Offsite Copy then begins copying the new recovery points to the Offsite Copy destination.

The most recent recovery points are copied first, followed by the next newest recovery points. If you have set up two Offsite Copy destinations, Offsite Copy copies recovery points to the destination that was added first. If an Offsite Copy destination is unavailable, Offsite Copy tries to copy recovery points to the second destination, if it is available. If neither destination is available, then Offsite Copy copies the recovery points the next time an Offsite Copy destination becomes available.

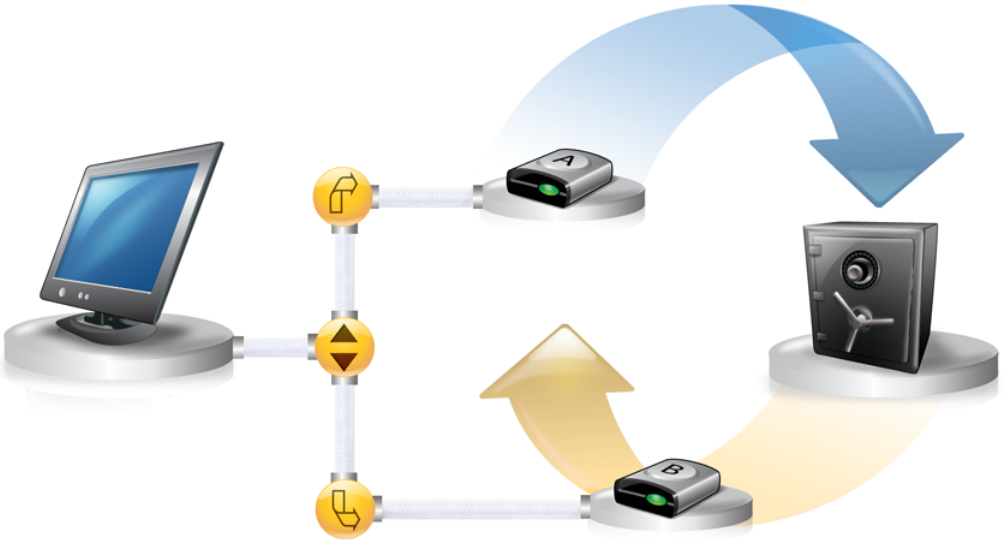
For example, suppose you have configured a backup policy to run at 18:00 and configured an external drive as an Offsite Copy destination. However, when you leave the office at 17:30, you take the drive with you for safekeeping. When the backup policy completes at 18:20, Symantec System Recovery detects that the Offsite Copy destination drive is not available and the copy process is ended. The following morning, you plug the drive back in to the computer. Symantec System Recovery detects the presence of the Offsite Copy destination drive and copies your recovery points.

About using external drives as your Offsite Copy destination

You can use an external drive as your Offsite Copy destination. This method lets users take a copy of their data with them when they leave the office. By using two external hard disks, the users can be certain that they have a recent copy of their data both on site and off site.

For example, suppose on a Monday morning you define a new backup policy of a system drive on a user's computer. You choose a recovery point set as the backup type. The user has set up an external drive (A), which you use as the first Offsite Copy destination. The user has also added another external drive (B), which you use as the second Offsite Copy destination. You schedule the backup job to run every midnight except on the weekends. You also enable recovery point encryption to protect the user's data from unauthorized access.

Before the user leaves the office on Monday evening, drive A is plugged in and drive B is taken home by the user.



On Tuesday morning, the user finds that Monday's base recovery point is successfully copied to drive A. At the end of the day, the user unplugs drive A and takes it home for safekeeping.

On Wednesday morning, the user brings drive B to the office and plugs it in. Symantec System Recovery detects that drive B is an Offsite Copy destination. The next time the backup policy runs, Symantec System Recovery begins copying Monday night's base recovery point and Tuesday night's incremental recovery point. At the end of the day Wednesday, the user takes drive B home and places it in a safe place with drive A.

The user now has the following:

- Multiple copies of recovery points stored at two separate, physical locations.
- The original recovery points are stored on their backup destinations at the office.
- Copies of those same recovery points are also stored on their Offsite Copy destination drives.

The Offsite Copy destination drives are stored in a safe place at the user's home.

The next morning, Thursday, the user takes drive A to the office and plugs it in. Tuesday and Wednesday night's recovery points are copied to drive A.

Each time the user plugs in either drive A or B, the latest recovery points are added to the drive. This method provides multiple points in time for recovering their

computer in the event that the original backup destination drives fail or become unrecoverable.

Using external drives as Offsite Copy destinations ensures that users have a copy of their backup data stored at two separate, physical locations.

Symantec System Recovery does not support a USB drive that is used as an Offsite Copy destination on a client computer. If a client computer is brought under management and it already had a local backup job defined that uses a USB drive as an Offsite Copy destination, the local backup job is deleted

If a local drive, with the same drive letter, exists on the computer to which the backup policy is assigned, the backup policy is marked as supported in the Symantec System Recovery 2013 R2 Management Solution user interface.

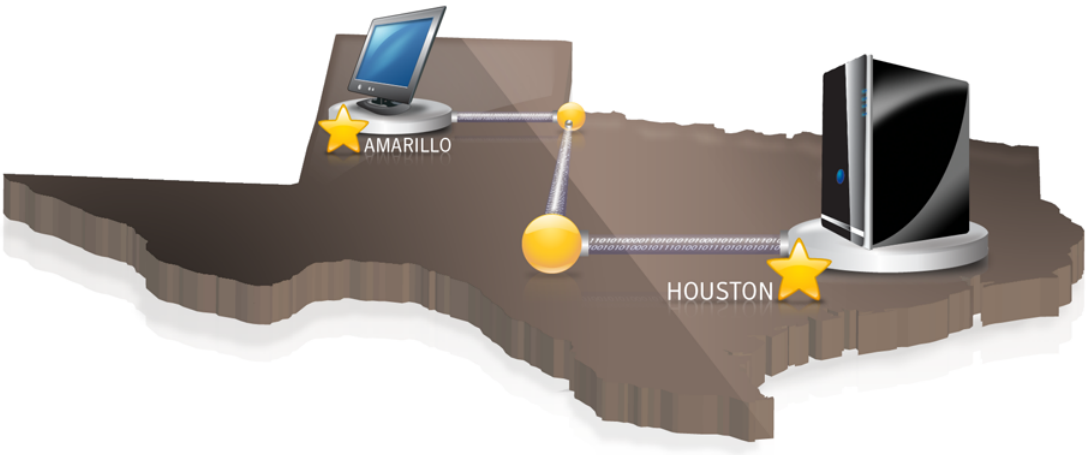
About using a network share as the Offsite Copy destination

You can specify a local area network share as an Offsite Copy destination. You must be able to access the server that you plan to use. You must either map a local drive to the server or provide a valid UNC path.

For example, suppose that you set up a local external drive as your first Offsite Copy destination. Then you identify a server that is located at a second physical location from your own office. You add the remote server as a second Offsite Copy destination. As backups occur, recovery points are copied first to the external hard drive, and then to the remote server.

If the remote server becomes unavailable for a period of time, Offsite Copy copies all recovery points that were created since the last connection. If an Offsite Copy destination runs out of storage space for recovery points, the Offsite Copy task stops and an error is logged in Symantec System Recovery. You can review the error information in Symantec System Recovery 2013 R2 Management Solution by viewing the details of a client computer.

See "Viewing Symantec System Recovery details for a client computer" on page 146.



About using an FTP server as your Offsite Copy destination

Using an FTP server as your Offsite Copy destination is similar to using a network path. You must provide a valid FTP path to the FTP server.

You must also provide the correct FTP connection information to Symantec System Recovery 2013 R2 Management Solution in order for this method to work correctly. When Offsite Copy is configured correctly, it copies recovery points to the folder that you specified on the FTP server. If the server becomes unavailable for a period of time, Offsite Copy copies all recovery points that were created since the last connection.

If an Offsite Copy destination runs out of storage space for recovery points, the Offsite Copy task stops and an error is logged in Symantec System Recovery. You can review the error information in Symantec System Recovery 2013 R2 Management Solution by viewing the details of a client computer.

See "Viewing Symantec System Recovery details for a client computer" on page 146.

Creating an advanced backup policy

When you create or schedule a basic backup policy, you can set advanced options for recovery points, if wanted.

See "Creating a basic backup policy" on page 89.

See "Editing a backup policy" on page 130.

See "Editing the schedule of a backup policy" on page 139.

To create an advanced backup policy

1. Make sure that you have already created a basic backup policy.
2. On the Symantec System Recovery 2013 R2 Management Solution **Manage** tab, in the left pane, click **Backup Policies**.
3. In the left pane, click the folder **Backup Policies**.
4. In the middle pane, select the name of a backup policy.
5. Click **Edit** on the toolbar.
6. In the displayed panel, click **Advanced Options**.

7 On the **Advanced Options** panel, in the **Compression** list, set the compression level for the recovery points.

None	Indicates that compression is not used on the recovery point. You can choose this option if storage space is not an issue. If the recovery point is saved to a busy network drive, high compression may be faster than no compression because less data needs to be written across the network
Standard (recommended)	Lets you use low compression for a 40 percent average data compression ratio on recovery points. This setting is the default.
Medium	Lets you use medium compression for a 45 percent average data compression ratio on recovery points.
High	Lets you use high compression for a 50 percent average data compression ratio on recovery points. This setting is usually the slowest method. When a high compression recovery point is created, CPU usage may be higher than normal. Other processes on the computer may also be slower. To compensate, you can adjust the operation speed of the backup process. Speed adjustments may improve the performance of other resource-intensive applications that you run at the same time.

8 On the **Advanced Options** panel, set the recovery point options, and then click **Apply**.

Active backup policy	Activates the backup policy on the managed client computer. If you deselect this option, the backup policy is still sent to the managed client computer but it is not activated.
Limit the number of recovery point sets (bases) saved for this backup (Recovery point sets only) or **Limit the number of recovery points saved for this backup** (Independent recovery points only)	Specifies the maximum number of recovery points or recovery point sets that are saved for each drive. When this limit is reached, each successive recovery point or set is first created and stored. The oldest, previously created recovery point or set is then deleted (including all associated incrementals, if applicable) from the same storage location. Ensure that you have enough hard disk space to accommodate the number of recovery points or sets you specify, plus one additional recovery point or set. If you run out of hard disk space before the number is reached, the recurring recovery point process cannot complete successfully, and a current recovery point or set is not created
Verify recovery point after creation	Checks whether a recovery point or recovery point set is valid or corrupt immediately following its creation. For steps on how to verify the integrity of a recovery point long after it has been created, refer to the Symantec System Recovery product documentation. When you verify a recovery point, it can approximately double the time that is required to create the recovery point.
Disable SmartSector copying	Speeds up the copying process by copying only hard disk sectors with data. However, in some cases, it may be desirable to copy all sectors in their original layout, whether or not they contain data. If you want to copy both used and unused hard disk sectors, select **Disable SmartSector Copying**. When you select this option, it increases the process time, and usually results in a larger recovery point file size.
Ignore bad sectors during copy	Creates a recovery point even if bad sectors are on the hard drive. Although most drives do not have bad sectors, the potential for problems increases during the lifetime of the hard drive.

Perform full VSS backup

Lets you perform a full backup on the VSS storage and send a request for VSS to review its own transaction log. This option is used for VSS applications, such as Microsoft SQL.

VSS determines what transactions are already committed to the database and then truncates those transactions. Among other things, truncated transaction logs help keep the file size manageable and limits the amount of hard drive space that the file uses.

If you do not select this option, backups still occur on the VSS storage. However, VSS does not automatically truncate the transaction logs following a backup.

Note: This option does not apply to Symantec System Recovery Linux Edition.

Divide into smaller files to simplify archiving

Splits a recovery point into two or more smaller files. This feature is useful if you create or export a recovery point that you want to copy to removable media later for safekeeping. The recovery point is split into smaller, more manageable files. You can then copy the files onto separate, removable media, such as a DVD or CD.

If Symantec System Recovery creates an .sv2i file in addition to the .v2i files, you need to save the .sv2i file on the same media as the first .v2i file.

If you create a recovery point of volumes with thousands of files on a computer that has low memory, splitting the recovery point into smaller segments can help speed the process.

If a recovery point is divided into multiple files, the file names for subsequent files are appended with _S01, _S02, and so forth. For example, if the default file name were Dev-RBrough_C_Drive.v2i, the second file name would be Dev-RBrough_C_Drive_S01.v2i, and so on.

Enable search engine support for Google Desktop	Uses your search engine software to index all of the file names that are contained in each recovery point. By indexing file names, you can then use a search engine of choice to locate the files that you want to retrieve. A search tool such as Google Desktop, may already be installed on their computer to search their recovery points. See *Appendix A: Using a search engine to search recovery points* in the *Symantec System Recovery User's Guide* for information about using Google Desktop to retrieve files. **Note:** This option does not apply to Symantec System Recovery Linux Edition.
Include system and temporary files	Includes the indexing support for the operating system and temporary files when a recovery point is created on the client computer. **Note:** This option does not apply to Symantec System Recovery Linux Edition.

9 If appropriate, click **Command file settings**, set the options you want, and then click **Apply**.

Use command file package to deliver command files to the local machine	Indicates if you intend to deploy the Symantec System Recovery command file package that is stored on the Notification Server computer. See "Deploying the command files package to client computers for use during a backup" on page 115. When you deselect this option, you can specify a folder on a network share where the command files are stored for deployment.
Command files folder	Lets you specify the location of command files if you want them to be located in a place other than the default location. You can also specify a location on a per-job basis, as well as specify a location that can be shared among several computers. If you specify a network location, you are prompted for network credentials.
User name	Lets you specify the user name to a command file folder that is located in a network path.
Password	Lets you specify the password to a command file folder that is located in a network path.
Confirm password	Lets you retype the password to a command file folder that is located in a network path.

Run before snapshot creation	Lets you run a command file after a backup has started and before a recovery point is created. You can run a command during this stage to prepare for the recovery point creation process. For example, you can close any open applications that use the drive. **Note:** If you use this option, be sure that the command file has an error recovery mechanism built into it. If the computer has one or more services that must be stopped at this stage (such as stopping a non-VSS aware database or a resource-intensive application), and the command file does not contain any form of error recovery, one or more of the stopped services may not be restarted. An error in the command file can cause the recovery point creation process to stop immediately. No other command files can run.
Run after snapshot creation	Lets you run a command file after a snapshot is created. Running a command during this stage is a safe point for allowing services to resume normal activity on the drive while continuing the recovery point creation. Because the snapshot takes only a few seconds to create, the database is in the backup state momentarily. A minimal number of log files are created.
Run after recovery point creation	Lets you run a command file after the recovery point file is created. You can run a command during this stage to act on the recovery point itself. For example, you can copy it to an offline location.
Timeout (applies to each stage)	Lets you specify the amount of time (in seconds) that a command file is allowed to run.

See "Creating the cold, warm, and hot recovery points" on page 222.

10 In the displayed pane, near the upper-right corner, make sure **On** is selected from the list to enable the software delivery policy.

11 Set the deployment options.

Program name	Identifies the name of the program that you want to run.
Enable Verbose Reporting of Status Events	Sends the plug-in status events to the Notification Server computer.
Applied to	Identifies the resource target to which you want the software task applied.
Package multicast	Lets you uncheck (default) this option if you want to enable package multicast when the Symantec Management Agent's multicast option is disabled.
Schedule	Runs the software task either at a specific start time, or at specified start, end, and duration times. You can specify as many schedules as you need. You can also have any number of schedules active at once.

12 Click **Save changes**.

13 In the middle pane, click **Apply** on the toolbar.

14 Select the targets to which you want the policy to be applied, and then click **OK**.

You can also click **Unapply** on the toolbar in the middle pane to remove the policy from selected targets.

About running command files during a backup

You can use command files (.exe programs with no user interface, .cmd, .bat) and configure them to run during all phases of a backup. You can use command files to integrate with any backup routines that you may run on the client computer or to integrate with the applications that may use a drive on the client computer.

Note: You cannot run the command files that include a graphical user interface, such as notepad.exe. Running such command files causes the backup job to fail.

You can run a command file during any of the following stages during the creation of a recovery point:

- Run before snapshot creation
- Run after snapshot creation
- Run after recovery point creation

Table 4-4 Command Files Settings options

Option	Description
Use command file package to deliver command files to the local machine	Indicates if you intend to deploy the Symantec System Recovery command file package that is stored on the Notification Server computer. See "Deploying the command files package to client computers for use during a backup" on page 115. When you deselect this option, you can specify a folder on a network share where the command files are stored for deployment.
Command files folder	Lets you specify the location of command files if you want them to be located in a place other than the default location. You can also specify a location on a per-job basis, as well as specify a location that can be shared among several computers. If you specify a network location, you are prompted for network credentials.
User name	Lets you specify the user name to a command file folder that is located in a network path.
Password	Lets you specify the password to a command file folder that is located in a network path.
Confirm password	Lets you retype the password to a command file folder that is located in a network path.

Table 4-4 Command Files Settings options *(continued)*

Option	Description
Run before snapshot creation	Lets you run a command file after a backup has started and before a recovery point is created. You can run a command during this stage to prepare for the recovery point creation process. For example, you can close any open applications that use the drive. **Note:** If you use this option, be sure that the command file has an error recovery mechanism built into it. If the computer has one or more services that must be stopped at this stage (such as stopping a non-VSS aware database or a resource-intensive application), and the command file does not contain any form of error recovery, one or more of the stopped services may not be restarted. An error in the command file can cause the recovery point creation process to stop immediately. No other command files can run.
Run after snapshot creation	Lets you run a command file after a snapshot is created. Running a command during this stage is a safe point for allowing services to resume normal activity on the drive while continuing the recovery point creation. Because the snapshot takes only a few seconds to create, the database is in the backup state momentarily. A minimal number of log files are created.
Run after recovery point creation	Lets you run a command file after the recovery point file is created. You can run a command during this stage to act on the recovery point itself. For example, you can copy it to an offline location.
Timeout (applies to each stage)	Lets you specify the amount of time (in seconds) that a command file is allowed to run.

When you use command files (.exe, .cmd, .bat) during a backup, stop and restart non-VSS-aware databases (Windows 2000) that you want to back up with Symantec System Recovery.

See "About backing up non-VSS-aware databases" on page 221.

Any command files that you specify in the **Command File Settings** panel can be deployed using one of two different methods. You can choose to deploy command files as a software delivery policy to a resource target. Or, you can specify a UNC path to a folder on a network share where the command files reside. You need to

specify the user name and password to access the folder location with create, read, and write privileges.

See "Deploying the command files package to client computers for use during a backup" on page 115.

When you deploy the backup policy to client computers, any command files that you specified are also assigned to the backup. Ensure that you have the necessary rights to run each command file.

To use a Visual Basic script file (.vbs) during a backup, you can create a batch file (.bat) that runs the script. For example, you can create a batch file that is called stop.bat that contains the following syntax:

```
Cscript script_filename.vbs
```

Make sure that `Cscript` precedes the Visual Basic script file name.

Warning: The command files that you install and use (such as an .exe) cannot depend on any user interaction or have a visible user interface while they run during a backup. You should test all of the command files you intend to use, outside of Symantec System Recovery, before you use them during a backup.

Symantec System Recovery runs any script using a high privilege account. When the command files are to be located at a place other than the default location, the `Command Files` folder specifies the location of these files.

Note: Symantec recommends that only high privilege users or an administrator have the permission to modify a backup script and access the `Command Files` folder.

When the backup begins, the command file is run during the specified stage. The backup is stopped if an error occurs while a command file is running. Or, the backup is stopped if the command file does not finish in the time you specified (regardless of the stage). In either case, the command file is terminated (if necessary), and the error information is logged and displayed.

See "Creating an advanced backup policy" on page 105.

Deploying the command files package to client computers for use during a backup

When you select the option **Use command file package to deliver command files to the local machine** to create an advanced backup policy that uses command

files, you need to deploy the Symantec System Recovery Command File Delivery package to client computers.

Table 4-5 Command Files Settings options

Option	Description
Use command file package to deliver command files to the local machine	Indicates if you intend to deploy the Symantec System Recovery command file package that is stored on the Notification Server computer. See "Deploying the command files package to client computers for use during a backup" on page 115. When you deselect this option, you can specify a folder on a network share where the command files are stored for deployment.
Command files folder	Lets you specify the location of command files if you want them to be located in a place other than the default location. You can also specify a location on a per-job basis, as well as specify a location that can be shared among several computers. If you specify a network location, you are prompted for network credentials.
User name	Lets you specify the user name to a command file folder that is located in a network path.
Password	Lets you specify the password to a command file folder that is located in a network path.
Confirm password	Lets you retype the password to a command file folder that is located in a network path.
Run before snapshot creation	Lets you run a command file after a backup has started and before a recovery point is created. You can run a command during this stage to prepare for the recovery point creation process. For example, you can close any open applications that use the drive. **Note:** If you use this option, be sure that the command file has an error recovery mechanism built into it. If the computer has one or more services that must be stopped at this stage (such as stopping a non-VSS aware database or a resource-intensive application), and the command file does not contain any form of error recovery, one or more of the stopped services may not be restarted. An error in the command file can cause the recovery point creation process to stop immediately. No other command files can run.

Table 4-5 Command Files Settings options *(continued)*

Option	Description
Run after snapshot creation	Lets you run a command file after a snapshot is created. Running a command during this stage is a safe point for allowing services to resume normal activity on the drive while continuing the recovery point creation. Because the snapshot takes only a few seconds to create, the database is in the backup state momentarily. A minimal number of log files are created.
Run after recovery point creation	Lets you run a command file after the recovery point file is created. You can run a command during this stage to act on the recovery point itself. For example, you can copy it to an offline location.
Timeout (applies to each stage)	Lets you specify the amount of time (in seconds) that a command file is allowed to run.

See "Creating an advanced backup policy" on page 105.

See "About running command files during a backup" on page 112.

To deploy the command files package to client computers for use during a backup

1. On the Symantec System Recovery 2013 R2 Management Solution **Packages and Policies** tab, in the **Install Policies** list in the left pane, under **Command Files**, click **Install Files for all Backup Policies**.
2. In the right pane, near the upper-right corner, click **On** from the list to enable the software delivery policy.

3 Set the deployment options.

Program name	Identifies the name of the program that you want to run.
Enable Verbose Reporting of Status Events	Sends the plug-in status events to the Notification Server computer.
Applied to	Identifies the resource target to which you want the software task applied.
Package multicast	Lets you uncheck (default) this option if you want to enable package multicast when the Symantec Management Agent's multicast option is disabled.
Schedule	Runs the software task either at a specific start time, or at specified start, end, and duration times. You can specify as many schedules as you need. You can also have any number of schedules active at once.

4 Click **Save changes**.

Creating an independent backup task

You can create an independent (one-time) backup task that is scheduled to run only once on the assigned resource target, on the time and date you specify. You can run an independent backup task on Windows- and Linux-based computers that have Symantec System Recovery installed.

You can also create an independent backup task to create an independent recovery point and you can apply a schedule to the task. However, an independent backup task is typically run only once on the resource targets that you have selected using Quick Run.

The independent backup task is only available from the **Monitor Tasks** tab area. You can apply the task to multiple computers at a time. The independent backup task, however, is not available from the **Manage Tasks** tab. Tasks on that tab can only be applied to one computer at a time.

Note: Recovery points are overwritten if you run the independent backup task again on the same location.

See “Creating a basic backup policy” on page 89.

See “Creating an advanced backup policy” on page 105.

See “Deploying a backup policy” on page 127.

To run an independent backup task

1. On the Symantec System Recovery 2013 R2 Management Solution **Monitor Tasks** tab, right-click **Symantec System Recovery Tasks**, and then click **New > Task**.
2. In the **Client Tasks** tree, click **Symantec System Recovery Tasks > Independent Backup**.
3. On the **Create New Task** panel, in the right pane, type a name for the task.
4. Specify the backup options you want.

All drives on the selected computers	Lets you define a backup policy for two or more computers. You should select this option to protect all drives (including hidden or unmounted), that exist on the client computers.
By drive	Lets you select the drives that you want to back up on the selected client computers. If you chose to create a recovery point set, hidden drives are not displayed in the **By Drive** list. Sometimes a selected drive letter is not available for backing up on a particular client computer. The drive has been deleted or the entire hard disk has been removed from the client computer since Symantec System Recovery was installed. In such cases, when the recovery point is created, it does not include the drive.
Destination	Indicates the location where you want to store the recovery points, relative to the managed computers.
Create subfolder for each computer	Lets you create new subfolders on the network share that serves as the backup destination. The new subfolders are given the same names as each client computer that is backed up. For example, suppose you have two client computers. One is named "CathyReadLaptop" and the other is named "MyLaptop". The new subfolders are named \CathyReadLaptop and \MyLaptop.
Offsite Destination 1	Lets you use a primary Offsite Copy destination to make copies of your recovery points to store at a remote location for added backup protection. See “About Offsite Copy” on page 100.

Offsite Destination 2
Lets you use a secondary Offsite Copy destination to make copies of your recovery points to store at a remote location for added backup protection.

See "About Offsite Copy" on page 100.

Enable password protection
Sets a password and enables AES encryption on the recovery point when it is created.

This check box is selected by default.

Password
Lets you specify a password for the backup. Passwords can include standard characters. Passwords cannot include extended characters, or symbols. (Use characters with an ASCII value of 128 or lower.)

You must type this password before you restore a backup or view the contents of the recovery point.

Confirm password
Lets you retype the password for confirmation.

AES encryption
Encrypts recovery point data to add another level of protection to your recovery points.

Note: If the **Use Password** check box is selected, you must define AES encryption.

Choose from the following encryption levels:

- **Standard 128-bit (8+ character password)**
- **Medium 192-bit (16+ character password)**
- **High 256-bit (32+ character password)**

You may have older backup policies created using Symantec System Recovery 2013 Management Solution or Symantec System Recovery 2011 Management Solution, where password protection was not enabled. If you edit the older policies using Symantec System Recovery 2013 R2 Management Solution, the AES Encryption field displays **None**. You need to select one of the options in the list to enable AES encryption.

While higher strengths require longer passwords, the result is greater security for your data.

Create new destination
Lets you define and use a new destination path for the recovery point.

User name
Lets you specify the user name to a destination folder that is located in a network path.

Password
Lets you specify the password to a destination that is located in a network path.

Confirm password	Lets you retype the password for confirmation.
Add destination	Adds the destination to the **Destination** list, and the **Offsite Destination 1** and the **Offsite Destination 2** lists.

5 Click **Advanced**, and then set the options you want on the various tabs.

General tab: Compression options for an independent backup task

None	Indicates that compression is not used on the recovery point. You can choose this option if storage space is not an issue. If the recovery point is saved to a busy network drive, using high compression can be faster than no compression because less data needs to be written across the network
Standard (recommended)	Lets you use low compression for a 40 percent average data compression ratio on recovery points. This is the default setting.
Medium	Lets you use medium compression for a 45 percent average data compression ratio on recovery points.
High	Lets you use high compression for a 50 percent average data compression ratio on recovery points. This setting is usually the slowest method. When a high compression recovery point is created, CPU usage may be higher than normal. Other processes on the computer may also be slower. To compensate, you can adjust the operation speed of the backup process. Speed adjustments may improve the performance of other resource-intensive applications that you run at the same time.

General tab: Advanced recovery point options for an independent backup task

Verify recovery point after creation	Checks whether a recovery point or recovery point set is valid or corrupt immediately following its creation. For steps on how to verify the integrity of a recovery point long after it has been created, refer to the Symantec System Recovery product documentation. When you verify a recovery point, it can approximately double the time that is required to create the recovery point.
Disable SmartSector copying	Speeds up the copying process by copying only hard disk sectors with data. However, in some cases, it may be desirable to copy all sectors in their original layout, whether or not they contain data. If you want to copy both used and unused hard disk sectors, select **Disable SmartSector Copying**. When you select this option, it increases the process time, and usually results in a larger recovery point file size.

Ignore bad sectors during copy

Creates a recovery point even if bad sectors are on the hard drive. Although most drives do not have bad sectors, the potential for problems increases during the lifetime of the hard drive.

Divide into smaller files to simplify archiving

Splits a recovery point into two or more smaller files. This feature is useful if you create or export a recovery point that you want to copy to removable media later for safekeeping. The recovery point is split into smaller, more manageable files. You can then copy the files onto separate, removable media, such as a DVD or CD.

If Symantec System Recovery creates an .sv2i file in addition to the .v2i files, you need to save the .sv2i file on the same media as the first .v2i file.

If you create a recovery point of volumes with thousands of files on a computer that has low memory, splitting the recovery point into smaller segments may help speed the process.

If a recovery point is divided into multiple files, the file names for subsequent files are appended with _S01, _S02, and so forth. For example, if the default file name were Dev-RBrough_C_Drive.v2i, the second file name would be Dev-RBrough_C_Drive_S01.v2i, and so on.

Enable search engine support for Google Desktop

Uses your search engine software to index all of the file names that are contained in each recovery point.

By indexing file names, you can then use a search engine of choice to locate the files that you want to retrieve. A search tool such as Google Desktop, may already be installed on their computer to search their recovery points.

See *Appendix A: Using a search engine to search recovery points* in the *Symantec System Recovery User's Guide* for information about using Google Desktop to retrieve files.

Note: This option does not apply to Symantec System Recovery Linux Edition.

Include system and temporary files

Includes indexing support for the operating system and temporary files when a recovery point is created on the client computer.

Note: This option does not apply to Symantec System Recovery Linux Edition.

Perform full VSS backup	Lets you perform a full backup on the VSS storage and send a request for VSS to review its own transaction log. This option is used for VSS applications, such as Microsoft SQL. VSS determines what transactions are already committed to the database and then truncates those transactions. Among other things, truncated transaction logs help keep the file size manageable and limits the amount of hard drive space that the file uses. If you do not select this option, backups still occur on the VSS storage. However, VSS does not automatically truncate the transaction logs following a backup. **Note:** This option does not apply to Symantec System Recovery Linux Edition.
Description	Lets you type a description that you want associated with the recovery point.

Command File Settings options for an independent backup task

Use command file package to deliver command files to the local machine	Indicates if you intend to deploy the Symantec System Recovery command file package that is stored on the Notification Server computer. See "Deploying the command files package to client computers for use during a backup" on page 115. When you deselect this option, you can specify a folder on a network share where the command files are stored for deployment.
Command files folder	Lets you specify the location of command files if you want them to be located in a place other than the default location. You can also specify a location on a per-job basis, as well as specify a location that can be shared among several computers. If you specify a network location, you are prompted for network credentials.
User name	Lets you specify the user name to a command file folder that is located in a network path.
Password	Lets you specify the password to a command file folder that is located in a network path.
Confirm password	Lets you retype the password to a command file folder that is located in a network path.
Run before snapshot creation	Lets you run a command file after a backup has started and before a recovery point is created. You can run a command during this stage to prepare for the recovery point creation process. For example, you can close any open applications that use the drive. **Note:** If you use this option, be sure that the command file has an error recovery mechanism built into it. If the computer has one or more services that must be stopped at this stage (such as stopping a non-VSS aware database or a resource-intensive application), and the command file does not contain any form of error recovery, one or more of the stopped services may not be restarted. An error in the command file can cause the recovery point creation process to stop immediately. No other command files can run.

Run after snapshot creation	Lets you run a command file after a snapshot is created. Running a command during this stage is a safe point for allowing services to resume normal activity on the drive while continuing the recovery point creation. Because the snapshot takes only a few seconds to create, the database is in the backup state momentarily. A minimal number of log files are created.
Run after recovery point creation	Lets you run a command file after the recovery point file is created. You can run a command during this stage to act on the recovery point itself. For example, you can copy it to an offline location.
Timeout (applies to each stage)	Lets you specify the amount of time (in seconds) that a command file is allowed to run.

Image File Name tab options for an independent backup task

Image file name	Lets you type a name for the image file or you can leave the default name.

6 Click **OK** to return to the **Create New Task** page.

7 Click **OK**.

8 In the **Task Status** field for your selected backup task, do one of the following.

To run the task immediately on a computer	Click **Quick Run**. Select the computer on which you want the task to run, and then click **Run**.
To run the task immediately on multiple computers	Click **New Schedule**, and then do one of the following: Click **Now** and then select the computers for which you want to apply the task. Click **Schedule** at the bottom of the page.
To run the task on multiple computers using a schedule	Click **New Schedule**. Click **Schedule**. Specify the date and time to run the task, and then select the computers for which you want to apply the task. Click **Schedule** at the bottom of the page.

9 Double-click the description in the **Task Status** table to review a detailed summary of the task's progress.

Deploying a backup policy

You can deploy backup policies to the resource targets that have Symantec System Recovery installed.

See "Deploying a backup policy" on page 127.

See "Creating a basic backup policy" on page 89.

See "Creating an advanced backup policy" on page 105.

See "Deploying an existing backup policy as soon as possible" on page 128.

When you deploy backups to resource targets, all of the computers within a given target have the same backup schedule.

Note: Make sure that any backups you deploy do not overlap in time; otherwise an error occurs. Also, suppose you have two backup policies. Each policy has the recovery point set options pointing to the same drives. When the policy is assigned to the client computer, the policies fail with no generated errors.

To deploy a backup policy

1. On the Symantec System Recovery 2013 R2 Management Solution **Manage Tasks** tab, in the **Backup Policies** list in the left pane, click **Backup Policies**.
2. In the middle panel, click a backup policy name.
3. On the table's toolbar, click **Edit**.
4. In the displayed panel near the upper-right corner, click **On** from the list to enable the software delivery policy.
5. Set the deployment options.

Program name	Identifies the name of the program that you want to run.
Enable Verbose Reporting of Status Events	Sends the plug-in status events to the Notification Server computer.
Applied to	Identifies the resource target to which you want the software task applied.
Package multicast	Lets you uncheck (default) this option if you want to enable package multicast when the Symantec Management Agent's multicast option is disabled.
Schedule	Runs the software task either at a specific start time, or at specified start, end, and duration times. You can specify as many schedules as you need. You can also have any number of schedules active at once.

6. Click **Save changes**.

Deploying an existing backup policy as soon as possible

After you have created one or more backup policies, you can use Symantec Management Console to create a Client Task. A manual backup starts immediately if no other tasks or policies are in the queue.

Within the Client Task you can use **Quick Run** to create the following items on demand:

- An independent recovery point.
- A recovery point set.
- An incremental recovery point of the drive's most recent changes.

See "Deploying a backup policy" on page 127.

To deploy an existing backup policy as soon as possible

1. On the Symantec System Recovery 2013 R2 Management Solution **Monitor Tasks** tab, right-click **Symantec System Recovery Tasks**, and then click **New > Task**.
2. In the **Client Tasks** tree, click **Symantec System Recovery Tasks > Run Backup Policy**.
3. On the **Create New Task** page, in the right pane, type a name for the task.
4. Select a backup policy from the list, and then click **OK**.
5. In the **Task Status** field for your selected backup task, do one of the following.

To run the task immediately on a computer	Click **Quick Run**. Select the computer on which you want the task to run, and then click **Run**.
To run the task immediately on multiple computers	Click **New Schedule**, and then do one of the following: Click **Now** and then select the computers for which you want to apply the task. Click **Schedule** at the bottom of the page.
To run the task on multiple computers using a schedule	Click **New Schedule**. Click **Schedule**. Specify the date and time to run the task, and then select the computers for which you want to apply the task. Click **Schedule** at the bottom of the page.

6. Double-click the description in the **Task Status** table to review a detailed summary of the task's progress.

Viewing the status of computers within a backup policy

You can select an existing backup policy to view the progress of any currently running backups, or the backup status of all computers in the resource targets that are assigned to that policy. For example, if one or more drives on a computer are

not included in a backup policy, the status icon changes to reflect the level of backup protection

See "Creating a basic backup policy" on page 89.

See "Creating an advanced backup policy" on page 105.

To view the status of computers within a backup policy

1. On the Symantec System Recovery 2013 R2 Management Solution **Manage Tasks** tab, in the left pane, click **Backup Policies**.
2. In the middle panel, select a backup policy name.
3. On the table's toolbar, click **Edit**.
4. Expand the Backup Status area at the bottom of the page.

Editing a backup policy

You can edit any of the properties and options of a backup policy, except the selected drives that are backed up and the backup type. The resulting backup policy is updated on any computers that are in its assigned resource target.

See "Creating a basic backup policy" on page 89.

See "Creating an advanced backup policy" on page 105.

See "Viewing the status of computers within a backup policy" on page 129.

See "Editing the schedule of a backup policy" on page 139.

To edit a backup policy

1. On the Symantec System Recovery 2013 R2 Management Solution **Manage Tasks** tab, in the left pane, click **Backup Policies**.
2. In the middle panel, select a backup policy name.
3. On the table's toolbar, click **Edit**.
4. In the displayed pane, use the available options and backup properties to make any changes that you want to the policy.

   Backup Policy Schedule tab options for a recovery point set

Schedule	Lets you select the days and a start time for when the backup should run.
Start time (24 hour format)	Lets you customize the start time of the backup .

Sun Mon Tue Wed Thu Fri Sat	Lets you customize the days of the week for the backup to run. The default is to run the backup Monday through Friday.
Run more than once per day	Lets you run the backup more than once a day to protect the data that you edit or change frequently.
Time between backups	Lets you specify the maximum time that should occur between backups.
Number of times	Lets you specify the number of times per day that the backup should run.
Automatically optimize	Lets you select how often optimization should occur for the backup destination to manage the used disk space. You can choose from the following options: ■ **Never** Indicates that no deletion of incremental recovery points is performed. ■ **Every four hours** Indicates that a deletion of incremental recovery points that are four hours old (or older) is performed every four hours. Also, after the first incremental of the day is taken, all incremental files from two days previous are consolidated to a single file. ■ **Every twelve hours** Indicates that a deletion of incremental recovery points that are 12 hours old (or older) is performed every 12 hours. Also, after the first incremental of the day is taken, all incremental files from two days previous are consolidated to a single file.

Distribute strategy randomly across (minutes)

Indicates that the policy is distributed randomly across a specified number of minutes (0-1440) to all the computers that are assigned to the policy. This option applies if you save recovery points to a network destination.

For example, suppose you want to distribute a backup policy in 60 minutes to 120 computers. Each of the 120 computers would randomly choose a time within the 60 minutes, before or after the scheduled start time, to start the backup.

This option helps to run not the policy at the same start time for all computers, which can cause a denial of service condition on the network, the recovery point destination, or both.

Start a new recovery point set

Lets you select how frequently a new recovery point set should be started.

Your options for starting new recovery point set (base) include the following:

- **Weekly**
  Creates a new recovery point set on the first scheduled or manual backup of the week.
- **Monthly**
  Creates a new recovery point set on the first scheduled or manual backup of the month.
- **Quarterly**
  Creates a new recovery point set on the first scheduled or manual backup every three months from the date when you selected this option.
- **Yearly**
  Creates a new recovery point set on the first scheduled or manual backup of the year, once a year, on the date that you selected for this option.
- **Custom**
  Lets you set specific weekly or monthly options for starting a new recovery point set.

Custom	Lets you customize the start time, and the days of the week or month to run the backup. **Note:** If you choose to archive recovery points, consider creating recovery point sets more frequently to keep the size of your recovery point sets smaller.

Backup Policy Triggers tab options for a recovery point set

Any application is installed	Indicates that an incremental recovery point is created at the time users begin to install a software application on their computer.
Specified applications are launched	Indicates that an incremental recovery point is created at the time users run a specified software application on their computer.
Any user logs on to the computer	Indicates that an incremental recovery point is created when users log on to Windows on their computer.
Any user logs off from the computer	Indicates that an incremental recovery point is created at the moment users log off from Windows on their computer (but does not turn off Windows).
Data added to the drive exceeds	Indicates that an incremental recovery point is created when the added data on a drive exceeds an amount (in megabytes) that you specify.

Backup Policy ThreatCon tab options for a recovery point set

Do Not Monitor - Disable	Lets you turn off monitoring of ThreatCon levels for the selected backup policy. **Note:** Level 1 of Symantec ThreatCon indicates that there are no discernable security threats. Because level 1 suggests no threats, it is not an option.
Level 2	Security threats can occur, although no specific threats have been known to occur.
Level 3	An isolated security threat is in progress.

Level 4	Extreme global security threats are in progress.

Backup Policy Schedule options for an independent recovery point

Automatically create a recovery point	Lets you specify a weekly or monthly backup schedule. The scheduling options include the following: ■ **Weekly** Creates a new, independent recovery point on each day of the week that you check, and at the specified time. When you create independent recovery points one or more times per week, large amounts of disk storage space may be required. ■ **Monthly** Creates a new, independent recovery point on each day of the month that you check, and at the specified time. ■ **No Schedule** Saves all of the backup policy settings except a schedule. You can later deploy the backup policy at your convenience by assigning a schedule to the policy. You can also create a single independent recovery point once, with no schedule. See "Creating an independent backup task" on page 118.
Start time (24 hour format)	Lets you customize the start time of the backup .
Days of the week	Lets you customize the days of the week for the backup policy to run.
Days of the month	Lets you customize the days of the month for the backup policy to run.

Distribute strategy randomly across (minutes)

Indicates that the policy is distributed randomly across a specified number of minutes (0-1440) to all the computers that are assigned to the policy. This option applies if you save recovery points to a network destination.

For example, suppose you want to distribute a backup policy in 60 minutes to 120 computers. Each of the 120 computers would randomly choose a time within the 60 minutes, before or after the scheduled start time, to start the backup.

This option helps to not run the policy at the same start time for all computers, which can cause a denial of service condition on the network, the recovery point destination, or both.

Backup Destination options

Enter a folder relative to the managed computers

Indicates the location where you want to store the recovery points, relative to the managed computers.

Browse

Lets you browse to locate a destination that you want to use, relative to the managed computers. You must have create, read, and write privileges at the specified location.

If there is insufficient space at the destination where the recovery point is stored, the policy fails and an error is reported on the Symantec System Recovery 2013 R2 Management Solution **Home** tab.

User name

Lets you specify the user name to a destination folder that is located in a network path.

Password

Lets you specify the password to a destination that is located in a network path.

Confirm password

Lets you retype the password for confirmation.

Advanced recovery point options

Active backup policy

Activates the backup policy on the managed client computer. If you deselect this option, the backup policy is still sent to the managed client computer but it is not activated.

Limit the number of recovery point sets (bases) saved for this backup (Recovery point sets only) or **Limit the number of recovery points saved for this backup** (Independent recovery points only)	Specifies the maximum number of recovery points or recovery point sets that are saved for each drive. When this limit is reached, each successive recovery point or set is first created and stored. The oldest, previously created recovery point or set is then deleted (including all associated incrementals, if applicable) from the same storage location. Ensure that you have enough hard disk space to accommodate the number of recovery points or sets you specify, plus one additional recovery point or set. If you run out of hard disk space before the number is reached, the recurring recovery point process cannot complete successfully, and a current recovery point or set is not created
Verify recovery point after creation	Checks whether a recovery point or recovery point set is valid or corrupt immediately following its creation. For steps on how to verify the integrity of a recovery point long after it has been created, refer to the Symantec System Recovery product documentation. When you verify a recovery point, it can approximately double the time that is required to create the recovery point.
Disable SmartSector copying	Speeds up the copying process by copying only hard disk sectors with data. However, in some cases, it may be desirable to copy all sectors in their original layout, whether or not they contain data. If you want to copy both used and unused hard disk sectors, select **Disable SmartSector Copying**. When you select this option, it increases the process time, and usually results in a larger recovery point file size.
Ignore bad sectors during copy	Creates a recovery point even if bad sectors are on the hard drive. Although most drives do not have bad sectors, the potential for problems increases during the lifetime of the hard drive.

Perform full VSS backup

Lets you perform a full backup on the VSS storage and send a request for VSS to review its own transaction log. This option is used for VSS applications, such as Microsoft SQL.

VSS determines what transactions are already committed to the database and then truncates those transactions. Among other things, truncated transaction logs help keep the file size manageable and limits the amount of hard drive space that the file uses.

If you do not select this option, backups still occur on the VSS storage. However, VSS does not automatically truncate the transaction logs following a backup.

Note: This option does not apply to Symantec System Recovery Linux Edition.

Divide into smaller files to simplify archiving

Splits a recovery point into two or more smaller files. This feature is useful if you create or export a recovery point that you want to copy to removable media later for safekeeping. The recovery point is split into smaller, more manageable files. You can then copy the files onto separate, removable media, such as a DVD or CD.

If Symantec System Recovery creates an .sv2i file in addition to the .v2i files, you need to save the .sv2i file on the same media as the first .v2i file.

If you create a recovery point of volumes with thousands of files on a computer that has low memory, splitting the recovery point into smaller segments can help speed the process.

If a recovery point is divided into multiple files, the file names for subsequent files are appended with _S01, _S02, and so forth. For example, if the default file name were Dev-RBrough_C_Drive.v2i, the second file name would be Dev-RBrough_C_Drive_S01.v2i, and so on.

Enable search engine support for Google Desktop	Uses your search engine software to index all of the file names that are contained in each recovery point. By indexing file names, you can then use a search engine of choice to locate the files that you want to retrieve. A search tool such as Google Desktop, may already be installed on their computer to search their recovery points. See *Appendix A: Using a search engine to search recovery points* in the *Symantec System Recovery User's Guide* for information about using Google Desktop to retrieve files. **Note:** This option does not apply to Symantec System Recovery Linux Edition.
Include system and temporary files	Includes the indexing support for the operating system and temporary files when a recovery point is created on the client computer. **Note:** This option does not apply to Symantec System Recovery Linux Edition.

Command File Settings options

Use command file package to deliver command files to the local machine	Indicates if you intend to deploy the Symantec System Recovery command file package that is stored on the Notification Server computer. See "Deploying the command files package to client computers for use during a backup" on page 115. When you deselect this option, you can specify a folder on a network share where the command files are stored for deployment.
Command files folder	Lets you specify the location of command files if you want them to be located in a place other than the default location. You can also specify a location on a per-job basis, as well as specify a location that can be shared among several computers. If you specify a network location, you are prompted for network credentials.
User name	Lets you specify the user name to a command file folder that is located in a network path.
Password	Lets you specify the password to a command file folder that is located in a network path.

Confirm password	Lets you retype the password to a command file folder that is located in a network path.
Run before snapshot creation	Lets you run a command file after a backup has started and before a recovery point is created. You can run a command during this stage to prepare for the recovery point creation process. For example, you can close any open applications that use the drive. **Note:** If you use this option, be sure that the command file has an error recovery mechanism built into it. If the computer has one or more services that must be stopped at this stage (such as stopping a non-VSS aware database or a resource-intensive application), and the command file does not contain any form of error recovery, one or more of the stopped services may not be restarted. An error in the command file can cause the recovery point creation process to stop immediately. No other command files can run.
Run after snapshot creation	Lets you run a command file after a snapshot is created. Running a command during this stage is a safe point for allowing services to resume normal activity on the drive while continuing the recovery point creation. Because the snapshot takes only a few seconds to create, the database is in the backup state momentarily. A minimal number of log files are created.
Run after recovery point creation	Lets you run a command file after the recovery point file is created. You can run a command during this stage to act on the recovery point itself. For example, you can copy it to an offline location.
Timeout (applies to each stage)	Lets you specify the amount of time (in seconds) that a command file is allowed to run.

5 Click **Save changes**.

Editing the schedule of a backup policy

Depending on the recovery point type that you create, you can edit the schedule settings of a backup.

See "Editing a backup policy" on page 130.

The resulting schedule is updated on the resource target that is assigned to the backup policy.

See "Creating a basic backup policy" on page 89.

To edit the schedule of a backup policy

1. On the Symantec System Recovery 2013 R2 Management Solution **Manage Tasks** tab, in the left pane, click **Backup Policies**.
2. In the middle panel, select a backup policy name.
3. On the table's toolbar, click **Edit**.
4. In the **Schedule Details** field, click the associated hyperlink.
5. Set the backup policy schedule options and properties that you want, and then click **Apply**.

   Backup Policy Schedule tab options for a recovery point set

Schedule	Lets you select the days and a start time for when the backup should run.
Start time (24 hour format)	Lets you customize the start time of the backup .
Sun Mon Tue Wed Thu Fri Sat	Lets you customize the days of the week for the backup to run. The default is to run the backup Monday through Friday.
Run more than once per day	Lets you run the backup more than once a day to protect the data that you edit or change frequently.
Time between backups	Lets you specify the maximum time that should occur between backups.
Number of times	Lets you specify the number of times per day that the backup should run.

Automatically optimize

Lets you select how often optimization should occur for the backup destination to manage the used disk space.

You can choose from the following options:

- **Never**
  Indicates that no deletion of incremental recovery points is performed.
- **Every four hours**
  Indicates that a deletion of incremental recovery points that are four hours old (or older) is performed every four hours. Also, after the first incremental of the day is taken, all incremental files from two days previous are consolidated to a single file.
- **Every twelve hours**
  Indicates that a deletion of incremental recovery points that are 12 hours old (or older) is performed every 12 hours. Also, after the first incremental of the day is taken, all incremental files from two days previous are consolidated to a single file.

Distribute strategy randomly across (minutes)

Indicates that the policy is distributed randomly across a specified number of minutes (0-1440) to all the computers that are assigned to the policy. This option applies if you save recovery points to a network destination.

For example, suppose you want to distribute a backup policy in 60 minutes to 120 computers. Each of the 120 computers would randomly choose a time within the 60 minutes, before or after the scheduled start time, to start the backup.

This option helps to run not the policy at the same start time for all computers, which can cause a denial of service condition on the network, the recovery point destination, or both.

Start a new recovery point set

Lets you select how frequently a new recovery point set should be started.

Your options for starting new recovery point set (base) include the following:

- **Weekly**
  Creates a new recovery point set on the first scheduled or manual backup of the week.
- **Monthly**
  Creates a new recovery point set on the first scheduled or manual backup of the month.
- **Quarterly**
  Creates a new recovery point set on the first scheduled or manual backup every three months from the date when you selected this option.
- **Yearly**
  Creates a new recovery point set on the first scheduled or manual backup of the year, once a year, on the date that you selected for this option.
- **Custom**
  Lets you set specific weekly or monthly options for starting a new recovery point set.

Custom

Lets you customize the start time, and the days of the week or month to run the backup.

Note: If you choose to archive recovery points, consider creating recovery point sets more frequently to keep the size of your recovery point sets smaller.

Backup Policy Triggers tab options for a recovery point set

Any application is installed

Indicates that an incremental recovery point is created at the time users begin to install a software application on their computer.

Specified applications are launched

Indicates that an incremental recovery point is created at the time users run a specified software application on their computer.

Any user logs on to the computer

Indicates that an incremental recovery point is created when users log on to Windows on their computer.

Any user logs off from the computer

Indicates that an incremental recovery point is created at the moment users log off from Windows on their computer (but does not turn off Windows).

Data added to the drive exceeds	Indicates that an incremental recovery point is created when the added data on a drive exceeds an amount (in megabytes) that you specify.

Backup Policy ThreatCon tab options for a recovery point set

Do Not Monitor - Disable	Lets you turn off monitoring of ThreatCon levels for the selected backup policy. **Note:** Level 1 of Symantec ThreatCon indicates that there are no discernable security threats. Because level 1 suggests no threats, it is not an option.
Level 2	Security threats can occur, although no specific threats have been known to occur.
Level 3	An isolated security threat is in progress.
Level 4	Extreme global security threats are in progress.

Backup Policy Schedule options for an independent recovery point

Automatically create a recovery point	Lets you specify a weekly or monthly backup schedule. The scheduling options include the following: ■ **Weekly** Creates a new, independent recovery point on each day of the week that you check, and at the specified time. When you create independent recovery points one or more times per week, large amounts of disk storage space may be required. ■ **Monthly** Creates a new, independent recovery point on each day of the month that you check, and at the specified time. ■ **No Schedule** Saves all of the backup policy settings except a schedule. You can later deploy the backup policy at your convenience by assigning a schedule to the policy. You can also create a single independent recovery point once, with no schedule. See "Creating an independent backup task" on page 118.
Start time (24 hour format)	Lets you customize the start time of the backup.

Days of the week	Lets you customize the days of the week for the backup policy to run.
Days of the month	Lets you customize the days of the month for the backup policy to run.
Distribute strategy randomly across (minutes)	Indicates that the policy is distributed randomly across a specified number of minutes (0-1440) to all the computers that are assigned to the policy. This option applies if you save recovery points to a network destination. For example, suppose you want to distribute a backup policy in 60 minutes to 120 computers. Each of the 120 computers would randomly choose a time within the 60 minutes, before or after the scheduled start time, to start the backup. This option helps to not run the policy at the same start time for all computers, which can cause a denial of service condition on the network, the recovery point destination, or both.

6 Click **Save changes**.

Renaming a backup policy

You can change the name of any backup policy you have created.

See "Editing a backup policy" on page 130.

See "Editing the schedule of a backup policy" on page 139.

To rename a backup policy

1 On the Symantec System Recovery 2013 R2 Management Solution **Manage** **Tasks** tab, in the left pane, click **Backup Policies**.

2 In the middle panel, select a backup policy name.

3 On the table's toolbar, click **Rename**.

4 Type a new backup policy name.

5 Click **OK**.

Disabling a backup policy

You can disable a backup policy using one of two methods. You can remove the backup policy entirely from each client computer in the resource target. Or, you can

deactivate the backup policy on client computers so recovery points are not created. In such cases, you can reactivate the backup later when you want recovery point creation to resume.

To disable a backup policy on resource targets

1. On the Symantec System Recovery 2013 R2 Management Solution **Manage Tasks** tab, in the left pane, click **Backup Policies**.
2. In the middle panel, select a backup policy name.
3. On the toolbar, in the middle panel, click **Edit**.
4. Click **Advanced Options**, uncheck **Active Backup Policy**, and then click **Apply**.

   This deactivates the backup policy on client computers. The policy, however, remains on client computers.
5. Click **Save changes**.

See "Editing a backup policy" on page 130.

See "Editing the schedule of a backup policy" on page 139.

See "Disabling a backup schedule" on page 145.

See "Deleting a backup policy" on page 146.

Disabling a backup schedule

You can temporarily disable the schedule of a backup so that the creation of recovery points is reduced on the resource targets that are assigned to the backup. For example, any event triggers that are associated with the backup can still cause the creation of recovery points despite the schedule being disabled.

To disable a backup schedule

1. On the Symantec System Recovery 2013 R2 Management Solution **Manage Tasks** tab, in the left pane, click **Backup Policies**.
2. In the middle panel, select a backup policy name.
3. On the toolbar, in the middle panel, click **Edit**.
4. In the **Schedule Details** field, click the associated hyperlink.
5. Do one of the following:
   - If the backup type is a recovery point set, in the **Backup Policy Schedule** panel, uncheck **Schedule**, and then click **Apply**.

- If the backup type is an independent recovery point set, select **No schedule** from the drop-down list, and then click **Apply**.

6 Click **Save changes**.

See "Editing a backup policy" on page 130.

See "Editing the schedule of a backup policy" on page 139.

See "Disabling a backup policy" on page 144.

See "Deleting a backup policy" on page 146.

Deleting a backup policy

Deleting a backup policy removes it from the console and all client computers to which you have it assigned. Any recovery points that the backup policy creates are left intact.

To delete a backup policy

1 On the Symantec System Recovery 2013 R2 Management Solution **Manage Tasks** tab, in the left pane, click **Backup Policies**.

2 In the middle panel, select a backup policy name.

3 On the toolbar, in the middle panel, click **Delete**.

4 Click **OK**.

See "Editing a backup policy" on page 130.

See "Editing the schedule of a backup policy" on page 139.

See "Disabling a backup schedule" on page 145.

See "Disabling a backup policy" on page 144.

Viewing Symantec System Recovery details for a client computer

You can view Symantec System Recovery properties and details about a selected computer that you manage.

You can view the following details:

- Backup status, volume status, and history of the computer.
- An event log that identifies errors, information, and warnings.
- The backup type that is created and the backup destination.

- Symantec System Recovery license status.

The following table describes the tab and the details within that tab that you can view.

Table 4-6 Symantec System Recovery details

Tab	Description
Status	

Table 4-6 Symantec System Recovery details *(continued)*

Tab	Description
	Computer status types include the following: ■ **At Risk** A computer that has no recovery points available for the reported drives. A computer at risk can be recovered if the volumes are set to back up. For example, suppose you have a C:\, D:\, and E:\ volume on a client computer, but only a backup of C:\ exists. While Symantec System Recovery 2013 R2 Management Solution shows the client computer at risk, you can still recover the C:\ volume. ■ **Attention Needed** A computer that has a backup policy assigned but it has not been run for a long time. Or, the policy has missed the last scheduled backup (meaning that existing recovery points are probably old). A computer drive that needs attention can be recovered. However, if the recovery points are older, the recovery points do not contain the latest versions of files or folders. ■ **Backed up** A computer that has made a recovery point of all drives (set to report full status) in the last 30 days. And, the computers have not missed the last scheduled backup. Computers are considered backed up without having an assigned backup policy as long as one or more recovery points are created within the last 30 days. A backed-up drive can be fully recovered. ■ **Not Reporting** A computer that is either not connected to the network, is unplugged, or the Symantec Management Agent is not installed. ■ **Unknown** The status is not yet calculated, or the computer has an unsupported version of Symantec System Recovery. ■ **Not Installed** A computer does not have the Symantec System Recovery Plug-in installed. See "Creating a basic backup policy" on page 89. License status types include the allowing: ■ **License** The number of computers that have a current license

Table 4-6 Symantec System Recovery details *(continued)*

Tab	Description
	assigned. ■ **Not Licensed** The number of computers on which an expired trial version of Symantec System Recovery is installed or on which no license was activated. ■ **Trial License** The number of computers that have a trial version of Symantec System Recovery installed. The **Status** tab also shows you the Symantec System Recovery version, license model used, and the license expiration date.
Events	Lists the information, errors, or warnings for the selected computer. You can also use the Windows Event Viewer on the computer to view events from the application logs.
Backup History	Lists the backup history of a computer and general status information, such as the recovery point type, size, and destination. You can also view a chronological history of all of the recovery points of selected drives (even if the recovery point has been deleted from the storage location). The picture icon next to each drive letter gives indicates the type of recovery point that is created (a recovery point set, or an independent recovery point).
Volume Status	Lists specific information about the computer's hard drive (like the file system that is used and the storage capacity), the storage location for the last recovery point, and when the last recovery point occurred. In the **Volume Status** window, in the **Last Backup** column, notice that any unprotected drives (that is, any drives that have not yet had a backup policy run on them) are labeled **Never**. Each drive's protection status also appears in the **Status** column.
Client Configuration	Lists the selected computer's Symantec System Recovery client settings. For example, you can view the Symantec System Recovery settings for event logs, FTP configuration, log files, backup performance, SMTP and SNMP notifications, and system tray icon details. See "Configuring a client option policy for computers" on page 213.

Table 4-6 Symantec System Recovery details *(continued)*

Tab	Description
Recovery History	Lists the recovery history of a computer based on the recovery date, the drive that was recovered, and the recovery point that was used. The status of the recovery is also displayed.

To view Symantec System Recovery details for a client computer

1. On the Symantec System Recovery 2013 R2 Management Solution **Manage Tasks** tab, in the left pane, expand the **Computers** area.
2. In the left pane, do one of the following:
   - Click **Select Organizational Views**, and then click a computer group name.
   - In **Computers** tree, click **Computers**.
3. If necessary, in the middle pane, use the **Filter results** bar above the table to refine the list of computers.
4. In the middle pane, in the table, select a computer name, and then click **Details** on the toolbar above the table.
5. Click the tab of the detail that you want to view.

Chapter 5

Managing recovery points

This chapter includes the following topics:

Best practices for creating recovery points

The following table describes the best practices you can take to ensure the successful creation of recovery points.

See "Best practices for managing recovery points" on page 154.

Table 5-1 Best practices for creating recovery points

Best practice	Description
Schedule backups when you know computers are turned on	Computers must be turned on and Windows must be running at the time a backup occurs. If the computer remains off after it is polled six times, the computer is put into a **Needs attention** state. However, if Symantec System Recovery (with a user interface) is installed on the client computer, Symantec System Recovery prompts users to run the missed backup. In the meantime, the backup status of the client computer in Symantec System Recovery 2013 R2 Management Solution console is set at **Needs Attention**.
Where possible, separate the operating system from the business data	This practice helps speed the creation of recovery points and reduce the amount of information that needs to be restored.

Table 5-1 Best practices for creating recovery points *(continued)*

Best practice	Description
Use a network destination or a secondary hard disk on the client computer as the recovery point storage location	You should store recovery points to a network share or to a hard disk on the client computer other than the primary hard disk C. This practice helps ensure that you can recover the system in the event that the client's primary hard disk fails.
Understand how backups are run on computers in different time zones	When you back up computers across time zones, the backup runs on the day and local time where the managed client computer is physically located. For example, suppose a client computer's physical location is two hours ahead of the Symantec System Recovery 2013 R2 Management Solution console time. You create a backup policy to run at 18:00. When the backup policy begins on the client computer it is 18:00. However, the console displays the policy as beginning at 16:00.
Use defined recovery point destinations	Define recovery point destinations separate from backups and computers. This best practice helps you to see how many computers are backed up to a given location. It can also help you to optimize network load balancing during a backup.
Create recovery points often and regularly	Create backup policies with a schedule to ensure the consistent creation of recovery points.
Save recovery points to the proper location	Symantec System Recovery 2013 R2 Management Solution supports saving the recovery points to network locations or to a local hard disk. You should avoid storing recovery points on the Symantec System Recovery 2013 R2 Management Solution computer. As the number or size of recovery points grows, you have less disk space available for regular server use. When you save recovery points to a separate drive, network location, you eliminate this problem.
Configure client options to optimize client computer performance during a backup.	Symantec System Recovery requires significant system resources to run a backup. If remote users are at work on their computers when a backup starts, they might notice that the performance of their computer slows down. If a slow down occurs, you can adjust the speed of a backup to improve client computer performance. See "Configuring a client option policy for computers" on page 213.

Best practices for managing recovery points

The following table describes the best practices you can take for managing recovery points.

See "Best practices for creating recovery points" on page 152.

Table 5-2 Best practices for managing recovery points

Best practice	Description
Maintain duplicate recovery points for safety.	Store recovery points on the network and create CDs, DVDs, or tapes of recovery points for off-site storage in a safe, secure place. Use Symantec Backup Exec for Windows Servers to back up recovery point locations on the network to tape.
Verify that recovery points or recovery point sets are stable and usable.	Where possible, document and test your entire recovery process. Restore recovery points and single files on the original managed client computer where the recovery points were created. Such testing can uncover potential hardware or software problems. Enable the **Verify recovery point after creation** feature when you create a backup policy. See "Creating an advanced backup policy" on page 105.
Manage storage space by deleting old backup data.	Delete incremental recovery points to reduce the number of files you have to maintain. This strategy also uses hard disk space more efficiently.
Review information on the Symantec System Recovery 2013 R2 Management Solution portal page.	Periodically review the portal page and the contents and events in the **Status** tab of a selected backup policy. It ensures stability in the computer system. You should also review log files periodically.
Review the contents of recovery points.	Ensure that essential data is backed up by periodically reviewing the contents of recovery point files with Recovery Point Browser in Symantec System Recovery.

About deleting recovery points

If you no longer want a particular set of recovery points you can delete the set at any time. Deleting recovery point sets is particularly useful if you want to prevent an accumulation of obsolete backup data at the destination. After you delete a

recovery point set, access to files or system recovery from that point in time is no longer available.

See "Deleting a recovery point set" on page 155.

You can also reduce the amount of needed storage space for the recovery point set by deleting multiple incremental recovery points within a set. The base recovery point and the first and last incremental recovery points are required for a restore and cannot be deleted. Deleting incremental recovery points within a set consolidates the data only; it does not delete data.

See "Deleting recovery points within a set" on page 156.

Depending on the number of incremental recovery points that you delete, additional memory may be required to restore or browse a consolidated incremental recovery point. Additionally, when you delete recovery points over the network, network traffic may increase significantly.

Note: Be careful about which recovery points you choose to delete. For example, suppose a user created a new document that was captured in the third recovery point in your recovery points list. The remote user deletes the file accidentally, at which time the fourth recovery point captures the deletion. The user could lose the file permanently if you delete the third recovery point.

See "Creating a basic backup policy" on page 89.

Deleting a recovery point set

If you no longer want a particular recovery point set you can delete it at any time. Deleting recovery point sets is particularly useful if you want to prevent an accumulation of obsolete backup data at the destination.

After you delete a recovery point set, access to files or system recovery from that point in time is no longer available.

See "About deleting recovery points" on page 154.

See "Deleting recovery points within a set" on page 156.

To delete a recovery point set

1. On the Symantec System Recovery 2013 R2 Management Solution **Monitor Tasks** tab, right-click **Symantec System Recovery Tasks**, and then click **New > Task**.
2. In the **Client Tasks** tree, click **Symantec System Recovery Tasks > Delete Recovery Points**.
3. On the **Create New Task** page, in the right pane, type a name for the task.

4 Select the computer whose recovery points you want to delete.

5 Based on the creation date, select the recovery point that you want to delete.

6 Click **OK**.

7 In the **Task Status** field, click **New Schedule**.

8 Do one of the following:

- To run the task as soon as possible, click **Now**, and then click **Schedule**.
- To schedule the task to run at a later date and time, click **Schedule**. Specify the date and time to run the task, and then click **Schedule** at the bottom of the page.

Deleting recovery points within a set

You can delete specific recovery points or incrementals within a set.

If the backup policy includes a password, you may be prompted to type the password when you delete recovery points within a set.

See "About deleting recovery points" on page 154.

See "Deleting a recovery point set" on page 155.

To delete recovery points within a set

1 On the Symantec System Recovery 2013 R2 Management Solution **Monitor Tasks** tab, right-click **Symantec System Recovery Tasks**, and then click **New > Task**.

2 In the **Client Tasks** tree, click **Symantec System Recovery Tasks > Delete Incremental Recovery Points**.

3 On the **Create New Task** page, in the right pane, type a name for the task.

4 Select the computer whose incremental recovery points you want to delete.

5 Type the recovery point password in the associated text box.

6 Select the recovery points you want to delete.

7 Do one of the following:

- To automatically delete all but the first recovery point (the base) and the last recovery point in the set, click **Automatic Consolidation**.
- To manually select which recovery points in the set to delete, click **Manual**, and then select the recovery points you want to delete.
  You cannot select the first recovery point (the base) and the last recovery point to consolidate.

8 Click **OK**.

9 In the **Task Status** field, click **New Schedule**.

10 Do one of the following:

- To run the task as soon as possible, click **Now**, and then click **Schedule**.
- To schedule the task to run at a later date and time, click **Schedule**. Specify the date and time to run the task, and then click **Schedule** at the bottom of the page.

Chapter 6

Managing the conversion of recovery points to virtual disks

This chapter includes the following topics:

About converting recovery points to virtual disks

You can use schedule recovery point conversion of a physical computer to a virtual hard disk. You can create a VMware virtual disk , a Microsoft virtual disk , or a VMware ESX Server.

When you convert recovery points to virtual disks, it has the following benefits:

- Useful if the physical hardware on the client computer fails.
- You avoid losing the services on the physical computer. For example, when you perform a hot swap of a service from a physical to virtual environment.
- Excellent for testing and evaluation purposes.

You can find a list of platforms that support the virtual disks that are created from recovery points in the software compatibility list. The software compatibility list is available at the following URL:

http://entsupport.symantec.com/umi/V-306-17

Note: Be aware that each time the conversion task runs, the new virtual disk file that is created replaces the previous virtual disk file.

See "Configuring a Convert to Virtual by Computer task" on page 159.

See "Configuring a Convert to Virtual by Destination task" on page 165.

See "Configuring a one-time convert to virtual task" on page 170.

Configuring a Convert to Virtual by Computer task

You can create a schedule to convert the most recent recovery points and incremental recovery points of multiple managed computers. You can convert recovery points to VMware virtual disk format or Microsoft virtual disk format. You can also convert recovery points directly to a VMware ESX Server.

When you create a backup policy or an independent backup task, you can optionally assign a password to protect recovery points from unauthorized access. When you convert password-protected recovery points to virtual disks, you must first unlock the recovery points by using the specified password.

To help automate the conversion process, you can specify the existing passwords in the Passwords Store. When you run a convert to virtual task, the clients use the list of passwords to unlock the recovery points at the time of conversion.

See "Adding or removing recovery point passwords" on page 66.

Note: Be aware that each time the task runs, the new virtual disk file that is created replaces the previous virtual disk file.

See "Configuring a Convert to Virtual by Destination task" on page 165.

See "Configuring a one-time convert to virtual task" on page 170.

To configure a Convert to Virtual by Computer task

1. On the Symantec System Recovery 2013 R2 Management Solution **Monitor Tasks** tab, right-click **Symantec System Recovery Tasks**, and then click **New > Task**.
2. In the **Client Tasks** tree, click **Symantec System Recovery Tasks > Convert to Virtual by Computer**.
3. On the **Create New Task** page, in the right pane, type a name for the conversion task.
4. Click the virtual disk type and select the version that you want to create, if necessary.
5. Do one of the following:
   - To configure a conversion task for two or more computers, click **All drives on the selected computers**. This option converts the latest recovery points of all drives that exist on the selected computers, including hidden drive (excludes unmounted drives).
   - To convert recovery points of certain drive letters on the selected computers, click **By drive letter**, and then select the drive letters that you want.

     Sometimes a selected drive letter is not available for recovery point conversion on a particular client computer. The drive has either been deleted or the entire hard disk has been removed from the client computer since Symantec System Recovery was installed. In such cases, when the recovery point is converted, it does not include the drive.
6. Do one of the following based on the virtual disk type you selected earlier:
   - If you selected VMware virtual disk or Microsoft virtual disk as the virtual disk type, select a destination for the virtual disk file.

To use an existing destination for the resulting virtual disk	From the list of predefined locations, select the location where you want to save the virtual disk. See "Creating default recovery point destinations" on page 68.

To define a new destination for the resulting virtual disk	Select **Create new destination**, and then do one of the following and then click **Add Destination**: ■ Type a local folder path. The local folder path you specify is relative to the managed computer. It is not the folder path on the computer where you are running the Symantec System Recovery 2013 R2 Management Solution console. Local folder paths do not get indexed by the Backup Exec Retrieve Indexing Server; only network share paths get indexed. ■ Type a UNC path to a network share. ■ Type the IP address path to a network share. If you typed a path to a network share, specify the user name and password to access the location with create, read, and write privileges.

If there is not enough space at the destination where the virtual disk file is stored, the conversion fails when it runs. An error is also reported in the **Home Page** view.

You should avoid storing virtual disk files on the Symantec System Recovery 2013 R2 Management Solution server. As the number or size of virtual disks grows, you have less disk space available for regular server use. Saving virtual disk files to a separate drive or a network location eliminates this problem.

- If you selected VMware ESX Server as the virtual disk type, select a temporary location for the files.

To use an existing temporary location for the conversion files	From the list of predefined temporary locations, select the path where you want to save the temporary conversion files. See "Creating default recovery point destinations" on page 68.
To define a new temporary location for the conversion files	Click **Create new destination**. Type the name of the server or the server's IP address that you can use as a temporary location for files. If you selected a temporary location for files on a network, type a valid administrator user name that has sufficient rights. Type a valid password.

7 Click **Advanced**.

8 Do one of the following:

If you selected VMware virtual disk or Microsoft virtual disk as the virtual disk type	Go to the next step.
If you selected VMware ESX Server as the virtual disk type	Do the following: ■ On the **ESX Setup** tab, do one of the following: ■ Select a defined ESX Server location, upload location, and import location from the respective list boxes. ■ If there are no locations to choose from, on the **ESX Server Location** tab, set the appropriate options. ■ Select **Remove files from temporary location after conversion** if you want the temporary files to be removed after the virtual disk is created.

ESX Server Location options

ESX Server Name or Address	Specifies the name of the server or the server's IP address. **Note:** The virtual disk files are transferred to an ESX server through a Secure Shell (SSH) and secure file transfer protocol (SFTP). You might need to change the settings on the ESX server. For more information, see your ESX server documentation.
ESX Server credentials	Specifies a valid administrator name that has sufficient rights and a valid password to the server.
Create ESX Server	Lets you add the defined ESX Server whose name or address and credentials you have specified.
Upload Location	Lets you specify the path to the folder where the virtual disk files are written. Use the **Add**, **Remove**, and **Edit** options to configure the upload folder path you want.

Import Location

Specifies the path to the folder where you want to import virtual disk files.

Note: The folder that you select must be different than the upload location folder.

Use the **Add**, **Remove**, and **Edit** options to configure the import folder path you want.

9 On the **Conversion Options** tab, set the options you want.

Create one virtual disk per volume

Creates one virtual disk per converted volume.

If you do not select this option, each drive is matched to its respective hard drive letter assignment during the conversion. Therefore, it results in multiple drives within one virtual disk file.

Run Windows Mini-Setup

Runs Windows Mini-Setup when you restart the computer after recovery.

During recovery a text-based answer file is generated that scripts the answers for a series of dialog boxes. When the Mini-Setup Wizard starts, it looks for this file answer to automate the wizard. For example, the answer file by way of the wizard, can automatically apply network card settings and other hardware and software settings on the computer.

Unlike Windows Welcome, which can take up to 60 minutes or more to set up Windows, Mini-Setup takes about six minutes. Specific information, including accepting the End–User license agreement , and entering the product key , user name, and company name gets automatically applied by Mini-Setup.

Deselect this option if you want any of the following to occur at the time of recovery instead:

- You want to run Windows Welcome instead of Mini-Setup.
- You do not want to change any of the configurable options for which the Mini-Setup Wizard changes for you at the time of recovery. This scenario ensures that the computer is recovered to its original state before recovery.

For more detailed information about Mini-Setup, you can perform a search for "Mini-Setup" on the Microsoft Help & Support Web site

Split virtual disk into multiple 2 GB .vmdk files	Splits the virtual disk file into multiple 2 GB .vmdk files. For example, use this option if your virtual disks are stored on a FAT32 drive. Or, any file system that does not support files larger than 2 GB. Or, if you want to copy the virtual disk files to a DVD but the size is larger than the DVD allows. This option is specific to VMware; it is not available if you selected Microsoft virtual disk as the conversion format.

10 Click **OK** to return to the task page.

11 Click **OK**.

12 In the **Task Status** field, click **New Schedule**, and then set the options you want.

13 Do one of the following:

To run the task one time as soon as possible after the task is saved	Click **Now**.
To run the task at a specific time or multiple times	Click **Schedule**, and then set one of the following schedule options: ■ In the drop-down list, select **At date/time**, and then specify the date and time and how often the schedule repeats. ■ In the drop-down list, select **Shared Schedule**, and then select a shared schedule to use or create a new one to use.

14 In the **Task Status** field, do one of the following:

- To run the task as soon as possible, click **Now**, and then click **Schedule**.
- To schedule the task to run at a later date and time, click **Schedule**. Specify the date and time to run the task, and then click **Schedule** at the bottom of the page.

Double-click the description in the **Task Status** table to review a detailed summary of the task's progress.

Configuring a Convert to Virtual by Destination task

You can schedule the conversion of a computer's most recent recovery points and incremental recovery points to virtual disks. This type of task uses the .sv2i file to reduce the time it takes to convert multiple recovery points. When Symantec System Recovery creates a recovery point, a .sv2i file is saved with it. The .sv2i file contains a list of the most recent recovery points, which includes the original drive location of each recovery point.

You can convert recovery points and incremental recovery points to VMware virtual disk format or Microsoft virtual disk format. You can also convert recovery points directly to a VMware ESX Server.

Note: Be aware that each time the task runs, the new virtual disk file that is created replaces the previous virtual disk file.

See "Configuring a Convert to Virtual by Computer task" on page 159.

See "Configuring a one-time convert to virtual task" on page 170.

To configure a Convert to Virtual by Destination task

1. On the Symantec System Recovery 2013 R2 Management Solution **Monitor Tasks** tab, right-click **Symantec System Recovery Tasks**, and then click **New > Task**.
2. In the **Client Tasks** tree, click **Symantec System Recovery Tasks > Convert to Virtual by Destination**.
3. On the **Create New Task** page, in the right pane, type a name for the conversion task.
4. Select the computer that does the conversion.
5. Click the virtual disk type and select the version that you want to create, if required.
6. In the **Location of recovery points sets to convert** list, select the source location of the recovery points you want to convert.
7. Do one of the following:
   - Click **Convert all recovery point sets** to convert the latest recovery points of all computers at the source location that you selected in the previous step.
   - Click **Convert recovery point sets created by this computer**, and then select a computer from the list.
8. Do one of the following based on the virtual disk type you selected earlier:

- If you selected VMware virtual disk or Microsoft virtual disk as the virtual disk type, select a destination for the virtual disk file.

To use an existing destination for the resulting virtual disk	From the list of predefined locations, select the location where you want to save the virtual disk. See "Creating default recovery point destinations" on page 68.
To define a new destination for the resulting virtual disk	Select **Create new destination**, do one of the following: ■ Type a local folder path. The local folder path you specify is relative to the managed computer. It is not the folder path on the computer where you are running the Symantec System Recovery 2013 R2 Management Solution console. Local folder paths do not get indexed by the Backup Exec Retrieve Indexing Server; only network share paths. ■ Type a UNC path to a network share. ■ Type the IP address path to a network share. If you typed a path to a network share, specify the user name and password to access the location with create, read, and write privileges. Click **Add Destination**.

If there is not enough space at the destination where the virtual disk file is stored, the conversion fails when it runs. An error is also reported in the **Home Page** view.

You should avoid storing virtual disk files on the Symantec System Recovery 2013 R2 Management Solution server. As the number or size of virtual disks grows, you have less disk space available for regular server use. When you save virtual disk files to a separate drive or a network location it eliminates this problem.

- If you selected VMware ESX Server as the virtual disk type, select a temporary location for the files.

To use an existing temporary location for the conversion files	From the list of predefined temporary locations, select the path where you want to save the temporary conversion files. See "Creating default recovery point destinations" on page 68.

To define a new temporary location for the conversion files	Click **Create new destination**. Type the name of the server or the server's IP address that you can use as a temporary location for files. If you selected a temporary location for files on a network, type a valid administrator user name that has sufficient rights. Type a valid password.

9 Click **Advanced**.

10 Do one of the following:

If you selected VMware virtual disk or Microsoft virtual disk as the virtual disk type	Go to the next step.
If you selected VMware ESX Server as the virtual disk type	Do the following: ■ On the **ESX Setup** tab, do one of the following: ■ Select a defined ESX Server location, upload location, and import location from the respective list boxes. ■ If there are no locations to choose from, on the **ESX Server Location** tab, set the appropriate options. ■ Select **Remove files from temporary location after conversion** if you want the temporary files to be removed after the virtual disk is created.

ESX Server Location options

ESX Server Name or Address	Specifies the name of the server or the server's IP address. **Note:** The virtual disk files are transferred to an ESX server through a Secure Shell (SSH) and secure file transfer protocol (SFTP). You might need to change the settings on the ESX server. For more information, see your ESX server documentation.
ESX Server credentials	Specifies a valid administrator name that has sufficient rights and a valid password to the server.
Create ESX Server	Lets you add the defined ESX Server whose name or address and credentials you have specified.

Upload Location	Lets you specify the path to the folder where the virtual disk files are written. Use the **Add**, **Remove**, and **Edit** options to configure the upload folder path you want.
Import Location	Specifies the path to the folder where you want to import virtual disk files. **Note:** The folder that you select must be different than the upload location folder. Use the **Add**, **Remove**, and **Edit** options to configure the import folder path you want.

11 On the **Conversion Options** tab, set the options you want.

Create one virtual disk per volume	Creates one virtual disk per converted volume. If you do not select this option, each drive is matched to its respective hard drive letter assignment during the conversion. Therefore, it results in multiple drives within one virtual disk file.

Run Windows Mini-Setup

Runs Windows Mini-Setup when you restart the computer after recovery.

During recovery a text-based answer file is generated that scripts the answers for a series of dialog boxes. When the Mini-Setup Wizard starts, it looks for this file answer to automate the wizard. For example, the answer file by way of the wizard, can automatically apply network card settings and other hardware and software settings on the computer.

Unlike Windows Welcome, which can take up to 60 minutes or more to set up Windows, Mini-Setup takes about six minutes. Specific information, including accepting the End–User license agreement , and entering the product key , user name, and company name gets automatically applied by Mini-Setup.

Deselect this option if you want any of the following to occur at the time of recovery instead:

- You want to run Windows Welcome instead of Mini-Setup.
- You do not want to change any of the configurable options for which the Mini-Setup Wizard changes for you at the time of recovery. This scenario ensures that the computer is recovered to its original state before recovery.

For more detailed information about Mini-Setup, you can perform a search for "Mini-Setup" on the Microsoft Help & Support Web site

Split virtual disk into multiple 2 GB .vmdk files

Splits the virtual disk file into multiple 2 GB .vmdk files.

For example, use this option if your virtual disks are stored on a FAT32 drive. Or, any file system that does not support files larger than 2 GB. Or, if you want to copy the virtual disk files to a DVD but the size is larger than the DVD allows.

This option is specific to VMware; it is not available if you selected Microsoft virtual disk as the conversion format.

12 Click **OK** to return to the task page.

13 Click **OK**.

14 In the **Task Status** field, click **New Schedule**.

15 Do one of the following:

- To run the task as soon as possible, click **Now**, and then click **Schedule**.
- To schedule the task to run at a later date and time, click **Schedule**. Specify the date and time to run the task, and then click **Schedule** at the bottom of the page.

Configuring a one-time convert to virtual task

You can use Convert to Virtual to create a one-time recovery point conversion to a virtual disk. A one-time conversion is not scheduled. Instead, it runs only once on the computer that you have selected (it runs immediately after you finish the wizard). The selected computer must already have recovery points created before you can use this feature.

See "Configuring a Convert to Virtual by Computer task" on page 159.

See "Configuring a Convert to Virtual by Destination task" on page 165.

To configure a one-time convert to virtual task

1. On the Symantec System Recovery 2013 R2 Management Solution **Monitor Tasks** tab, right-click **Symantec System Recovery Tasks**, and then click **New > Task**.
2. In the **Client Tasks** tree, click **Symantec System Recovery Tasks > Convert to Virtual One Time**.
3. On the **Create New Task** page, in the right pane, type a name for the conversion task.
4. Select the computer that does the conversion.
5. Click the virtual disk type and select the version that you want to create, if necessary.
6. Do one of the following:

To convert the latest recovery points of the computer that you selected in step 4.	Click **Convert the latest recovery points to virtual disks**.
To convert one recovery point of the computer that you selected in step 4.	Do the following: ■ Click **Convert a single recovery point to a virtual disk**. ■ Optionally, click **Display recovery points only from local and network Offsite locations**. This option only applies if you use an Offsite Copy destination within a backup policy or you have configured a dedicated Offsite Copy location. See "About Offsite Copy" on page 100. ■ In the displayed table, select a recovery point that you want you to convert, based on the date it created.

7 Do one of the following based on the virtual disk type you selected earlier:

- If you selected **VMware Virtual Disk** or **Microsoft Virtual Disk** as the virtual disk type, select a destination for the virtual disk file.

To use an existing destination for the resulting virtual disk	From the list of predefined locations, select the location where you want to save the virtual disk. See "Creating default recovery point destinations" on page 68.
To define a new destination for the resulting virtual disk	Select **Create new destination**, do one of the following: ■ Type a local folder path. The local folder path you specify is relative to the managed computer. It is not the folder path on the computer where you are running the Symantec System Recovery 2013 R2 Management Solution console. Local folder paths do not get indexed by the Backup Exec Retrieve Indexing Server; only network share paths. ■ Type a UNC path to a network share. ■ Type the IP address path to a network share. If you typed a path to a network share, specify the user name and password to access the location with create, read, and write privileges. Click **Add Destination**.

If there is not enough space at the destination where the virtual disk file is stored, the conversion fails when it runs. An error is also reported in the **Home Page** view.
You should avoid storing virtual disk files on the Symantec System Recovery 2013 R2 Management Solution server. As the number or size of virtual disks grows, you have less disk space available for regular server use. When you save virtual disk files to a separate drive or a network location it eliminates this problem.

- If you selected VMware ESX Server as the virtual disk type, select a temporary location for the files.

To use an existing temporary location for the conversion files	From the list of predefined temporary locations, select the path where you want to save the temporary conversion files. See "Creating default recovery point destinations" on page 68.

To define a new temporary location for the conversion files	Click **Create new destination**. Type the name of the server or the server's IP address that you can use as a temporary location for files. If you selected a temporary location for files on a network, type a valid administrator user name that has sufficient rights. Type a valid password.

8 Click **Advanced**.

9 Do one of the following:

If you selected VMware virtual disk or Microsoft virtual disk as the virtual disk type	Go to the next step.
If you selected VMware ESX Server as the virtual disk type	Do the following: ■ On the **ESX Setup** tab, do one of the following: ■ Select a defined ESX Server location, upload location, and import location from the respective list boxes. ■ If there are no locations to choose from, on the **ESX Server Location** tab, set the appropriate options. ■ Select **Remove files from temporary location after conversion** if you want the temporary files to be removed after the virtual disk is created.

ESX Server Location options

ESX Server Name or Address	Specifies the name of the server or the server's IP address. **Note:** The virtual disk files are transferred to an ESX server through a Secure Shell (SSH) and secure file transfer protocol (SFTP). You might need to change the settings on the ESX server. For more information, see your ESX server documentation.
ESX Server credentials	Specifies a valid administrator name that has sufficient rights and a valid password to the server.
Create ESX Server	Lets you add the defined ESX Server whose name or address and credentials you have specified.

Upload Location

Lets you specify the path to the folder where the virtual disk files are written.

Use the **Add**, **Remove**, and **Edit** options to configure the upload folder path you want.

Import Location

Specifies the path to the folder where you want to import virtual disk files.

Note: The folder that you select must be different than the upload location folder.

Use the **Add**, **Remove**, and **Edit** options to configure the import folder path you want.

10 On the **Conversion Options** tab, set the options you want.

Create one virtual disk per volume

Creates one virtual disk per converted volume.

If you do not select this option, each drive is matched to its respective hard drive letter assignment during the conversion. Therefore, it results in multiple drives within one virtual disk file.

Run Windows Mini-Setup

Runs Windows Mini-Setup when you restart the computer after recovery.

During recovery a text-based answer file is generated that scripts the answers for a series of dialog boxes. When the Mini-Setup Wizard starts, it looks for this file answer to automate the wizard. For example, the answer file by way of the wizard, can automatically apply network card settings and other hardware and software settings on the computer.

Unlike Windows Welcome, which can take up to 60 minutes or more to set up Windows, Mini-Setup takes about six minutes. Specific information, including accepting the End–User license agreement , and entering the product key , user name, and company name gets automatically applied by Mini-Setup.

Deselect this option if you want any of the following to occur at the time of recovery instead:

- You want to run Windows Welcome instead of Mini-Setup.
- You do not want to change any of the configurable options for which the Mini-Setup Wizard changes for you at the time of recovery. This scenario ensures that the computer is recovered to its original state before recovery.

For more detailed information about Mini-Setup, you can perform a search for "Mini-Setup" on the Microsoft Help & Support Web site

Split virtual disk into multiple 2 GB .vmdk files

Splits the virtual disk file into multiple 2 GB .vmdk files.

For example, use this option if your virtual disks are stored on a FAT32 drive. Or, any file system that does not support files larger than 2 GB. Or, if you want to copy the virtual disk files to a DVD but the size is larger than the DVD allows.

This option is specific to VMware; it is not available if you selected Microsoft virtual disk as the conversion format.

11 Click the **Drives to Include** tab, and then set the options you want.

Drives found in selected recovery point	Lets you select one or more drives within the recovery point that you want to convert.
Create one virtual disk per volume	Creates one virtual disk per converted volume. If you do not select this option, each drive is matched to its respective hard drive letter assignment during the conversion. Therefore, it results in multiple drives within one virtual disk file.
Rename File	Lets you change the file name of the virtual disk. You do not need to add the file extension. The extension is automatically appended to the file name that is based on the virtual disk format you selected. (The virtual file name is based on the physical disk that the drive was a part of.)

12 Click **OK** to return to the task page.

13 Click **OK**.

14 In the **Task Status** field, click **New Schedule**.

15 Do one of the following:

- To run the task as soon as possible, click **Now**, and then click **Schedule**.
- To schedule the task to run at a later date and time, click **Schedule**. Specify the date and time to run the task, and then click **Schedule** at the bottom of the page.

Editing a convert to virtual task

You can edit any of the properties and options of a recovery point conversion task including the task name. You can also edit the schedule portion of an existing conversion task. The resulting edited conversion task is updated on any computers that are assigned to it.

Note: Be aware that each time the task runs, the new virtual disk file that is created replaces the previous virtual disk file.

See “About converting recovery points to virtual disks” on page 158.

To edit a convert to virtual task

1. On the Symantec System Recovery 2013 R2 Management Solution **Monitor Tasks** tab, expand the **Symantec System Recovery Tasks** folder.
2. Do one of the following:
   - In the **Symantec System Recovery Tasks** tree, click a convert to virtual task name.
   - Click the **Symantec System Recovery Tasks** folder, and then in the right pane, double-click the highlighted convert to virtual task name you want to edit.
3. In the right-pane, make any changes that you want to the properties, options, and schedule of the conversion task.
4. Click **Save changes** when you are done.

Deleting a convert to virtual task

You can delete recovery point conversion tasks that you no longer need or use.

Deleting a conversion task does not delete any recovery points or virtual disks from the storage location. Only the conversion task itself is deleted from the console and all client computers to which you have it assigned.

See "About converting recovery points to virtual disks" on page 158.

To delete a convert to virtual task

1. On the Symantec System Recovery 2013 R2 Management Solution **Monitor Tasks** tab, expand the **Symantec System Recovery Tasks** folder.
2. Do one of the following:
   - In the **Symantec System Recovery Tasks** tree, right-click a convert to virtual task name.
   - Click the **Symantec System Recovery Tasks** folder, and then in the right pane, right-click the highlighted convert to virtual task name you want to delete.
3. Click **Delete**.
4. Click **OK** to confirm the deletion.

Chapter 7

Remote recovery of drives and computers

This chapter includes the following topics:

About recovering a drive remotely

You can use the Recover Drive task to remotely recover a selected partition on the computer's hard disk.

For example, suppose a computer loses data on a secondary drive (a drive other than the system drive where the Windows operating system is installed). You can use an existing recovery point of that drive to restore the data.

Additionally, you can use LightsOut Restore to recover an entire primary (or system) drive. Such a recovery possible as long as its file system is intact and the computer still runs. Otherwise, you must visit the local physical computer and manually start it by using Symantec Recovery Disk to recover the drive.

When LightsOut Restore is installed on computers, a customized version of Symantec Recovery Disk is installed directly to the file system on the system partition. When a system recovery is initiated from the console (using the Symantec System Recovery task **Recover Drive**), the computer restarts directly into the Symantec Recovery Environment . It uses the files that are installed on its system partition. The recovery of the system drive occurs, and the results are reported back to the console.

See "Using LightsOut Restore to remotely recover client computers" on page 178.

Note: LightsOut Restore does not work on a multi-boot client computer (starting multiple operating systems from the same partition). It only works on the primary operating system. Also, if the file system becomes corrupt and you are not able to access the boot menu, LightsOut Restore does not work. In such cases, you must start the computer from the Symantec Recovery Disk DVD.

See "Recovering a drive" on page 180.

Using LightsOut Restore to remotely recover client computers

You must deploy the LightsOut Restore installation policy before you can perform a remote recovery using the LightsOut Restore capability.

Table 7-1 Installing LightsOut Restore on client computers:

Step	Description
Step 1	Edit the LightsOut Restore Configuration policy in Symantec System Recovery 2013 R2 Management Solution.
Step 2	Edit the LightsOut Restore install policy.
Step 3	Deploy the LightsOut Restore policy to client computers.

See "Configuring and installing LightsOut Restore 2013 R2 on client computers" on page 50.

Note: To run the LightsOut Restore feature you need a minimum of 1 GB of memory on the client computer.

The LightsOut Restore policy installs a custom version of Symantec Recovery Disk directly to the file system on the system partition of the client computer. It then places a Symantec Recovery Environment boot option in the **Windows boot** menu. Whenever the boot menu option is selected, the computer starts LightsOut Restore (Symantec Recovery Disk). It uses the files that are installed on the system partition.

It also uses the **Windows boot** menu, and hardware devices such as RILO and DRAC. These features combine to let an administrator remotely control a system during the startup process.

After you configure LightsOut Restore and add the boot menu option, you can use a hardware device to remotely connect to the system. After you connect, you can turn on or restart the system into the recovery environment.

Note: If you use Microsoft's BitLocker Drive Encryption to encrypt the data on a drive, be aware that LightsOut Restore does not work on encrypted drives. You must turn off BitLocker and then decrypt the drive before you can use LightsOut Restore on it.

See "Setting up and using LightsOut Restore" on page 179.

Setting up and using LightsOut Restore

LightsOut Restore works only on the primary operating system. It does not work on multiple-boot computers (for example, a computer that starts multiple operating systems from the same partition). LightsOut Restore is accessible only from the boot menu. If the file system becomes corrupt and you cannot access the boot menu, you must start the computer from the Symantec Recovery Disk DVD.

If you use Microsoft's BitLocker Drive Encryption to encrypt the data on a drive, be aware that LightsOut Restore does not work on encrypted drives. You must turn off BitLocker and then decrypt the drive before you can use LightsOut Restore on it.

See "Using LightsOut Restore to remotely recover client computers" on page 178.

Table 7-2 The process for setting up and using LightsOut Restore

Step	Description
Step 1	Ensure that all of your servers can be managed remotely through a hardware device. Such hardware devices include a RILO card or a DRAC card.
Step 2	Install Symantec System Recovery on the client computers that you want to protect, and then define and run backup policies to create recovery points.
Step 3	Install LightsOut Restore directly to the client computer's local file system.
Step 4	Use the RILO or the DRAC device to connect to the remote server so you can recover a file or system from a remote location. Then you can turn on the system or restart it.

Table 7-2 The process for setting up and using LightsOut Restore *(continued)*

Step	Description
Step 5	Open the boot menu as the remote server starts, and then select the name you have given to the recovery environment. The remote server starts Symantec Recovery Disk and the connection through RILO or DRAC is lost.

See "Configuring and installing LightsOut Restore 2013 R2 on client computers" on page 50.

Recovering a drive

To remotely recover a data drive, a current recovery point that includes the drive to be recovered must already exist. When the recovery is finished, the computer is restarted automatically.

In some cases, the remote drive cannot be locked to perform the recovery under Windows. This issue may occur because the drive is in use by a program. In such cases, the Symantec Recovery Environment is started to complete the recovery.

LightsOut Restore must already be installed on the client computer if you intend to recover a system drive. If LightsOut Restore is not installed on the client computer, you cannot save the **Recover Drive** task.

See "Setting up and using LightsOut Restore" on page 179.

Note: Before you proceed, you may want to inform the user of the client computer. The user should close any applications and files that may be running or open on the drive that you want to recover.

Warning: When you recover a drive, all the existing data on the drive is overwritten with the data that is found in the recovery point. Any changes that you made to the data on a drive, after the date of the recovery point you use to recover, are lost. For example, if you created a new word-processing file on the drive after you created the recovery point, the new word-processing file is not recovered.

See "Recovering a remote computer" on page 183.

To configure a remote Recover Drive task from the Monitor Tasks tab

1. Instruct the user of the client computer to close any applications and files that may be running or open on the drive to recover.
2. On the Symantec System Recovery 2013 R2 Management Solution **Monitor Tasks** tab, right-click **Symantec System Recovery Tasks**, and then click **New > Task**.
3. In the **Client Tasks** tree, click **Symantec System Recovery Tasks > Recover Drive**.
4. In the right pane of the **Create New Task** page, type a name for the task.
5. On the drop-down list, select a computer whose drive you want to recover.
6. Do one of the following:
   - Click **View recovery points of the selected managed client computer**.
   - Click **View recovery points of all managed client computers**.
7. Optionally, click **Display recovery points from local and network offsite locations**.

   This option only applies if you use an Offsite Copy destination within a backup policy or you have configured a dedicated Offsite Copy location.

   See "About Offsite Copy" on page 100.
8. Select a recovery point that you want to restore.
9. If the recovery point is password-protected, enter the correct password in the text field.
10. Click **Advanced**.
11. On the **Select Destination** tab, select the drive that you want to restore.

    If the drive does not have enough space available to restore a recovery point, select multiple, contiguous destinations on the same hard disk.
12. On the **Options** tab, set the restore options.

Verify recovery point before restore	Determines whether a recovery point is valid or corrupt before it is restored. If the recovery point is corrupt, the recovery process is discontinued. This option significantly increases the time that is required for the recovery to complete. However, it ensures that the recovery point being restored is valid.
Check for file system errors	Checks the recovered drive for errors after the recovery point is restored.

Resize restored drive	Expands the drive to occupy the target drive's unallocated space.
Set drive active (for booting OS)	Makes the recovered drive the active partition (the drive the client computer starts from). Only one drive can be active at a time. If you recover a secondary drive, do not check this option. (A secondary drive is a drive other than the one where the Windows operating system is installed.)
Restore original disk signature	Restores the original, physical disk signature of the hard drive. Disk signatures are included in Windows Server 2003/Advanced Server/NT Server 4.0 Enterprise Edition (SP3 and later). Disk signatures are required to use the hard drive. Select this option if either of the following situations are true: ■ A computer's drive letters are atypical (for example, assigned letters other than C, D, E, and so forth). ■ You restore a recovery point to a blank hard drive.
Partition type	Includes the following options: ■ Primary partition Because hard disks are limited to four primary partitions, select this type if the drive has four or fewer partitions. ■ Logical partition Select this type if you need more than four partitions. You can have up to three primary partitions, plus any number of logical partitions, up to the maximum size of the hard disk.
Drive letter	Assigns a drive letter to the partition.

13 Click **OK** to return to the **Create New Task** page.

14 Click **OK**.

15 In the **Task Status** field, do one of the following:

- To run the task as soon as possible, click **Now**, and then click **Schedule**.
- To schedule the task to run at a later date and time, click **Schedule**. Specify the date and time to run the task, and then click **Schedule** at the bottom of the page.

Double-click the description in the **Task Status** table to review a detailed summary of the task's progress.

Recovering a remote computer

You can use a **Recover Computer** task to restore one, multiple, or all drives on a selected computer. The recovery is based on the recovery point that you have selected.

See "About recovering a drive remotely" on page 177.

See "Performing an express recovery" on page 185.

See "Recovering a computer locally" on page 193.

To configure a remote Recover Computer task

1. Instruct the user of the client computer to close any applications and files that may be running or open on the drive to recover.
2. On the Symantec System Recovery 2013 R2 Management Solution **Monitor Tasks** tab, right-click **Symantec System Recovery Tasks**, and then click **New > Task**.
3. In the **Client Tasks** tree, click **Symantec System Recovery Tasks > Recover Computer**.
4. In the right pane of the **Create New Task** page, type a name for the task.
5. On the drop-down list, select a computer whose drives you want to recover.
6. Do one of the following:
   - Click **View recovery points of the selected managed client computer**.
   - Click **View recovery points of all managed client computers**.
7. Optionally, click **Display recovery points from local and network Offsite locations**.

   This option only applies if you use an Offsite Copy destination within a backup policy or you have configured a dedicated Offsite Copy location.

   See "About Offsite Copy" on page 100.
8. Select a recovery point that you want to recover.

   Recovery points that are stored on the local hard drive of a computer are accessed only by that computer.
9. If the recovery point is password-protected, enter the correct password in the text field.
10. Click **Advanced**.

11 On the **Select Destination** tab, select the drive that you want to restore.

If the drive does not have enough space available to restore a recovery point, select multiple, contiguous destinations on the same hard disk.

12 On the **Options** tab, set the restore options.

Verify recovery point before restore	Determines whether a recovery point is valid or corrupt before it is restored. If the recovery point is corrupt, the recovery process is discontinued. This option significantly increases the time that is required for the recovery to complete. However, it ensures that the recovery point being restored is valid.
Check for file system errors	Checks the recovered drive for errors after the recovery point is restored.
Resize restored drive	Expands the drive to occupy the target drive's unallocated space.
Set drive active (for booting OS)	Makes the recovered drive the active partition (the drive the client computer starts from). Only one drive can be active at a time. If you recover a secondary drive, do not check this option. (A secondary drive is a drive other than the one where the Windows operating system is installed.)
Restore original disk signature	Restores the original, physical disk signature of the hard drive. Disk signatures are included in Windows Server 2003/Advanced Server/NT Server 4.0 Enterprise Edition (SP3 and later). Disk signatures are required to use the hard drive. Select this option if either of the following situations are true: ■ A computer's drive letters are atypical (for example, assigned letters other than C, D, E, and so forth). ■ You restore a recovery point to a blank hard drive.

Partition type	Includes the following options: ■ Primary partition Because hard disks are limited to four primary partitions, select this type if the drive has four or fewer partitions. ■ Logical partition Select this type if you need more than four partitions. You can have up to three primary partitions, plus any number of logical partitions, up to the maximum size of the hard disk.
Drive letter	Assigns a drive letter to the partition.

13 Click **OK** to return to the **Create New Task** page.

14 Click **OK**.

15 In the **Task Status** field, do one of the following:

- To run the task as soon as possible, click **Now**, and then click **Schedule**.
- To schedule the task to run at a later date and time, click **Schedule**. Specify the date and time to run the task, and then click **Schedule** at the bottom of the page.

Double-click the description in the Task Status table to review a detailed summary of the task's progress.

Performing an express recovery

You can use an **Express Recovery** task to restore recovery points from a computer to a set of destination computers.

The express recovery task is only available from the **Monitor Tasks** tab area. You can apply the task to multiple computers at a time. The express recovery task, however, is not available from the **Manage Tasks** tab. Tasks on that tab can only be applied to one computer at a time.

See "Recovering a remote computer" on page 183.

To configure a remote Express Recovery task

1 On the Symantec System Recovery 2013 R2 Management Solution **Monitor Tasks** tab, right-click **Symantec System Recovery Tasks**, and then click **New > Task**.

2 In the **Client Tasks** tree, click **Symantec System Recovery Tasks > Express Recovery**.

3 In the right pane of the **Create New Task** page, type a name for the task.

4 Set the express recovery settings that you want.

Verify recovery point before recovery	Lets you ensure that the selected recovery point is stable and usable. When you verify a recovery point, it can approximately double the time that is required to restore the recovery point.
Check for file system errors	Lets you check the recovered drive for errors after the recovery point is restored.
Use the computer's latest recovery point	Lets you use the computer's most recent recovery point.
Use the computer's latest recovery point available on or before the specified date	Lets you use a computer's recovery point based on the date it was created. If the recovery point is not available (deleted) at the primary destination, the Offsite Copy destination is checked for the same recovery point. If the recovery point is found, then the express recovery task is performed. Otherwise, the task fails.
Use the selected recovery point	Lets you use the recovery point that you have selected.
Display recovery points from local and network Offsite locations	Lets you display recovery points from an Offsite Copy destination within a backup policy. Or, you have configured a dedicated Offsite Copy location. See "About Offsite Copy" on page 100. Select the recovery point that you want to restore. If the recovery point is password-protected, enter the correct password in the field.

5 Click **OK**.

6 Do one of the following:

To run the task one time as soon as possible after the task is saved	Click **Now**.

To run the task at a specific time or multiple times	Click **Schedule**, and then set one of the following schedule options: ■ In the list, select **At date/time**, and then specify the date and time and how often the schedule repeats. ■ In the drop-down list, select **Shared Schedule**, and then select a shared schedule to use or create a new one to use.

7 Do one or more of the following:

- In the **Quick add** drop-down list, select a computer to add to the list of computers to which the schedule applies.
- Click **Add** to add the computers to which the schedule applies.
  You can select computers individually and by target.
  When you select computers by target, it usually requires less maintenance than by individual computer. If the computers to which you want a schedule to apply are in a target, there is no need to change the schedule. The target membership changes. You get the most flexibility when you add computers individually. You can add any computer, regardless of how your targets are organized. In many situations, you can use a combination of targets and individual computers.

8 Click **Schedule** at the bottom of the page.

9 Double-click the description in the Task Status table to review a detailed summary of the task's progress.

Chapter 8

Local recovery of files, folders, drives, and computers

This chapter includes the following topics:

About recovering lost data locally

Symantec System Recovery can restore lost files, folders, or entire drives by using recovery points or file and folder backup data.

You must have either a recovery point or file and folder backup data to recover lost files and folders. You must have a recovery point to recover an entire drive. To recover recent changes to a lost file or folder you must make sure the recovery point is current. In other words, the backup must be at least as current as the changes that were made to the lost data.

If you cannot start Windows, you may need to recover the system drive. The system drive is the drive in which Windows is installed (typically C:). You can use Symantec Recovery Disk to recover the system drive.

Note: A backup or restore of files and folders is only possible if it is set up in Symantec System Recovery on the client computer. If you installed Symantec System Recovery without a user interface, on client computers, file and folder backup is not possible.

If you cannot find the files that you want to restore by browsing a recovery point, you can use the Symantec System Recovery Explore feature. This feature assigns a drive letter to a recovery point (mounts the recovery point) as if it were a working drive. You can then use the search feature in Windows Explorer to search for the files. You can drag and drop files to restore them.

See "Recovering files and folders locally by using file and folder backup data" on page 189.

See "Recovering files and folders locally by using a recovery point" on page 191.

Recovering files and folders locally by using file and folder backup data

If you defined a backup of files and folders and need to recover files, you can recover them from a recent file and folder backup.

Note: A backup or restore of files and folders is only possible if it is set up in Symantec System Recovery on the client computer. If you installed Symantec System Recovery without a user interface, on client computers, file and folder backup is not possible.

Symantec System Recovery includes a search tool to help you locate the files that you want to recover.

See "About recovering lost data locally" on page 188.

To recover files and folders locally by using file and folder backup data

1. On the client computer, in the Symantec System Recovery **Tasks** page, click **Recover My Files**.
2. In the left pane of the **Recover My Files** window, select **File and Folder**.
3. Do one of the following:
   - In the **Find files to recover** field, type the whole name or partial name of a file or folder that you want to restore, and then click **Search**.
     For example, type **recipe**. Such a search returns any file or folder that includes the word recipe in its name. For example, My Private Recipes.doc, Chocolate Chip Cookie Recipes.xls, Recipes for Success.mp3, and so forth.
   - Click **Advanced Search**, type your search criteria, and then click **Search**.
     To return to the standard search text box, click **Basic search**.
4. In the search results list box, select the files that you want to restore.
5. Click **Recover Files**.
6. In the **Recover My Files** dialog box, do one of the following:

To restore the files to the same folder where they existed when they were backed up	Click **Original folders**. If you want to replace the original files, check **Overwrite existing files**. If you do not check this option, a number is added to the file name. The original file is untouched. The **Overwrite existing files** option replaces the files of the same name that are stored at that location with the files that you want to restore.
To restore the files to a **Recovered Files** folder on the Windows desktop	Click **Recovered Files folder on the desktop**. Symantec System Recovery creates a new folder that is called **Recovered Files** which is created on the Windows desktop of the client computer.
To restore the files to a particular folder path	Click **Alternate folder**, and then type the path to the location in which you want to restore the files.

7. Click **Recover**.

8 If you are prompted to replace the existing file, click **Yes**. You should click **Yes** only if you are certain that the selected file is the one you want to recover.

9 Click **OK**.

Recovering files and folders locally by using a recovery point

You can also restore files or folders using recovery points, provided you have defined and run a drive-based backup.

Note: A backup or restore of files and folders is only possible if it is set up in Symantec System Recovery on the client computer. If you installed Symantec System Recovery without a user interface, on client computers, file and folder backup is not possible.

See "About recovering lost data locally" on page 188.

To recover files and folders locally by using a recovery point

1 On the client computer, in the Symantec System Recovery **Tasks** page, click **Recover My Files**.

2 In the left pane of the **Recover My Files** window, select **Recovery Point**.

3 If you want to use a different recovery point than the one selected for you in the **Recovery Point** box, click **Change**.

Note: If Symantec System Recovery cannot locate any recovery points, the **Select Recovery Point** dialog box opens automatically.

---

4 In the **Select Recovery Point** dialog box, set the **View by** option.

Date	Displays all of the discovered recovery points in the order in which they were created. If no recovery points were discovered, the table is empty. You should choose one of the remaining View by options.
File name	Lets you browse to another location. For example, an external (USB) drive, removable media, or a network location (with proper network credentials) to select a recovery point (.v2i).
System	Displays a list of all of the drives on the computer and shows any associated recovery points. You can also select a system index file (.sv2i) to display each recovery point that you want to recover.

5 In the **Find files to recover** box, type the whole name or partial name of a file or folder that you want to restore, and then click **Search**.

For example, type **recipe** to return any file or folder that includes the word recipe in its name, such as My Recipes.doc, Recipes.xls, Recipe poetry.mp3, and so forth.

6 In the table that lists the files, select the files that you want to restore.

7 Click **Recover Files** on the toolbar .

8 In the **Recover My Files** dialog box, do one of the following:

To restore the files to the same folder where they existed when they were backed up	Click **Original folders**. If you want to replace the original files, check **Overwrite existing files**. If you do not check this option, a number is added to the file name. The original file is untouched. **Note:** The **Overwrite existing files** option replaces files of the same name at that location, with the files that you want to restore.
To restore the files to a **Recovered Files** folder on the Windows desktop	Click **Recovered Files folder on the desktop**. Symantec System Recovery creates a new folder that is called **Recovered Files** which is created on the Windows desktop of the client computer.
To restore the files to a particular folder path	Click **Alternate folder**, and then type the path to the location in which you want to restore the files.

9 Click **Recover**.

10 If you are certain that the file you want to recover is the correct one, click **Yes**.

11 Click **OK**.

Recovering a computer locally

If Windows fails to start or does not run normally, you can recover the computer using the Symantec Recovery Disk and an available recovery point.

Note: If you can start Windows and the drive that you want to restore is a secondary drive, you can restore the drive within Windows. A secondary drive is any drive other than the system drive, (or the drive where your operating system is installed).

The Symantec Recovery Disk lets you run a recovery environment that provides temporary access to Symantec System Recovery's recovery features. For example, you can access the **Recover My Computer** Wizard to restart the computer into its previous, usable state.

Note: If you purchased Symantec System Recovery from a computer manufacturer, some features in the recovery environment might not be available. For example, if the manufacturer installed the recovery environment on the computer's hard disk. The manufacturer might also assign a keyboard key for the purpose of starting the recovery environment.

When you restart the computer, watch for instructions on the computer monitor, or refer to the manufacturer's instructions.

Table 8-1 Process for recovering a computer locally

Order	Action
Step 1	Set up the computer so that it can start from the Symantec Recovery Disk DVD. See "Configuring a computer locally to start from a CD/DVD" on page 195.
Step 2	Start the client computer using the Symantec Recovery Disk. See "Starting a computer locally by using Symantec Recovery Disk" on page 194.
Step 3	Scan the computer's hard disk to check for errors before you perform a recovery. See "Checking a hard disk for errors" on page 196.
Step 4	Recover the computer locally using Symantec Recovery Disk. See "About using Restore Anyware to recover locally to a computer with different hardware" on page 203. See "Recovering a computer locally by using Symantec Recovery Disk" on page 197.

Starting a computer locally by using Symantec Recovery Disk

Symantec Recovery Disk lets you start a computer that can no longer run the Windows operating system. When you start a computer using the Symantec Recovery Disk DVD, a simplified version of Windows that runs a recovery environment is started. In the recovery environment, you can access the recovery features of Symantec System Recovery.

The recovery environment requires a minimum of 1.5 GB of RAM to run. If a computer's video card is configured to share the computer's RAM, you might need more than 1.5 GB of RAM.

To start a computer locally by using Symantec Recovery Disk

1. If you store recovery points on a USB device, attach the device now (for example, an external hard drive).

   As a best practice, you should attach the device before you restart the computer using the Symantec Recovery Disk DVD.

2. On the client computer, insert the Symantec System Recovery DVD into its media drive.

   If a computer manufacturer installed Symantec System Recovery, the recovery environment already could be installed on the computer's hard drive. Either watch the computer monitor after the computer restarts for on-screen instructions, or refer to the manufacturer's documentation.

3. Restart the computer.

   If you cannot start the computer from the DVD, you might need to change the startup settings on the computer.

   See "Configuring a computer locally to start from a CD/DVD" on page 195.

4. As soon as you see the prompt "Press any key to boot from CD/DVD", press a key to start the recovery environment.

   Note: You must watch for this prompt. It can come and go quickly. If you miss the prompt, you must restart the computer again.

5. Read the license agreement, and then click **Accept**.

   If you decline, you cannot start the recovery environment, and the computer restarts.

Configuring a computer locally to start from a CD/DVD

To run Symantec Recovery Disk, you must be able to start the computer using a CD/DVD.

See "Starting a computer locally by using Symantec Recovery Disk" on page 194.

To configure a computer locally to start from a CD/DVD

1. Turn on the client computer.
2. As the computer starts, watch the bottom of the screen for a prompt that tells you how to access the BIOS setup.

   Generally, you need to press the Delete key or a function key to start a computer's BIOS program.
3. In the **BIOS setup** window, select **Boot Sequence**, and then press **Enter**.
4. Follow the on-screen instructions to make the CD or DVD device be the first startup device in the list.
5. Put the Symantec Recovery Disk DVD into the DVD drive, and then restart the computer.
6. Save the changes, and then exit the BIOS setup to restart the computer with the new settings.
7. Press any key to start the recovery environment (Symantec Recovery Disk).

   When you start a computer using the Symantec Recovery Disk DVD, you are prompted to “Press any key to boot from CD or DVD”. If you do not press a key within five seconds, the computer attempts to start from the next device that is listed in the BIOS.

Note: Watch carefully as the computer starts. If you miss the prompt, you must restart the computer again.

Checking a hard disk for errors

Before you start the recovery process, you should scan the hard disk to check it for corrupted data or surface damage.

To check a hard disk for errors

1. In the **Analyze** panel, click **Check Hard Disks for Errors**.
2. Select the drive that you want to check.

3 Set the check hard disk error options.

Automatically fix file system errors	Fixes the errors on the selected disk. When this option is not selected, errors are displayed but are not fixed.
Find and correct bad sectors	Locates the bad sectors and recovers readable information.

4 Click **Start**.

Recovering a computer locally by using Symantec Recovery Disk

You can restore a computer within the recovery environment. If you have a recovery point for the hard drives that you want to recover, you can fully recover the computer.

If you intend to use the Restore Anyware feature, you must save the recovery point file to a location that you can access. During a recovery with the Restore Anyware option enabled, you might be prompted to supply disk drivers, service packs, hot fixes, and so forth. You should have your Windows media CD available.

See "About using Restore Anyware to recover locally to a computer with different hardware" on page 203.

For more information about getting Restore Anyware drivers, go to the Symantec Knowledge Base at the following URL:

http://entsupport.symantec.com/umi/V-269-15

Warning: Before you restore a computer through Restore Anyware, test your access to the recovery points in the recovery environment. You should ensure that you have access to SAN volumes and that you can connect to the network.

See "Recovering a remote computer" on page 183.

See "Starting a computer locally by using Symantec Recovery Disk" on page 194.

To recover a computer locally by using Symantec Recovery Disk

1. Start the managed client computer by using the Symantec Recovery Disk DVD.
2. On the **Home** panel of Symantec System Recovery Disk, click **Recover My Computer**.

   If your recovery points are stored on media and you only have one media drive, you can eject the Symantec System Recovery Disk DVD now. Insert the CD or DVD that contains your recovery points.
3. On the **Welcome** page of the wizard, click **Next**.

4 On the **Select a Recovery Point to Restore** panel, select a recovery point to restore, and then click **Next**.

Select a Recovery Point to Restore options when you view recovery points by Date

View by - Date	Displays all of the discovered recovery points in the order in which they were created. If no recovery points were discovered, the table is empty. In such cases, you can search all local drives on the computer or browse to find a recovery point.
Select source folder	Lets you view a list of all available recovery points that may exist on your computer's local drives or on a specific drive.
Map a network drive	Lets you specify a shared network folder path and assign it a drive letter. You can then browse the folder location for the recovery point file you want.
Browse	Lets you locate a recovery point on a local drive or a network folder.
Select a recovery point	Lets you select the recovery point to restore.
Recovery point details	Gives you additional information about the recovery point you want to restore.

Select a Recovery Point to Restore options when you view recovery points by File name

View by - File name	Lets you view recovery points by their file name.
Recovery point folder and file name	Lets you specify a path and a file name of a recovery point.
Map a network drive	Lets you specify a shared network folder path and assign it a drive letter. You can then browse the folder location for the recovery point file you want.
Browse	Lets you locate a recovery point on a local drive or a network folder.
Recovery point details	Gives you additional information about the recovery point you want to restore.

Select a Recovery Point to Restore options when you view recovery points by System

View by - System	Lets you use the current system index file that is located in the recovery point storage location. The system index file displays a list of all of the drives on your computer and any associated recovery points from which you can select. The use of a system index file reduces the time it takes to convert multiple recovery points. When a recovery point is created, a system index file is saved with it. The system index file contains a list of the most recent recovery points, which includes the original drive location of each recovery point.
System index folder and filename	Lets you specify a path and a file name of a system index file that you want to use for recovery.
Map a network drive	Lets you specify a shared network folder path and assign it a drive letter. You can then browse the folder location for the system index file (.sv2i) you want.
Browse	Lets you browse to a path that contains a system index file. For example, you can browse to an external (USB) drive, a network location, or to removable media to select a system index file.

5 On the **Drives to Recover** panel, select each drive that you want to recover and set the options that you want, and then click **Next**.

Select drives to recover	Lets you select the drives that you want to recover.
Add	Lets you add additional drives you want to recover.
Remove	Lets remove selected drives from the list of drives to recover.
Edit	Lets you edit the recovery options for a selected drive.
Verify recovery point before restore	Lets you verify whether a recovery point is valid or corrupt before it is restored. If the recovery point is invalid, the recovery is discontinued. This option can significantly increase the time that is required for the recovery to complete.
Use Restore Anyware to recover to different hardware	Indicates that Restore Anyware is used to restore a recovery point to a computer with hardware different from the computer on which the backup was made. Selected automatically if any of the following are true: If you recover a data drive only to new or to different computer hardware, this option is not selected for you.

When you recover your computer, select the drive on which Windows is installed. On most computer systems, this drive is the C drive. In the recovery environment, the drive letters and labels might not match what appears in Windows. You might need to identify the correct drive based on its label. Or, you can identify the drive by its name, or by browsing the files and folders in the recovery point.

6 Optionally, select a drive that you want to recover, and then click **Edit**.

Select the options that you want to perform during the recovery process, and then click **OK** to return to the **Drives to Recover** panel.

Delete Drive	Deletes a selected drive in the list to make space available to restore your recovery point. When you use this option, the drive is only marked for deletion. The actual deletion of the drive takes place after you click **Finish** in the wizard.
Undo Delete	Returns a deleted drive to the list of drives.

Resize drive after recover (unallocated space only)	Resizes a disk after the recovery point is restored. After you select this option, you can specify the new size in megabytes. The size must be greater than the identified size of the disk that you selected in the list.
Primary partition	Because hard disks are limited to four primary partitions, this option is appropriate if the drive has four or fewer partitions.
Logical partition	This option is appropriate if you need more than four partitions. You can have up to three primary partitions, plus any number of logical partitions, up to the maximum size of your hard disk.
Check for file system errors after recovery	Checks the restored drive for errors after the recovery point is restored.
Set drive active (for booting OS)	Makes the restored drive the active partition (for example, the drive from which the computer starts). You should select this option if you restore the drive on which your operating system is installed.
Restore original disk signature	Restores the original, physical disk signature of the hard drive. Disk signatures are part of all Windows operating systems that Symantec System Recovery 2013 R2 Management Solution supports. Disk signatures are required to use the hard drive. Select this option if either of the following situations are true: ■ Your computer's drive letters are atypical (for example, assigned letters other than C, D, E, and so forth). ■ You restore a recovery point to a new, empty hard disk.

Restore master boot record

Restores the master boot record. The master boot record is contained in the first sector of a physical hard disk. The master boot record consists of a master boot program and a partition table that describes the disk partitions. The master boot program analyzes the partition table of the first hard disk to see which primary partition is active. It then starts the boot program from the boot sector of the active partition.

This option is recommended only for advanced users and is available only if you restore a whole drive in the recovery environment.

Select this option if any of the following situations are true:

- You want to restore a recovery point to a new, empty hard disk.
- You restore a recovery point to the original drive, but the drive's partitions were modified since the recovery point was created.
- You suspect that a virus or some other problem has corrupted your drive's master boot record.

7 Click **Next** to review the recovery options that you selected.

8 Select **Reboot when finished** if you want the computer to restart automatically after the recovery process finishes.

9 Click **Finish**.

10 Click **Yes** to begin the recovery process.

About using Restore Anyware to recover locally to a computer with different hardware

The Symantec System Recovery Restore Anyware feature lets administrators restore a system drive of a Windows 2000/2003/Vista/7 client computer. You can restore the system drive. This recovery is possible even if the hardware is different from the original computer from which the recovery point was made.

Restore Anyware lets you make the necessary changes for the system to be able to start. Depending on the client computer's configuration, you may need to make additional changes for the computer to run exactly as it did previously.

If you intend to restore to identical (or very similar) hardware, you do not need to select Restore Anyware.

For example, you can use Restore Anyware in the following scenarios:

- The motherboard fails
- You want to upgrade to new hardware from an older computer

This feature is used to recover drives only. The feature cannot be used to recover at a file or a folder level.

Note: You can obtain more information about domain controller support.

See http://entsupport.symantec.com/umi/V-269-16.

Warning: If you have an OEM license from a hardware vendor or a single-user license, you may be prompted to reactivate Windows software. You can reactivate by using your Windows product license key. Be aware that OEM and single-user licenses might have a limited number of activations. Verify that using Restore Anyware does not violate the operating system or application license agreements.

Keep in mind the following when you use Restore Anyware:

- Performing Restore Anyware to hardware that is significantly different might require you to do the following:
  - Add mass storage device drivers.
  - Install hot fixes for the Windows operating system that you restore.
  - Reactivate your Windows operating system when the system restarts.
  - Provide your license key when the system restarts.
  - Provide a local user name and password for the recovery point when the system restarts.
- When you restore a recovery point by using Restore Anyware, you might be prompted for the local administrator name and password. You should have this information ready before you perform the restore. Technical support cannot restore a lost password.
- You cannot use Restore Anyware to restore a single recovery point to multiple computers. The product does not generate a unique SID for every computer.
- If you use Restore Anyware with a computer that uses a static IP address, you must manually reconfigure the computer after the restore is complete.
- Symantec System Recovery supports one NIC on a system. If you have a dual NIC system, you might need to manually configure the additional NICs to perform a restore through Restore Anyware.

See "Recovering a computer locally by using Symantec Recovery Disk" on page 197.

Recovering files and folders locally by using Symantec Recovery Disk

You can use the Symantec Recovery Disk to start a computer and to restore files and folders from within a recovery point.

The recovery environment includes several support utilities that you can run to troubleshoot networking or hardware issues. For example, you can ping a computer, renew IP addresses, or get information about a hard disk partition table.

See "Starting a computer locally by using Symantec Recovery Disk" on page 194.

To recover files and folders locally by using Symantec Recovery Disk

1. Start the client computer by using the Symantec Recovery Disk DVD.
2. Click **Recover**, and then click **Recover My Files**.
3. Do one of the following:
   - If the Symantec Recovery Disk cannot locate any recovery points, you are prompted to locate one. In the **Open** dialog box, navigate to a recovery point, select one, and then click **Open**.
   - If the Symantec Recovery Disk finds recovery points, select a recovery point from the list, and then click **OK**.

   Note: If you have trouble finding the recovery points in a network location, in the **File name** box, type the name of the computer. Then type the share that holds the recovery points. For example, \\computer_name\share_name.

   If you still have problems, try entering the computer's IP address.
4. In the tree view pane of the Recovery Point Browser, double-click the drive that contains the files or folders that you want to restore.
5. In the content pane of the Recovery Point Browser, select the files or folders that you want to restore.

6 Click **Recover Files**.

Where possible, the **Recover Items** dialog box automatically completes the **Restore to this folder** box with the original path from which the files originated.

If the original location does not include a drive letter, you must type the drive letter at the beginning of the path.

Note: While in the recovery environment, drive letters and labels might not match what appears in Windows. You might have to identify the correct drive based on its label, which is the name assigned to it.

---

7 If the original path is unknown or you want to restore the selected files to a different location, click **Browse** to locate the destination.

8 Click **Recover** to restore the files.

9 Click **OK** to finish.

Exploring files and folders locally on a computer by using Symantec Recovery Disk

You can explore the files and folders on a computer from the recovery environment by using the Explore My Computer feature.

This feature uses the Recovery Point Browser and functions similarly to Windows Explorer. You can browse the file structure of any drive that is attached to the computer from the recovery environment.

To explore the computer

- In the **Analyze** pane, click **Explore My Computer**.

About using the networking tools in Symantec Recovery Disk

If you store your recovery points on a network, you need access to the network. This access lets you restore your computer or your files and folders from Symantec System Recovery Disk. The Symantec System Recovery Disk includes a variety of networking tools that you can use to assist you with recovery.

Note: Additional computer memory might be required to recover your computer or files across a network.

See "Starting networking services" on page 207.

See "Mapping a network drive from within Symantec Recovery Disk" on page 207.

See "Configuring network connection settings" on page 208.

Starting networking services

If you need to start networking services, you can do so manually.

To start networking services

- On the **Network** panel, click **Start My Networking Services**.

  To verify the connection to the network, you can map a network drive.

  See "Mapping a network drive from within Symantec Recovery Disk" on page 207.

Mapping a network drive from within Symantec Recovery Disk

If you started the networking services after you started the recovery environment, you must map a network drive. Doing so lets you browse to that drive and select the recovery point that you want to restore.

If there is no DHCP server or the DHCP server is unavailable, you must provide a static IP address and a subnet mask address.

See "Configuring network connection settings" on page 208.

After you provide the static IP address and subnet mask address, you can enter the recovery environment. However, there is no way to resolve computer names. When you run the **Recover My Computer** wizard or the **Recovery Point Browser**, you can only browse the network by using the IP addresses to locate a recovery point. You can map a network drive so that you can locate the recovery points more effectively. Or, you can use the mapped network drive as a destination for recovery points that you create from within the recovery environment.

To map a network drive from within Symantec System Recovery Disk

1. In Symantec System Recovery Disk, on the **Network** panel, click **Map a Network Drive**.
2. Map a network drive by using the UNC path of the computer on which the recovery point is located.

   For example: **\\computer_name\share_name** or **\\IP_address\share_name**

   You can also map a network drive from within the **Recover My Computer** wizard or the **Back Up My Computer** wizard in Symantec System Recovery Disk.

Configuring network connection settings

You can access the Network Configuration window to configure network settings while in the recovery environment.

To configure network connection settings

1. In the recovery environment main window, click **Network**, and then click **Configure Network Connection Settings**.
2. If you are prompted to start networking services, click **Yes**.

Getting a static IP address

You can restore a recovery point that is located on a network drive or share. Sometimes, however, you cannot map a drive or browse to the drive or share on the network to access the recovery point. The lack of an available DHCP service can cause such a failure. In such cases, you can assign a unique static IP address to the computer that is running the recovery environment. You can then map to the network drive or share.

To get a static IP address

1. In the recovery environment main window, click **Network**, and then click **Configure Network Connection Settings**.
2. In the **Network Adapter Configuration** box, click **Use the following IP address**.
3. Specify a unique IP address and subnet mask for the computer that you want to restore.

   Be sure that the subnet mask matches the subnet mask of the network segment.
4. Click **OK**.
5. Click **Close** to return to the recovery environment's main menu.
6. In the **Network** pane, click **Ping a Remote Computer**.
7. Type the address of the computer that you want to ping on the network segment.
8. Click **OK**.

   If you specified a computer name or a computer name and domain as the address method, make note of the IP address that is returned.

   If communication to the storage computer operates as expected, you can use the **Map Network Drive** utility to map a drive to the recovery point location.

Viewing the properties of a recovery point

You can view various properties of a recovery point by using the Recovery Point Browser, which is a component of Symantec System Recovery.

To view the properties of a recovery point

1. In the Recovery Point Browser, in the tree panel, select the recovery point that you want to view.
2. Do one of the following:
   - On the **File** menu, click **Properties**.
   - Right-click the recovery point, and then click **Properties**.

Description	Displays a user-assigned comment that is associated with the recovery point.
Size	Displays the total size (in megabytes) of the recovery point.
Created	Displays the date and time that the recovery point file was created.
Compression	Displays the compression level that is used in the recovery point.
Spanned	Indicates whether the entire recovery point file is spanned over several files.
Password protected	Displays the password protection status of the selected drive.
Encryption	Displays the encryption strength that is used with the recovery point.
Format	Displays the format of the recovery point.
Computer name	Displays the name of the computer on which the recovery point was created.
Restore Anyware	Identifies whether Restore Anyware was enabled for the recovery point, this property is displayed.
Cataloged	If you enabled search engine support for the recovery point, this property is displayed.
Created by	Identifies the application (Symantec System Recovery 2013 R2 Management Solution) that was used to create the recovery point.

Viewing the properties of a drive within a recovery point

You can view various properties of a recovery point by using the Recovery Point Browser.

To view the properties of a drive within a recovery point

1. In the Recovery Point Browser, in the tree panel, double-click the recovery point that contains the drive that you want to view.
2. Select a drive.
3. On the **File** menu, click **Properties**.

Description	Displays a user-assigned comment that is associated with the recovery point.
Original drive letter	Displays the original drive letter that was assigned to the drive.
Cluster size	Displays the cluster size (in bytes) that is used in a FAT, FAT32, or NTFS drive.
File system	Displays the file system type that is used within the drive.
Primary/Logical	Displays the selected drive's drive status as either the primary partition or the logical partition.
Size	Displays the total size (in megabytes) of the drive. This total includes used and unused space.
Used space	Displays the amount of used space (in megabytes) within the drive.
Unused space	Displays the amount of unused space (in megabytes) within the drive.
Contains bad sectors	Identifies whether there are any bad sectors on the drive.

About the Support Utilities on Symantec System Recovery Disk

The recovery environment has several support utilities that Symantec Technical Support might ask you to use to troubleshoot any hardware issues that you encounter.

You might be required to supply the information that these utilities generate if you call Symantec Technical Support for help resolving problems.

Note: You should only use these tools as directed by Symantec Technical Support.

Chapter 9

Monitoring computers and processes

This chapter includes the following topics:

Viewing reports

You can use the **Report Tasks** tab to generate various predefined reports with detailed information about your backup management system.

See "Viewing the status of computers within a backup policy" on page 129.

The following table describes the predefined reports that you can generate.

Table 9-1 Available reports

Report	Description
Backup policies	Displays a detailed overview of all backup policies that are available in Symantec System Recovery 2013 R2 Management Solution.
Backup Status of Managed Computers	Displays the backup status of client computers that Symantec System Recovery 2013 R2 Management Solution manages.
License Policies	Displays all available Symantec System Recovery license policies.
License Status of Managed Computers	Displays the Symantec System Recovery license status on computers.

Table 9-1 Available reports *(continued)*

Report	Description
Managed Computers with Symantec System Recovery	Displays a list of client computers that Symantec System Recovery 2013 R2 Management Solution manages with the Symantec System Recovery plug-in installed.
Managed Computers with Symantec System Recovery Linux Edition	Displays a list of client computers that Symantec System Recovery 2013 R2 Management Solution manages with the Symantec System Recovery Linux Edition plug-in installed.
Managed Computers with Recovery Points	Displays the information about available recovery points. Deleted recovery points are not included in the report.
Managed Computers with Unsupported Symantec System Recovery	Displays the computers that have an installed version of Symantec System Recovery that Symantec System Recovery 2013 R2 Management Solution does not support.
Volume Usage of Managed Computers	Displays a list of managed (and reporting) client computers and detailed information about each partition on its hard disk.

To view reports

1. On the Symantec System Recovery 2013 R2 Management Solution, click the **Report Tasks** tab.
2. In the **Symantec System Recovery** tree in the left pane, click the name of a report.

Configuring a client option policy for computers

You can set a variety of options that affect one computer or entire groups of computers.

To configure a client option policy for computers

1. On the Symantec System Recovery 2013 R2 Management Solution **Manage Tasks** tab, expand the **Configuration Policies** list in the left pane.
2. Do one of the following:

To edit the default client configuration policy	Do the following: ■ In the left pane, select a client configuration policy name. ■ In the right pane, select the name of the default policy in the table. ■ Click **Edit** on the table's toolbar.
To create a new client configuration policy	Do the following: ■ In the left pane, select a client configuration policy name. ■ In the right pane, on the table's toolbar, click **Create**. ■ In the displayed pane, in the text box, type a name for the new policy. ■ Click **Apply**. ■ In the right pane, on the table's toolbar, click **Edit**.

3 Near the upper-right corner of the displayed page, make sure **On** is selected from the list to enable the policy.

4 Based on the client configuration policy you selected, set the configuration options you want.

Event Log Sets the minimum priority level and error message types that are added to the Windows application log regarding Symantec System Recovery on the computer.

FTP Sets the default FTP connection settings if you use FTP as an Offsite Copy destination.

The following options are available:

- **Passive (Recommended)**
  Helps avoid conflicts with security systems. This mode is necessary for some firewalls and routers. When you use passive mode, the FTP client opens the connection to an IP address and port that the FTP server supplies.
- **Active**
  Uses the Active mode when connections or transfer tries fail in Passive mode, or when you receive data socket errors. When an FTP client connects with Active mode, the server opens a connection to an IP address and port that the FTP client supplies.
- **Limit connection attempts to**
  Specifies the number of times Symantec System Recovery on the client computer tries to connect to an FTP server before it gives up. Symantec System Recovery can try a maximum of 100 times.
- **Stop trying to connect after**
  Specifies the number of seconds Symantec System Recovery on the client computer tries to connect to an FTP server before it gives up. You can specify up to 600 seconds (10 minutes).
- **Default port**
  Specifies the port of the FTP server that listens for a connection. You should consult the FTP server administrator to be sure that the port you specify is configured to receive incoming data.

Log File Sets the following log file options:

- **Priority Level**
  Indicates the minimum priority level and error message types that you want logged to a file regarding Symantec System Recovery on the computer.
- **Log file location**
  Specifies the path that you want to use for storing log files.
- **Maximum file size**
  Specifies the maximum file size of the log file. When the maximum file size is reached, the log file is renamed (*.Old). A new log is started and the original file name is used.

Performance Adjusts the operation speed of Symantec System Recovery. This adjustment occurs during the creation of a recovery point by dragging the slider bar to the left or to the right. By reducing the operation speed of Symantec System Recovery, you can improve the performance of other software programs that may be running on the computer. When Symantec System Recovery (with a user interface) is installed, the throttle value that you set in the solution takes precedence. Therefore, any throttle value that a remote user sets is ignored.

If you save recovery points to a network storage location, you can also set a network throttle value. You set the value by specifying the maximum number of kilobytes per second (200-1048576) of recovery point data that is transferred over the network. If your network has limited bandwidth, you can enable network throttling during a recovery point to help reduce network traffic.

SMTP Notification Configures a user to receive SMTP email notification messages.

Lets you choose the minimum priority level and error message types that you want to send regarding Symantec System Recovery on the computer.

You can add the name of the SMTP mail server (for example, smtpserver.domain.com or server1) on which you have a valid account. Symantec System Recovery 2013 R2 Management Solution does not check the server name or the email address for validity.

You can increase the security of the sent email by specifying an authentication level (either Basic or NTLM), and a user name and password. Anonymous authentication does not require a user name and password.

You must have an SMTP-compliant email system, such as a POP3 mail server, to receive notification messages.

Also, suppose you change an existing **SMTP Notification** setting policy to **Off**. Even though the policy is off, it does not prevent resource targets with Symantec System Recovery from sending email notifications to the recipient. To stop email notifications, you must create an exclusive SMTP policy that has no SMTP settings. Select **On** to enable the policy, and then deploy it to the resource targets that you want.

SNMP Notification Receives the SNMP traps from Symantec System Recovery when you install and configure the Windows SNMP system service.

By default, Symantec System Recovery is not enabled to send traps to NMS managers.

Tray Icon Shows or hides the Symantec System Recovery system tray icon on computers.

Hiding the tray icon is useful for the following reasons:

- You want the actions of Symantec System Recovery to remain invisible to the user.
- You do not want to add another icon to the system tray of the computer.
- You want users to avoid having any intervention with Symantec System Recovery on critical computers such as product servers.

Symantec System Recovery and the Symantec System Recovery Plug-in must already be installed on the client computer.

You can choose the level of messages that you want the remote user to see, even if the system tray icon is hidden.

Volume Alert Changes how Symantec System Recovery 2013 R2 Management Solution reports the status of a particular drive on a client computer. For example, suppose drive D contains unimportant data and you have chosen not to include it in a backup job. The backup status reports that the computer is at risk. You can configure Symantec System Recovery 2013 R2 Management Solution to ignore drive D so that it does not calculate the status of drive D. Or, you can specify that only errors, such as missed or failed backups, are included in the status report.

The backup status is reported on each drive on a client computer wherever the drive is listed in the solution . When you customize status reporting for a drive, the status is reflected anywhere that the drive is listed in Symantec System Recovery 2013 R2 Management Solution.

You should first determine the importance of the data on a particular drive before you decide on the level of status reporting to assign it.

You can set the status reporting level that you want to be associated with the drives based on the following criteria:

- **Full Status Reporting**
  Shows the current status of the selected drives where the status is shown. Click this option if the data is critical.
- **Error Only Status Reporting**
  Shows the current status of the selected drives only when errors occur. Click this option if the data is important, but you only want the status to report errors when they occur.
- **No Status Reporting**
  Does not show any status for the selected drive. Click this option if the data is unimportant and the missed or failed backups do not need to be reported.

5 In the **Applied to** field, select a resource target, and then select the filtering rules that you want to be applied to the policy.

6 Click **Save Changes**.

Appendix A

About backing up databases

This appendix includes the following topics:

About backing up VSS-aware databases

Symantec System Recovery 2013 R2 Management Solution can co-exist with Microsoft VSS (Volume Shadow-copy Service) to automate the process of backing up VSS-aware databases such as the following:

- Exchange Server 2007 or later
- SQL Server 2005 or later
- Windows Server 2003-based domain controller or later

Note: Licensing Symantec System Recovery on client computers does not give users any rights to use VSS. VSS must be licensed separately from Microsoft, and users must conform to any license agreement or documentation that accompanies VSS.

See "About backing up non-VSS-aware databases" on page 221.

VSS-aware databases are auto-enabled and cannot be turned off. VSS lets IT administrators create a shadow copy backup of drives on a server. The shadow copy includes all files (including open files).

When a backup policy starts, Symantec System Recovery alerts the VSS that a recovery point is about to be created. VSS then communicates this information to the VSS-aware databases and puts them into a quiesced (sleep) state. (Symantec System Recovery always attempts to communicate with VSS if it is installed on a desktop or server and tries to provide VSS with information to quiesce databases.)

While in this quiesced state, the databases continue to write to transaction logs. Symantec System Recovery takes an instantaneous snapshot that also includes any open files. When a snapshot is complete, VSS is notified, the databases are activated, and the transaction logs continue writing to the database. (To verify that there are no errors and that VSS is running, you should check the Microsoft error logs.)

While the recovery point is created from the snapshot, the databases and the applications return to an active state and continue to write data. This kind of integration means that you can back up business-critical databases at anytime during the day without it affecting productivity.

Additional points for backing up and restoring VSS-aware databases include the following:

- Symantec System Recovery 2013 R2 supports Exchange Server 2007 or later, which implements VSS technology. If the database load is heavy, the VSS request might be ignored.
- Backups should run during the lightest load time.
- Additional backup applications are not needed to run Symantec System Recovery with Exchange databases.
- Make sure that you have installed the latest service packs for your given database.
- Symantec System Recovery prevents the VSS snapshots from occurring during the time the Symantec System Recovery create a recovery point.
- If a full System Restore is done from a recovery point, individual files can be restored from a VSS snapshot. However, the recommended restore process is to use Symantec System Recovery to mount the recovery point file as a virtual drive (using the Recovery Point Browser). Or, if you enabled file indexing when you defined the backup policy, you can use Backup Exec Retrieve to quickly restore the files you need.
- After a full System Restore from a Symantec System Recovery recovery point, a VSS snapshot that was taken before the date and time of the Symantec System Recovery snapshot cannot be used to restore the entire system.

Warning: Database corruption may occur if the computer is low on hard disk space when you rebuild a database at the same time you run a backup. To avoid database corruption, you should quiesce the database before backing it up. You should also not rebuild or restore the database at the same time that you back it up. To avoid possible conflict Symantec System Recovery does not let you take VSS snapshots and Symantec System Recovery snapshots at the same time.

About backing up non-VSS-aware databases

With Symantec System Recovery, you can create cold recovery points manually, warm recovery points automatically, or hot recovery points of non-VSS-aware databases.

The Symantec System Recovery 2013 R2 Management Solution server includes a database, which should back up the server on a regular basis. You must stop the Altiris Notification Server services before backing up so you do not lose or corrupt data. To stop the server, you can use Symantec System Recovery through Symantec System Recovery 2013 R2 Management Solution to create a cold recovery point automatically.

A manual cold (or offline) recovery point ensures that all database transactions are committed to the hard disk. You can then use Symantec System Recovery to create the recovery point, and then restart the database.

See "Creating the cold, warm, and hot recovery points" on page 222.

When you automate the creation of a warm recovery point (non-VSS-aware database), you run a command file in the backup policy. The command file is run before data capture to stop the database and commit all transaction logs to the hard disk. Symantec System Recovery snaps a "virtual volume recovery point." A second command file is run in the backup to automatically restart the database while the recovery point is created from the virtual volume recovery point.

The virtual volume snapshot takes only a few seconds to create. The database is in the recovery point state momentarily; which results in a minimal number of created log files.

See "To create a warm recovery point automatically" on page 222.

If a cold or warm recovery point is not possible in your organization, to back up non-VSS-aware databases, you can create a hot (or online) recovery point. Symantec System Recovery takes a crash-consistent recovery point. Such a recovery point is equivalent to the state of a system that was running when the power failed. A database that can recover from this type of failure can be recovered from a crash-consistent recovery point.

See "To create a hot recovery point" on page 223.

See "Backing up Notification Server and the database" on page 223.

See "About backing up VSS-aware databases" on page 219.

Creating the cold, warm, and hot recovery points

You can create cold recovery points manually, or warm recovery points automatically of non-VSS-aware databases. You can also create hot recovery points on non-VSS-aware recovery points.

See "About backing up non-VSS-aware databases" on page 221.

See "Backing up Notification Server and the database" on page 223.

See "Creating an independent backup task" on page 118.

To create a cold recovery point manually

1. Stop the database manually.
2. Use Symantec System Recovery 2013 R2 Management Solution to run a backup immediately using the Run Backup Policy task or the Independent Backup task.

   Symantec System Recovery instantaneously snaps a virtual volume recovery point of the database.
3. Manually restart the database anytime after the recovery point progress bar appears on the **Monitor** page of the console.

   While the database is restarted, the actual recovery point is created from the virtual volume recovery point.

To create a warm recovery point automatically

1. Define a backup that includes the command files that you have created for the following stages of the recovery point:

Before data capture	A command file that stops the database.
After data capture	A command file that restarts the database.

2. Use Symantec System Recovery to run the backup policy that includes the command files.

To create a hot recovery point

- Use Symantec System Recovery to create a recovery point without stopping or restarting the database.

  Symantec System Recovery instantaneously snaps a virtual volume recovery point from which the recovery point is created.

Backing up Notification Server and the database

Because Notification Server also includes a database, you should back up the server on a regular basis. This process requires you to stop the Altiris Notification Server before backing up so you do not lose or corrupt data. To automate such a backup process, you can use Symantec System Recovery through Symantec System Recovery 2013 R2 Management Solution to create a cold recovery point.

See "To create a warm recovery point automatically" on page 222.

Table A-1 Backing up Notification Server and the database

Step	Description
Step 1	Install the Symantec System Recovery Install Plug-in and Symantec System Recovery. See "Installing the Symantec System Recovery Plug-in on computers" on page 35. See "Installing Symantec System Recovery 2013 R2 or Symantec System Recovery 2013 R2 Linux Edition on client computers" on page 39. See "Configuring and installing LightsOut Restore 2013 R2 on client computers" on page 50.

Table A-1 Backing up Notification Server and the database *(continued)*

Step	Description
Step 2	Create a backup policy exclusively for Notification Server. No other computers should be assigned to this backup policy. ■ The backup policy needs to run two command files: One command file to stop the Altiris Notification Server before the snapshot is taken of the computer. And the other command file to restart Notification Server immediately after the snapshot. See "About running command files during a backup" on page 112. ■ Make sure that the backup policy runs at a time when backup policies for other managed computers do not run. For example, if most of your backup policies are scheduled to run at 02:00 A.M, the backup policy for the Symantec System Recovery 2013 R2 Management Solution server should run earlier than 02:00 A.M (or later).
Step 3	Make sure that the Symantec System Recovery 2013 R2 Management Solution server computer is not assigned to any Groups that you may have defined in the console. This ensures that the backup policies that are intended for other computers do not get assigned to the server.

Table A-2 Backup Policy Schedule tab options for a recovery point set

Schedule tab options	Description
Schedule	Lets you select the days and a start time for when the backup should run.
Start time (24 hour format)	Lets you customize the start time of the backup .
Sun Mon Tue Wed Thu Fri Sat	Lets you customize the days of the week for the backup to run. The default is to run the backup Monday through Friday.

Table A-2 Backup Policy Schedule tab options for a recovery point set *(continued)*

Schedule tab options	Description
Run more than once per day	Lets you run the backup more than once a day to protect the data that you edit or change frequently.
Time between backups	Lets you specify the maximum time that should occur between backups.
Number of times	Lets you specify the number of times per day that the backup should run.
Automatically optimize	Lets you select how often optimization should occur for the backup destination to manage the used disk space. You can choose from the following options: ■ **Never** Indicates that no deletion of incremental recovery points is performed. ■ **Every four hours** Indicates that a deletion of incremental recovery points that are four hours old (or older) is performed every four hours. Also, after the first incremental of the day is taken, all incremental files from two days previous are consolidated to a single file. ■ **Every twelve hours** Indicates that a deletion of incremental recovery points that are 12 hours old (or older) is performed every 12 hours. Also, after the first incremental of the day is taken, all incremental files from two days previous are consolidated to a single file.

Table A-2 Backup Policy Schedule tab options for a recovery point set *(continued)*

Schedule tab options	Description
Distribute strategy randomly across (minutes)	Indicates that the policy is distributed randomly across a specified number of minutes (0-1440) to all the computers that are assigned to the policy. This option applies if you save recovery points to a network destination. For example, suppose you want to distribute a backup policy in 60 minutes to 120 computers. Each of the 120 computers would randomly choose a time within the 60 minutes, before or after the scheduled start time, to start the backup. This option helps to run not the policy at the same start time for all computers, which can cause a denial of service condition on the network, the recovery point destination, or both.
Start a new recovery point set	Lets you select how frequently a new recovery point set should be started. Your options for starting new recovery point set (base) include the following: ■ **Weekly** Creates a new recovery point set on the first scheduled or manual backup of the week. ■ **Monthly** Creates a new recovery point set on the first scheduled or manual backup of the month. ■ **Quarterly** Creates a new recovery point set on the first scheduled or manual backup every three months from the date when you selected this option. ■ **Yearly** Creates a new recovery point set on the first scheduled or manual backup of the year, once a year, on the date that you selected for this option. ■ **Custom** Lets you set specific weekly or monthly options for starting a new recovery point set.

Table A-2 Backup Policy Schedule tab options for a recovery point set *(continued)*

Schedule tab options	Description
Custom	Lets you customize the start time, and the days of the week or month to run the backup. **Note:** If you choose to archive recovery points, consider creating recovery point sets more frequently to keep the size of your recovery point sets smaller.

Table A-3 Backup Policy Triggers tab options for a recovery point set

Triggers tab options	Description
Any application is installed	Indicates that an incremental recovery point is created at the time users begin to install a software application on their computer.
Specified applications are launched	Indicates that an incremental recovery point is created at the time users run a specified software application on their computer.
Any user logs on to the computer	Indicates that an incremental recovery point is created when users log on to Windows on their computer.
Any user logs off from the computer	Indicates that an incremental recovery point is created at the moment users log off from Windows on their computer (but does not turn off Windows).
Data added to the drive exceeds	Indicates that an incremental recovery point is created when the added data on a drive exceeds an amount (in megabytes) that you specify.

Table A-4 Backup Policy ThreatCon tab options for a recovery point set

ThreatCon tab options	Description
Do Not Monitor - Disable	Lets you turn off monitoring of ThreatCon levels for the selected backup policy. **Note:** Level 1 of Symantec ThreatCon indicates that there are no discernable security threats. Because level 1 suggests no threats, it is not an option.
Level 2	Security threats can occur, although no specific threats have been known to occur.
Level 3	An isolated security threat is in progress.

Table A-4 Backup Policy ThreatCon tab options for a recovery point set *(continued)*

ThreatCon tab options	Description
Level 4	Extreme global security threats are in progress.

Table A-5 Backup Policy Schedule options for an independent recovery point

Schedule option	Description
Automatically create a recovery point	Lets you specify a weekly or monthly backup schedule. The scheduling options include the following: ■ **Weekly** Creates a new, independent recovery point on each day of the week that you check, and at the specified time. When you create independent recovery points one or more times per week, large amounts of disk storage space may be required. ■ **Monthly** Creates a new, independent recovery point on each day of the month that you check, and at the specified time. ■ **No Schedule** Saves all of the backup policy settings except a schedule. You can later deploy the backup policy at your convenience by assigning a schedule to the policy. You can also create a single independent recovery point once, with no schedule. See "Creating an independent backup task" on page 118.
Start time (24 hour format)	Lets you customize the start time of the backup .
Days of the week	Lets you customize the days of the week for the backup policy to run.
Days of the month	Lets you customize the days of the month for the backup policy to run.

Table A-5 Backup Policy Schedule options for an independent recovery point *(continued)*

Schedule option	Description
Distribute strategy randomly across (minutes)	Indicates that the policy is distributed randomly across a specified number of minutes (0-1440) to all the computers that are assigned to the policy. This option applies if you save recovery points to a network destination. For example, suppose you want to distribute a backup policy in 60 minutes to 120 computers. Each of the 120 computers would randomly choose a time within the 60 minutes, before or after the scheduled start time, to start the backup. This option helps to not run the policy at the same start time for all computers, which can cause a denial of service condition on the network, the recovery point destination, or both.

Appendix B

About Active Directory

This appendix includes the following topics:

About the role of Active Directory

When protecting a domain controller with Symantec System Recovery 2013 R2 Management Solution, be aware of the following:

- If your domain controller is Windows Server 2003, it supports VSS. Symantec System Recovery 2013 R2 Management Solution automatically calls VSS (Volume Shadow-copy Service) to prepare the Active Directory database for backup. Windows 2000 domain controllers do not support VSS. In cases where the domain controller is running on a Windows 2000 server, the Active Directory database must be backed up using NTbackup. This backup should be done before you use Symantec System Recovery 2013 R2 Management Solution to protect the full system. This process can be automated using an external command that Symantec System Recovery 2013 R2 Management Solution calls. When you configure a backup job, you have the option to enter external commands. This option provides a process for protecting the domain controllers that do not support VSS.

  See "About running command files during a backup" on page 112.

- To participate on a domain, every domain computer must negotiate a trust token with a domain controller. This token is refreshed every 30 days by default. This time frame can be changed, and is referred to as a secure channel trust. The domain controller does not automatically update a trust token that a recovery point contains. Therefore, when you recover a computer using a recovery point that contains an outdated token, the computer cannot participate in the domain. The computer must be added to the domain by someone who has the required credentials.

In Symantec System Recovery 2013 R2 Management Solution, this trust token can be re-established automatically if the computer already participates in the domain at the time the recovery process starts.

- In most cases, domain controllers should be restored non-authoritatively. This action prevents outdated objects in the Active Directory from being restored. Outdated objects are referred to as tombstones. Active Directory does not restore data older than the limits it sets. Restoring a valid recovery point of a domain controller is the equivalent of a non-authoritative restore. To determine which type of restore you want to perform, please refer to the Microsoft documentation. A non-authoritative restore prevents tombstone conflicts.

For additional details about protecting non-VSS aware domain controllers, see the white paper titled "Protecting Active Directory," which is located at the following website.

http://sea.symantec.com/protectingdc

You can also refer to the following Symantec Knowledge Base:

http://entsupport.symantec.com/umi/V-269-16

Appendix C

Backing up Microsoft virtual environments

This appendix includes the following topics:

About backing up Microsoft virtual hard disks

Microsoft Windows 7/Server 2008 R2 now support the use of Virtual Hard Disks (VHDs). Microsoft does not support backing up a physical disk and a VHD on that physical disk in the same backup job. This limitation also applies to Symantec System Recovery 2013 R2 Management Solution. You cannot back up a physical disk and its VHD counterpart in the same backup job using Symantec System Recovery 2013 R2 Management Solution. Also not supported is the ability to back up a VHD that is hosted on or "nested" within another VHD. If you want to back up a physical disk and a VHD on that disk, you must create separate backup jobs for each disk.

Backing up a physical disk that hosts a VHD is supported as long as it is not included as another volume in the same backup. When a physical disk hosting a VHD is backed up, the VHD is treated as another file that is part of the physical disk backup.

VHDs can be attached and detached from their physical disk hosts (volumes). Microsoft recommends that you detach a VHD that is stored on a host volume before you back up. Not detaching a VHD before you back up a host volume can result in an inconsistent copy of the VHD in the backup. After you restore a host volume, you can re-attach the VHD file.

http://entsupport.symantec.com/umi/V-306-2

You can find more information on backing up VHDs on the Microsoft website.

http://technet.microsoft.com/en-us/library/dd440865(WS.10).aspx

Find information about backing up and restoring Microsoft Hyper-V virtual machines:

See "About backing up and restoring Microsoft Hyper-V virtual machines" on page 233.

About backing up and restoring Microsoft Hyper-V virtual machines

To create a backup of a Microsoft Hyper-V virtual machine, you must back up the volumes of the computer where the virtual machine is hosted. Create either a live backup or a system state backup of the host machine. You cannot back up or restore a specific virtual machine. A live backup is created while the virtual machine is running (hot backup).

A system state backup is created in any of the following conditions:

- The guest operating system on the virtual machine is not running (cold backup).
- The Hyper-V VSS integration component is not installed in the virtual machine.

Note: Symantec System Recovery 2013 R2 Management Solution is unable to back up cluster shared volumes. Because volumes in such a configuration are accessible to each of the clustered Hyper-V host computers, a given volume cannot be locked for backup . However, clustered disks can be backed up by Symantec System Recovery 2013 R2 Management Solution because one host has exclusive access to the disk.

To create a backup of a running virtual machine, the following conditions must be met:

- The guest operating system must be running.
- The guest computer must be running Windows Server 2003 or later.
  If the guest computer is running Windows 2000, you can only create a system state backup (cold backup).
- The Hyper-V VSS integration component must be installed on each virtual machine to be backed up.
  If you move a virtual machine from Virtual Server 2005 to Hyper-V, first uninstall the Virtual Server 2005 integration component from the virtual machine. After you Virtual Server 2005 integration component, you can install the Hyper-V VSS integration component.

- The guest virtual machine should be configured to only use basic disks, not dynamic disks.
  This configuration is the default for installing a Windows virtual machine.
- All the volumes on the fixed disks must support the creation of snapshots.

If you perform a backup when these conditions are not met, Symantec System Recovery 2013 R2 Management Solution creates a system state recovery point that is crash-consistent. A crash-consistent recovery point captures the virtual machine as if it had experienced a system failure or power outage.

You can restore a specific virtual machine from the recovery point of the host computer using the Recovery Point Browser. Use the Recovery Point Browser to extract the files that make up the virtual machine. The host computer recovery point must include the volume that holds the virtual machine that you want to restore.

To know about the limitations of Hyper-V when backing up databases on virtual machines, refer to the Symantec Knowledge Base:

http://entsupport.symantec.com/umi/V-306-2

Find information about backing up Microsoft virtual hard disks:

See “About backing up Microsoft virtual hard disks” on page 232.

http://entsupport.symantec.com/umi/V-306-2

Appendix D

About Symantec System Recovery 2013 R2 Management Solution and Windows Server 2008 Core

This appendix includes the following topics:

About Symantec System Recovery 2013 R2 and Windows Server 2008 Core

Windows Server 2008 Core does not include the traditional graphical user interface (GUI) that is available with other versions of Windows. It is installed and managed primarily using commands at the command line interface.

Although Symantec System Recovery 2013 R2 can be installed on Windows Server 2008 Core, it is an agent only install. Windows Server 2008 Core does not support Microsoft .NET. Therefore, the Symantec System Recovery GUI cannot be installed. Symantec System Recovery is supported on Windows Server 2008 Core by a headless agent only. You can install Symantec System Recovery 2013 R2 using commands at the command line. You can also install (push) the agent from a remote machine.

One-to-one management is the only supported method for backing up and restoring a Windows Server 2008 Core computer. This means, after you install the agent on a Windows Server 2008 Core computer, connect to it from a remote machine running one of the following:

- Symantec System Recovery 2013 R2
- Symantec System Recovery 2013 R2 Management Solution

Before installing the agent remotely on a Windows Server 2008 Core computer, you must configure the firewall to allow access to the server. By default, the firewall is configured to allow no access to the server.

For more information on configuring the firewall on a Windows Server 2008 Core computer, see the Microsoft website.

Windows-on-Windows 64-bit (WoW64) is a subsystem of the Windows operating system and is required for running 32-bit applications on 64-bit versions of Windows. It is installed by default and is included on all 64-bit versions of Windows. If you have uninstalled WoW64 on a Windows Server 2008 Core R2 computer, you must reinstall it before installing Symantec System Recovery 2013 R2.

See "Installing Symantec System Recovery 2013 R2 on Windows Server 2008 Core using commands" on page 236.

Installing Symantec System Recovery 2013 R2 on Windows Server 2008 Core using commands

The following options exist for installing Symantec System Recovery 2013 R2 on a Windows Server 2008 Core system. They are

- Full install with GUI support
- Full silent install with logging
- Agent-only silent install with logging

Installing Symantec System Recovery 2013 R2 using the option for full install with GUI support

1. On the Symantec System Recovery 2013 R2 DVD, browse to and run `Browser.exe`.

   A graphical environment (GUI) is launched where you complete the remainder of the installation.

2. Complete the installation by following the steps in the installation wizard.

   Even though the full Symantec System Recovery is installed, only the agent is needed and used on Windows Server 2008 Core.

To install Symantec System Recovery 2013 R2 using the option for full silent install with logging

1. On the Symantec System Recovery 2013 R2 DVD, change to the Install directory.
2. Run the following command:

   ```
   Setup.exe /S: /FULL:
   ```

   Even though the full Symantec System Recovery is installed, only the agent is needed and used on Windows Server 2008 Core.

To install Symantec System Recovery 2013 R2 using the option for agent-only silent install with logging

1. On the Symantec System Recovery 2013 R2 DVD, change to the Install directory.
2. Run the following command:

   ```
   Setup.exe /S: /SERVICE:
   ```

Appendix E

Using a search engine to search recovery points

This appendix includes the following topics:

About using a search engine to search recovery points

Symantec System Recovery supports the use of Google Desktop for searching file names in recovery points.

Note: Only Symantec System Recovery 2011 and Backup Exec System Recovery 2010 provide support to use Google Desktop Search engine to search file names in recovery points. Symantec System Recovery 2013 does not support Google Desktop search engine.

Note: Backup Exec Retrieve is also supported, but your company's IT department must install it . When they install it, there is nothing you have to do to enable it. Ask your IT department for details.

When a backup runs, Symantec System Recovery generates a catalog of all of the files that are included in the recovery point. Google Desktop can then use the catalog to generate an index of the files that are contained in each recovery point.

When you enable search engine support, Symantec System Recovery creates a catalog of all of the files that are contained in a recovery point. Search engines like Google Desktop use the catalog file to generate an index. You can then search for files by name. Google Desktop does not index the content of files. It only indexes the file names.

Recovery points that already exist when you enable this feature cannot be indexed. This restriction is because the generated list of required files by search engines for generating searchable indexes are appended to recovery points. After you enable this feature, run each backup policy to create a new recovery point that contains the required information for indexing.

Note: If the backup destination is on a network drive, be sure to add the location to the Google Desktop preferences.

See "Enabling search engine support in recovery points" on page 239.

See "Recovering files by using Google Desktop's Search Desktop feature" on page 246.

See "Troubleshooting Google Desktop with Symantec System Recovery 2013 R2 Management Solution" on page 247.

Enabling search engine support in recovery points

To search recovery points with a search engine such as Google Desktop, you must do all of the following:

Table E-1 Process for enabling search engine support in recovery points

Process	Description
Install a search engine	An organization's IT department installs Backup Exec Retrieve. Ask your IT department if it is available. You can download and install Google Desktop for free from the Internet. Visit desktop.google.com. See "To install Google Desktop" on page 243.
Enable Google Desktop support	A Google plug-in for Symantec System Recovery on the client computer is required before you can use Google Search to locate and recover files. The plug-in is installed for you automatically when you enable this feature. See "Installing Google Desktop" on page 243.

Table E-1 Process for enabling search engine support in recovery points *(continued)*

Process	Description
Enable search engine support when defining or editing a backup policy	When you create or edit an advanced backup policy, enable search engine support. The next time the backup is run, it creates a list of all files that are contained in the resulting recovery point. A search engine such as Google Desktop can then use the list to generate its own index and let you perform searches by file name.

Table E-2 Advanced recovery point options

Option	Description
Active backup policy	Activates the backup policy on the managed client computer. If you deselect this option, the backup policy is still sent to the managed client computer but it is not activated.
Limit the number of recovery point sets (bases) saved for this backup (Recovery point sets only) or **Limit the number of recovery points saved for this backup** (Independent recovery points only)	Specifies the maximum number of recovery points or recovery point sets that are saved for each drive. When this limit is reached, each successive recovery point or set is first created and stored. The oldest, previously created recovery point or set is then deleted (including all associated incrementals, if applicable) from the same storage location. Ensure that you have enough hard disk space to accommodate the number of recovery points or sets you specify, plus one additional recovery point or set. If you run out of hard disk space before the number is reached, the recurring recovery point process cannot complete successfully, and a current recovery point or set is not created.
Verify recovery point after creation	Checks whether a recovery point or recovery point set is valid or corrupt immediately following its creation. For steps on how to verify the integrity of a recovery point long after it has been created, refer to the Symantec System Recovery product documentation. When you verify a recovery point, it can approximately double the time that is required to create the recovery point.

Table E-2 Advanced recovery point options *(continued)*

Option	Description
Disable SmartSector copying	Speeds up the copying process by copying only hard disk sectors with data. However, in some cases, it may be desirable to copy all sectors in their original layout, whether or not they contain data. If you want to copy both used and unused hard disk sectors, select **Disable SmartSector Copying**. When you select this option, it increases the process time, and usually results in a larger recovery point file size.
Ignore bad sectors during copy	Creates a recovery point even if bad sectors are on the hard drive. Although most drives do not have bad sectors, the potential for problems increases during the lifetime of the hard drive.
Perform full VSS backup	Lets you perform a full backup on the VSS storage and send a request for VSS to review its own transaction log. This option is used for VSS applications, such as Microsoft SQL. VSS determines what transactions are already committed to the database and then truncates those transactions. Among other things, truncated transaction logs help keep the file size manageable and limits the amount of hard drive space that the file uses. If you do not select this option, backups still occur on the VSS storage. However, VSS does not automatically truncate the transaction logs following a backup. **Note:** This option does not apply to Symantec System Recovery Linux Edition.

Table E-2 Advanced recovery point options *(continued)*

Option	Description
Divide into smaller files to simplify archiving	Splits a recovery point into two or more smaller files. This feature is useful if you create or export a recovery point that you want to copy to removable media later for safekeeping. The recovery point is split into smaller, more manageable files. You can then copy the files onto separate, removable media, such as a DVD or CD. If Symantec System Recovery creates an .sv2i file in addition to the .v2i files, you need to save the .sv2i file on the same media as the first .v2i file. If you create a recovery point of volumes with thousands of files on a computer that has low memory, splitting the recovery point into smaller segments can help speed the process. If a recovery point is divided into multiple files, the file names for subsequent files are appended with _S01, _S02, and so forth. For example, if the default file name were Dev-RBrough_C_Drive.v2i, the second file name would be Dev-RBrough_C_Drive_S01.v2i, and so on.
Enable search engine support for Google Desktop	Uses your search engine software to index all of the file names that are contained in each recovery point. By indexing file names, you can then use a search engine of choice to locate the files that you want to retrieve. A search tool such as Google Desktop, may already be installed on their computer to search their recovery points. See *Appendix A: Using a search engine to search recovery points* in the *Symantec System Recovery User's Guide* for information about using Google Desktop to retrieve files. **Note:** This option does not apply to Symantec System Recovery Linux Edition.
Include system and temporary files	Includes the indexing support for the operating system and temporary files when a recovery point is created on the client computer. **Note:** This option does not apply to Symantec System Recovery Linux Edition.

Installing Google Desktop

You turn on search engine support in recovery points by installing Google Desktop. You must then enable Google Desktop support and search engine support in a backup policy.

See "About using a search engine to search recovery points" on page 238.

See "Recovering files by using Google Desktop's Search Desktop feature" on page 246.

To install Google Desktop

1. Start Symantec System Recovery on the client computer.
2. Click **Tasks > Options > Google Desktop**.
3. Click **Download Google Desktop from the Web** and follow instructions for installation.
4. After it is installed, click **OK** in the **Symantec System Recovery Options** window.

   For more information, visit desktop.google.com.

   Now you must enable Google Desktop support in Symantec System Recovery.
5. Click **Tasks > Options > Google Desktop**.
6. Check **Enable Google Desktop File and Folder Recovery**.
7. Click **OK** to install the Google plug-in.

   Now you must enable search engine support for a backup policy.
8. In Symantec System Recovery 2013 R2 Management Solution, do one of the following:
   - Edit an existing backup policy and check **Enable search engine support for Google Desktop and Backup Exec Retrieve** in the **Advanced** options.
   - Create a new, advanced backup policy and check **Enable search engine support for Google Desktop and Backup Exec Retrieve** in the **Advanced** options.

Active backup policy	Activates the backup policy on the managed client computer. If you deselect this option, the backup policy is still sent to the managed client computer but it is not activated.

Limit the number of recovery point sets (bases) saved for this backup (Recovery point sets only) or **Limit the number of recovery points saved for this backup** (Independent recovery points only)	Specifies the maximum number of recovery points or recovery point sets that are saved for each drive. When this limit is reached, each successive recovery point or set is first created and stored. The oldest, previously created recovery point or set is then deleted (including all associated incrementals, if applicable) from the same storage location. Ensure that you have enough hard disk space to accommodate the number of recovery points or sets you specify, plus one additional recovery point or set. If you run out of hard disk space before the number is reached, the recurring recovery point process cannot complete successfully, and a current recovery point or set is not created.
Verify recovery point after creation	Checks whether a recovery point or recovery point set is valid or corrupt immediately following its creation. For steps on how to verify the integrity of a recovery point long after it has been created, refer to the Symantec System Recovery product documentation. When you verify a recovery point, it can approximately double the time that is required to create the recovery point.
Disable SmartSector copying	Speeds up the copying process by copying only hard disk sectors with data. However, in some cases, it may be desirable to copy all sectors in their original layout, whether or not they contain data. If you want to copy both used and unused hard disk sectors, select **Disable SmartSector Copying**. When you select this option, it increases the process time, and usually results in a larger recovery point file size.
Ignore bad sectors during copy	Creates a recovery point even if bad sectors are on the hard drive. Although most drives do not have bad sectors, the potential for problems increases during the lifetime of the hard drive.

Perform full VSS backup

Lets you perform a full backup on the VSS storage and send a request for VSS to review its own transaction log. This option is used for VSS applications, such as Microsoft SQL.

VSS determines what transactions are already committed to the database and then truncates those transactions. Among other things, truncated transaction logs help keep the file size manageable and limits the amount of hard drive space that the file uses.

If you do not select this option, backups still occur on the VSS storage. However, VSS does not automatically truncate the transaction logs following a backup.

Note: This option does not apply to Symantec System Recovery Linux Edition.

Divide into smaller files to simplify archiving

Splits a recovery point into two or more smaller files. This feature is useful if you create or export a recovery point that you want to copy to removable media later for safekeeping. The recovery point is split into smaller, more manageable files. You can then copy the files onto separate, removable media, such as a DVD or CD.

If Symantec System Recovery creates an .sv2i file in addition to the .v2i files, you need to save the .sv2i file on the same media as the first .v2i file.

If you create a recovery point of volumes with thousands of files on a computer that has low memory, splitting the recovery point into smaller segments can help speed the process.

If a recovery point is divided into multiple files, the file names for subsequent files are appended with _S01, _S02, and so forth. For example, if the default file name were Dev-RBrough_C_Drive.v2i, the second file name would be Dev-RBrough_C_Drive_S01.v2i, and so on.

Enable search engine support for Google Desktop	Uses your search engine software to index all of the file names that are contained in each recovery point. By indexing file names, you can then use a search engine of choice to locate the files that you want to retrieve. A search tool such as Google Desktop, may already be installed on their computer to search their recovery points. See *Appendix A: Using a search engine to search recovery points* in the *Symantec System Recovery User's Guide* for information about using Google Desktop to retrieve files. **Note:** This option does not apply to Symantec System Recovery Linux Edition.
Include system and temporary files	Includes the indexing support for the operating system and temporary files when a recovery point is created on the client computer. **Note:** This option does not apply to Symantec System Recovery Linux Edition.

Recovering files by using Google Desktop's Search Desktop feature

If you have correctly set up and enabled support for Google Desktop, you can search recovery points to recover files by using Google Desktop.

See "Troubleshooting Google Desktop with Symantec System Recovery 2013 R2 Management Solution" on page 247.

See "About using a search engine to search recovery points" on page 238.

See "Installing Google Desktop" on page 243.

To recover files by using Google Desktop

1. Start Google Desktop on the client computer.
2. Enter the name (or part of the name) of a file you want to recover, and then click **Search Desktop**.
3. Click the search result that contains the file you want to recover.
4. Do one of the following:
   - To save the recovered file when the file opens, click **File > Save As**.
   - To open the recovery point in the Recovery Point Browser, right-click the name of the file, and then click **Open**.

Troubleshooting Google Desktop with Symantec System Recovery 2013 R2 Management Solution

Sometimes you may find that a file is included in a recovery point that has search engine support enabled, but the file is not found. In such cases, you can do the following:

- Re-index the recovery point.
  Right-click the Google Desktop icon in the system tray of the client computer and click **Indexing > Re-Index**.
  Re-indexing can take a significant amount of time. Be sure to wait until it completes before attempting to search again.
- Verify that the option to index the content of the recovery point is enabled.
  Right-click the Google Desktop icon in the system tray of the client computer and click **Preferences**.
  Under **Search Types**, verify that **web history** is checked. If this option is not checked, then Google Desktop cannot index the content of recovery points.
- Verify that the drive with the recovery points (backup destination) is available.
  For example, if the backup destination is a USB drive, be sure that the drive is plugged in and that the power is turned on. Or, if the backup destination is on a network, be sure that you are connected and logged on with the correct credentials.
- Add **v2i** to the search string to narrow down the number of search results.
  For example, if you search for Cathy Read mp3, add v2i so that the search string is **Cathy Read mp3 v2i**.
  Recovery point files use .v2i as their file extension name.
- If the backup destination is on a network drive, be sure to add the location to the **Search These Locations** setting in Google Desktop Preferences.

See "Recovering files by using Google Desktop's Search Desktop feature" on page 246.

Index

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V