Backup Exec™ System Recovery 2010 Management Solution

Administrator's Guide

Backup Exec™ System Recovery 2010 Management Solution Administrator's Guide

Documentation version: 9.0

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 Backup Exec System Recovery 2010 Management Solution

This chapter includes the following topics:

About Backup Exec System Recovery 2010 Management Solution

Backup Exec System Recovery 2010 Management Solution provides enterprise-level backup management tasks for server and desktop protection.

Using Backup Exec System Recovery 2010 Management Solution, you can centrally monitor the recovery point status for 500-1000 remote 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 Backup

Exec System Recovery, you can also perform remote system and drive recovery of Windows computers (Linux computers must be recovered locally).

What is new in Backup Exec System Recovery 2010 Management Solution

Backup Exec System Recovery 2010 Management Solution includes many enhancements and new features since Backup Exec System Recovery Solution 8.5, including the following:

Table 1-1 What is new in Backup Exec System Recovery 2010 Management Solution

Feature	Description
Support for backing up Linux-based computers	You can now deploy Backup Exec System Recovery 2010 Linux Edition to Linux-based computers and then use the Independent Backup task in Backup Exec System Recovery 2010 Management Solution to backup them. **Note:** Backup Exec System Recovery 2010 Linux Edition is available in English only. See "About installing the Backup Exec System Recovery Plug-in on client computers" on page 45. See "About installing Backup Exec System Recovery 2010, Backup Exec System Recovery 2010 Linux Edition, or LightsOut Restore 2010 on client computers " on page 49. See "Creating an Independent Backup task" on page 115.
Enhanced user interface in the Home tab and Manage Tasks tab of Backup Exec System Recovery 2010 Management Solution	An improved user interface simplifies what you need to know and do to successfully back up or recover drives, or your entire computer. See "About the Backup Exec System Recovery 2010 Management Solution Home page" on page 38.

Table 1-1 What is new in Backup Exec System Recovery 2010 Management Solution *(continued)*

Feature	Description
Recovery point password store	You can use the password store to add all potential passwords that you have used for recovery points. When you run a Convert to Virtual task, for example, the client computer can use the password store to find the correct password and unlock the recovery point. See "About the recovery point password store" on page 66.
Offsite Copy	The new Offsite Copy feature adds an additional level of protection to your data by copying recovery points to a second hard disk drive. You can copy them over the network to a remote location through a local area connection, or using FTP. See "Creating a basic backup policy" on page 88. There is also a new Dedicated Offsite Copy feature. See "Configuring a Dedicated Offsite Copy task" on page 73.
Convert recovery points to virtual disks	Create scheduled conversions of recovery points to VMware Virtual Disk, Microsoft Virtual Disks, or directly to VMware ESX Server. See "About convert to virtual" on page 131.
Express Recovery	You can use an Express Recovery task to restore multiple computers at once using a selected computer's recovery points. See "Configuring a remote Express Recovery task" on page 165.
FTP configuration policy	Set the default FTP connection settings if you use FTP as an offsite copy destination. See "Configuring a client option policy for computers" on page 150.

Table 1-1 What is new in Backup Exec System Recovery 2010 Management Solution *(continued)*

Feature	Description
Recovery history	View 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. See "About viewing Backup Exec System Recovery details for a client computer" on page 122.
Support for hidden volumes	Ability to backup or convert to virtual disk all drives that exist on a client computer, including hidden drives (partitions).
Windows 7 and Windows Server 2008 R2 support	You can install Backup Exec System Recovery on computers that run Windows 7 or Windows Server 2008 R2..
Symantec ThreatCon integration	Symantec ThreatCon is Symantec's early threat warning system. You can now configure Backup Exec System Recovery to detect a change in the threat level whenever your computer is connected to the Internet. When the threat level meets or exceeds the level you specify, Backup Exec System Recovery automatically starts a backup job. You can specify a different ThreatCon level for each backup. See "Scheduling options for creating recovery points " on page 92. See "About the Backup Exec System Recovery 2010 Management Solution Home page" on page 38.

Components of Backup Exec System Recovery 2010 Management Solution

An installation of Backup Exec System Recovery 2010 Management Solution consists of several main components for managing recovery points on client computers.

Table 1-2 describes these main components.

Table 1-2 Components of Backup Exec System Recovery 2010 Management Solution

Component	Description
Backup Exec System Recovery 2010 Management Solution	Backup Exec System Recovery 2010 Management Solution lets you remotely run and manage backup policies and recovery on client computers from a central location. See "About the Backup Exec System Recovery 2010 Management Solution Home page" on page 38.
Backup Exec System Recovery 2010 Management Solution configuration file	The 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. ■ Backup Exec System Recovery Plug-in install file. Backup Exec System Recovery 2010 Management Solution already comes with a software delivery policy of Backup Exec System Recovery 2010 that you can deploy to resource targets. You can also create your own Backup Exec System Recovery Plug-in software delivery policies by editing the packages already provide in the solution. Or, you can create new Backup Exec 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.
Backup Exec System Recovery 2010 Management Solution Web pages	Installs all the Web pages that the solution uses.

Table 1-2 Components of Backup Exec System Recovery 2010 Management Solution *(continued)*

Component	Description
Backup Exec System Recovery Plug-in	The Backup Exec System Recovery Plug-in is a necessary component of Backup Exec System Recovery. It must be installed on each computer that has backups you want to manage. The 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 ■ Backup Exec System Recovery version ■ Any configuration changes that are made to the computer A computer is considered "managed" by Backup Exec System Recovery 2010 Management Solution when the Backup Exec System Recovery Plug-in is installed on it. See "About installing the Backup Exec System Recovery Plug-in on client computers" on page 45.
Microsoft IIS Virtual Directory path	The IIS virtual directory path references the Web folder of your solution installation path.

Backup Exec System Recovery

Backup Exec System Recovery provides advanced backup and recovery for Windows-based client computers and backup for Linux-based client computers. Backup Exec System Recovery 2010 Management Solution comes with a software delivery policy of Backup Exec System Recovery 2010. You can also create and deploy your software delivery policies of Backup Exec System Recovery 8.0 or 8.5 or Backup Exec System Recovery 2010 Linux Edition to the resource targets you want.

Note: Backup Exec System Recovery 2010 Linux Edition is available in English only.

See "About installing Backup Exec System Recovery 2010, Backup Exec System Recovery 2010 Linux Edition, or LightsOut Restore 2010 on client computers " on page 49.

To learn more about Backup Exec System Recovery, see the *Backup Exec System Recovery 2010 User's Guide* in PDF. To learn more about Backup Exec System Recovery 2010 Linux Edition, see the *Backup Exec System Recovery 2010 User's Guide Linux Edition* in PDF.

How Backup Exec System Recovery 2010 Management Solution works

In Backup Exec System Recovery 2010 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 Backup Exec System Recovery 2010 Management Solution components on the server process them. All interaction to the Backup Exec System Recovery 2010 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 group 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, including backup failures, and delete recovery point task status.

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

What you can do with Backup Exec System Recovery 2010 Management Solution

Backup Exec System Recovery 2010 Management Solution lets you work from a remote location to back up and recover Windows-based computers or back up Linux-based computers.

Table 1-3 describes the most frequently used tasks.

Table 1-3 What you can do with Backup Exec System Recovery 2010 Management Solution

Task	Description
Define backup policies and tasks and recovery point storage locations	■ 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. ■ Define an Independent Backup task for Linux-based computers.
Remotely recover one drive, multiple drives, or an entire computer (Windows-based)	■ Remotely recover a data drive on a managed client computer. ■ Remotely recover a system drive on a managed client computer that is bootable, using LightsOut Restore.
Deploy command files on Windows-based computer	■ 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. ■ Or, you can specify a folder on a network share where the command files are access by managed client computers during a particular stage in the recovery point creation process.
Remotely delete recovery points	■ Delete entire recovery point sets. ■ Delete recovery points within a set.
Administer server, desktop, and laptop computers	■ Troubleshoot and resolve backup policies remotely. ■ Run various predefined reports on managed computers. ■ Manage Backup Exec System Recovery licenses on resource targets. ■ Monitor the overall status of recovery points for an entire network of Windows computers.

Best practices for creating recovery points

The following list represents some best practices for creating recovery points:

- Before a backup
- During a backup
- After a backup

Before a backup

Table 1-4 describes best practices to ensure the successful creation of recovery points.

Table 1-4 Before a backup

Before a backup	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 being polled six times, the computer is put into a "Needs attention" state. However, if Backup Exec System Recovery (with a user interface) is installed on the client computer, Backup Exec System Recovery asks the user if they want to run the missed backup (after the computer is turned on and they log on to Windows). In the meantime, the backup status of the client computer in Backup Exec System Recovery 2010 Management Solution console is "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.
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 use the console to create recovery points of computers across one or more 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 2 hours ahead of the Backup Exec System Recovery 2010 Management Solution console time. You create a backup policy to run at 6:00 p.m.. When the backup policy begins on the client computer it is 6:00 p.m. However, the console displays the policy as beginning at 4:00 p.m..
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.

Table 1-4 Before a backup *(continued)*

Before a backup	Description
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	Backup Exec System Recovery 2010 Management Solution supports saving recovery points to network locations or to a local hard disk. You should avoid storing recovery points on the Backup Exec System Recovery 2010 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.

During a backup

Improve client computer performance during a backup.

Backup Exec System Recovery requires significant system resources to run a backup. If remote users 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 150.

After a backup

Table 1-5 describes best practices after a backup occurs.

Table 1-5 After a backup

After a backup	Description
Maintain duplicate recovery points for safety.	Store recovery points on the network and create CDs, DVDs, or tapes of recovery points for storage off-site in a safe, secure place. Use Symantec Backup Exec for Windows Servers to back up recovery point locations on the network to tape.

Table 1-5 After a backup *(continued)*

After a backup	Description
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 (using the Recovery Point Browser in Backup Exec System Recovery) 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.
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 Backup Exec System Recovery 2010 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 you back up essential data by periodically reviewing the contents of recovery points files with Recovery Point Browser in Backup Exec System Recovery.

Chapter 2

Installing Backup Exec System Recovery 2010 Management Solution

This chapter includes the following topics:

Before you install

Backup Exec System Recovery 2010 is already included as a software delivery policy with Backup Exec System Recovery 2010 Management Solution.

Refer to the Backup Exec System Recovery 2010 or the Backup Exec System Recovery 2010 Linux Edition product documentation for complete system requirements.

If you intend to define your own software delivery policies of Backup Exec System Recovery 8.0 or 8.5 or Backup Exec System Recovery 2010 Linux Edition, the system requirements vary depending on the package contents.

See "About installing Backup Exec System Recovery 2010, Backup Exec System Recovery 2010 Linux Edition, or LightsOut Restore 2010 on client computers " on page 49.

Backup Exec System Recovery 2010 Management Solution supports 500-1000 installations of Backup Exec System Recovery for each installation of the solution. However, network performance varies greatly among organizations. The total number of supported installations of Backup Exec System Recovery may be more or less for your network. Network performance should be monitored to ensure that installations of Backup Exec System Recovery are not extended beyond the capacity and capability of your network.

Migrating managed client computers from Backup Exec System Recovery Manager 8.5 to Backup Exec System Recovery 2010 Management Solution

You can migrate managed client computers from Backup Exec System Recovery Manager 8.5 to Backup Exec System Recovery 2010 Management Solution. Also, hardware that was used for hosting the Backup Exec System Recovery Manager 8.5 server can be repurposed to host the Backup Exec System Recovery 2010 Management Solution server. The minimum system requirements still apply. You may not need to purchase or provision new hardware for the migration.

When you migrate managed client computers from Backup Exec System Recovery Manager 8.5 to Backup Exec System Recovery 2010 Management Solution, you must first do the following:

- Install the Altiris Agent on all the client computers that Backup Exec System Recovery Manager 8.5 manages.
- Install the Backup Exec System Recovery Plug-in on all the client computers that Backup Exec System Recovery Manager 8.5 manages.

When the newly managed client computers in Backup Exec System Recovery 2010 Management Solution publish information back to the Backup Exec System Recovery 2010 Management Solution server, the following occurs:

- Client computers with Backup Exec System Recovery already installed can be discovered and targeted from Backup Exec System Recovery 2010 Management Solution. A default resource target of computers with Backup Exec System Recovery already installed comes with Backup Exec System Recovery.

- Management Control, as used by Backup Exec System Recovery Manager 8.5 and installed on client computers, is automatically removed. This event occurs when the client computer with Backup Exec System Recovery is brought under management by the Backup Exec System Recovery 2010 Management Solution server.
- The Backup Exec System Recovery Agent Plug-in and the Backup Exec System Recovery 2010 install package is centrally 'push-able' from the Backup Exec System Recovery 2010 Management Solution server.
- Client computer history and events are preserved. Such preservation means you can recover from recovery points that were created before the migration to Backup Exec System Recovery 2010 Management Solution.
- Client computer settings for Backup Exec System Recovery are preserved. However, if the administrator has created policies in Backup Exec System Recovery 2010 Management Solution to adjust those settings, then they are not preserved.

The following are not preserved after the migration:

- Backup jobs and policies, and backup destination are not preserved following the migration. Backup policies, as they are known in Backup Exec System Recovery 2010 Management Solution, and backup destinations must be recreated.
- The Backup Exec System Recovery Manager database is not preserved. Instead, the new Backup Exec System Recovery 2010 Management Solution database is re-populated with client computer data as each one is brought under backup management.

http://entsupport.symantec.com/umi/V-306-5

Upgrading from Backup Exec System Recovery Solution 8.5 to Backup Exec System Recovery 2010 Management Solution

If you are upgrading from Backup Exec System Recovery Solution 8.5 to Backup Exec System Recovery 2010 Management Solution, all configurations, policies, tasks, and recovery points are preserved.

http://entsupport.symantec.com/umi/V-306-5

About installing Backup Exec System Recovery 2010 Management Solution

You can install Backup Exec System Recovery 2010 Management Solution using one of the following methods:

- Symantec Installation Manager
  You use the Symantec Installation Manager to install Backup Exec System Recovery 2010 Management Solution on the Notification Server. 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.
  At a minimum, you must install this product on a computer that runs Windows Server/Enterprise Server 2003.
  For detailed installation instructions, please refer to the *Symantec Management Platform Installation Guide*.
- The Backup Exec System Recovery 2010 Management Solution product DVD
  During the installation, the following components may be installed if they do not already exist:
  - Microsoft .NET Framework 3.5.
  - Microsoft SQL Server 2005 Express Edition. This software is included on the Backup Exec System Recovery 2010 Management Solution media. Symantec recommends that you install Microsoft SQL Server on a computer separate from the one on which you install Backup Exec System Recovery 2010 Management Solution
  - Symantec Installation Manager.

  Depending on the product DVD you have, you can install the following products:
  - Backup Exec System Recovery 2010 Management Solution
  - Backup Exec System Recovery 2010
  - Backup Exec System Recovery 2010 Linux Edition
  - LightsOut Restore 2010
  - Altiris Agent for UNIX, Linux and Mac

See "System requirements for Backup Exec System Recovery 2010 Management Solution " on page 29.

See "Installing Backup Exec System Recovery 2010 Management Solution " on page 30.

System requirements for Backup Exec System Recovery 2010 Management Solution

The computer on which you install and use Backup Exec System Recovery 2010 Management Solution must meet the following minimum system requirements.

See "About installing Backup Exec System Recovery 2010 Management Solution" on page 28.

Table 2-1 Backup Exec System Recovery 2010 Management Solution system requirements

Component	Requirements
Processor	Intel® Pentium® 4 CPU 2.0 GHz or faster
RAM	2 GB or more
Available disk space	20 GB or more
Software	The following must be installed on the computer on which you want to installBackup Exec System Recovery 2010 Management Solution: ■ 32-bit versions of Microsoft Windows Server 2003 R2, Enterprise Edition, or Standard Edition ■ Microsoft SQL Server 2005 Express Edition is included on the Backup Exec System Recovery 2010 Management Solution media. Symantec recommends that you install Microsoft SQL Server on a computer separate from the one on which you install Backup Exec System Recovery 2010 Management Solution to avoid computer performance issues. ■ Microsoft Internet Information Services ■ Microsoft .NET Framework 3.5 ■ Microsoft ASP.NET ■ Microsoft Internet Explorer 7 or later ■ Microsoft Silverlight 3.0 or later ■ Symantec Installation Manager ■ Symantec Management Platform **Note:** Installation of Backup Exec System Recovery 2010 Management Solution is not supported on encrypted file systems.
Internet access	High speed Internet access is recommended at the computer where you install Backup Exec System Recovery 2010 Management Solution.
DVD ROM drive	Required for installation.

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

Installing Backup Exec System Recovery 2010 Management Solution

The Symantec Management Platform requires a Microsoft SQL Server database. SQL Server Express 2005 database is already included on the product DVD. 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 "About installing Backup Exec System Recovery 2010 Management Solution" on page 28.

See "About preparing to manage the backups of client computers" on page 42.

To install the Backup Exec System Recovery 2010 Management Solution

1. Log on to your computer by using either the Administrator account or an account that has administrator privileges.
2. Do one of the following:

If you install Backup Exec System Recovery 2010 Management Solution from the Symantec Installation Manager	■ On the Notification Server computer, click **Start > All Programs > Altiris > Symantec Installation Manager > Symantec Installation Manager**. ■ Click **Install new products**. ■ Continue with step 10.
If you install Backup Exec System Recovery 2010 Management Solution from the product DVD	Continue to the next step below.

3. Insert the Backup Exec System Recovery 2010 Management Solution DVD into the DVD drive of the computer.
4. In Windows Explorer, in the left pane, click **My Computer**.
5. In the right pane, double-click the name of the product DVD to start the installation.
6. In the **Backup Exec System Recovery 2010 Management Solution Installation Welcome** panel, click **Next**.

7 Do one of the following:

To create a new SQL Server Express instance	Click **Create a new SQL Server Express instance**. The name of the new instance is SQLExpress. Write down this name. You must enter it later in the installation process when you are prompted to specify the Microsoft SQL Server name. The Symantec Management Platform uses this SQL Server instance.
To use an existing SQL Server instance	Click **Use an existing SQL Server Instance**. Symantec does not recommend using an instance of SQL Server Express that hosts another application. Uninstalling the other application can render the Symantec Management Platform configuration management database unusable. In addition, other applications may use some SQL Server Express settings that may be incompatible with the Symantec Management Platform. If you decide to use an existing SQL Server instance, you are prompted to select it later in the installation process.

8 Click **Next**.

The Backup Exec System Recovery 2010 Management Solution program files are installed.

9 Do one of the following:

If the Symantec Installation Manager is not installed	The **Symantec Installation Manager - Install Package** dialog box appears. Do the following: ■ Click **Continue**. ■ Specify the folder where you want to extract the Symantec Installation Manager files. ■ Click **OK** to extract the Symantec Installation Manager files. ■ Following the extraction, click **OK** again to start the Symantec Installation Manager Setup wizard. ■ In the **Welcome** panel, click **Next**. ■ Read the end-user license agreement, check **I accept the terms in the license agreements**, and then click **Next**. ■ Click **Being Install**. Symantec Installation Manager is installed. ■ Click **Finish** to launch the Symantec Installation Manager.. ■ In the Backup Exec System Recovery 2010 Management Solution Installation Finish panel, click **Finish**.
If the Symantec Installation Manager is installed.	The Symantec Installation Manager is launched. Continue with the next step below.

10 On the **Install New Products** panel, in the **Filter** drop-down list, select **None**.

11 Select the following products:

- Backup Exec System Recovery 2010 Management Solution
- Backup Exec System Recovery 2010 Installer
- Backup Exec System Recovery 2010 Linux Management Solution (only required if you intend to back up Linux-based computers)
- Backup Exec System Recovery 2010 LightsOut Restore
- Symantec Management Platform SP2
- Altiris Agent for UNIX, Linux and Mac (only required if you intend to back up Linux-based computers)

The Symantec Installation Manager may automatically select additional software components that are required to complete the installation.

12 Click **Review selected products**.

13 In the **Selected Products and Features** panel, review the list of selected products, and then click **Next**.

14 In 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 install readiness check to make sure you have met all computer requirements. The results of the install readiness check appear in the **Install Readiness Check** panel.

15 In 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, install the missing software component, and then start the Backup Exec System Recovery 2010 Management Solution installation again.

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

Check mark	The requirement 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.

16 Click **Next**.

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

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

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

20 In the **installation** panel, click **Finish** to launch the Symantec Management Console.

Post-installation tasks

Some of the post-installation tasks to get you started include the following:

- See "About the Backup Exec System Recovery 2010 Management Solution Home page" on page 38.
- See "About installing the Backup Exec System Recovery Plug-in on client computers" on page 45.
- See "About installing Backup Exec System Recovery 2010, Backup Exec System Recovery 2010 Linux Edition, or LightsOut Restore 2010 on client computers " on page 49.
- See "Creating a basic backup policy" on page 88.

Uninstalling Backup Exec System Recovery 2010 Management Solution

You can uninstall Backup Exec System Recovery 2010 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.

If you uninstall Backup Exec System Recovery 2010 Management Solution, be aware that Backup Exec System Recovery is not uninstalled from any managed client computers that you added to the console.

To uninstall Backup Exec System Recovery 2010 Management Solution

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

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

3 Select **Backup Exec System Recovery 2010 Management Solution** in the Installed products list.

4 Click **Uninstall**.

5 Click **Yes**.

Chapter 3

Getting started with Backup Exec System Recovery 2010 Management Solution

This chapter includes the following topics:

■ About managing Backup Exec System Recovery license policies

About the Backup Exec System Recovery 2010 Management Solution Home page

The solution's Home page provides a visual overall status of servers and desktop computers (the computers must have Backup Exec System Recovery Plug-in and Backup Exec System Recovery installed to show up on the Home page). Those computers may or may not be protected by Backup Exec System Recovery. Actual data regarding computer incidents populates this page.

You can edit the solution's Home page by adding or deleting Web parts. You can add or delete Web parts from other solutions, Backup Exec System Recovery 2010 Management Solution, or from default Web parts that the Symantec Management Console includes.

Table 3-1 describes the product's Web parts that you can delete from or add to the solution's portal page.

Table 3-1 Backup Exec System Recovery 2010 Management Solution Home page information

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

Table 3-1 Backup Exec System Recovery 2010 Management Solution Home page information *(continued)*

Web part name	Description
Backup Status	Filters backup status results by collection. Client computer status types include the following: ■ Backed up The number of managed client computers that have made a recovery point of all drives (set to report full status) in the last 30 days. And, the client computers have not missed the last scheduled backup . Client computers can be considered "Backed up" without having an assigned backup policy 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 The number of managed client computers that have a backup policy assigned but it has not been 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 older, the recovery points do not contain the latest versions of files or folders. ■ At Risk The number of managed client computers that have no recovery points available for the reported drives. A client computer at risk can be recovered if the volumes are set to backup. For example, suppose you have a C:\, D:\, and E:\ volume on a client computer, but only a backup of C:\ exists. While Backup Exec System Recovery 2010 Management Solution shows the client computer at risk, you can still recover the C:\ volume. ■ Not Reporting The number of managed client computers that have not reported back to the Backup Exec System Recovery 2010 Management Solution server. The computers must report within a set time interval regardless of whether or not any policies are assigned to them. This error is often caused by network connectivity issues, like the computer or laptop not being connected to the network or being turned off.
Computer Statistics	Displays a summary of all of the managed client computers that have a supported version of Backup Exec System Recovery installed. The information is sorted by servers and desktops. You can click Desktops or Servers in the legend to open a detailed view of the managed client computers within that group.

Table 3-1 Backup Exec System Recovery 2010 Management Solution Home page information *(continued)*

Web part name	Description
Destination Storage	Displays a table summary of all defined local and network destinations for recovery points. The table displays, among other things, the destination type and path to the destination.
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 if the backup 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 Backup Exec System Recovery 2010 Management Solution. It also includes a link to Help that lists 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 The number of managed client computers that have a current license assigned to them. ■ Not Licensed The number of managed client computers on which an expired trial version of Backup Exec System Recovery is installed or on which no license was activated. ■ Trial License The number of managed client computers that have a trial version of Backup Exec System Recovery installed. You can click a license status in the legend to open a detailed view of the client computers within that status.
Operating System Statistics	Displays a summary of all of the managed client computers that have a supported version of Backup Exec System Recovery installed. The information is sorted by a particular version of Windows. You can click an operating system in the legend to open a detailed view of the managed client computers within that group.

Table 3-1 Backup Exec System Recovery 2010 Management Solution Home page information *(continued)*

Web part name	Description
ThreatCon Response Level	ThreatCon is 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. ThreatCon levels ■ Level 1 No discernable security threats exist. ■ Level 2 Security threats could 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.

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

See "Starting Backup Exec System Recovery 2010 Management Solution" on page 41.

Starting Backup Exec System Recovery 2010 Management Solution

You can start Backup Exec System Recovery 2010 Management Solution using several different methods.

See "About the Backup Exec System Recovery 2010 Management Solution Home page" on page 38.

To start Backup Exec System Recovery 2010 Management Solution

1 Do one of the following:

- On the computer where Notification Server is installed, on the Windows taskbar, click **Start > All Programs > Altiris > Solutions > Backup Exec System Recovery 2010 Management Solution**.
- On the computer where Notification Server is installed, on the Windows taskbar, click **Start > All Programs > Altiris > Symantec Management Console 7.0**.

In the Symantec Management Console, on the Home menu, click **Backup and Recovery > Backup Exec System Recovery 2010 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 > Backup Exec System Recovery 2010 Management Solution**.

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

Sending feedback

Please take a moment to share your feedback and comments with Symantec regarding Backup Exec System Recovery 2010 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 Backup Exec System Recovery 2010 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**.

About 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 configuration takes place and certain components are installed to the resource targets you want.

- Discover computers on the network
  See "Discovering client computers on the network" on page 43.
- Install the Altiris Agent
  See "Installing the Altiris Agent on client computers" on page 44.
- Install the Backup Exec System Recovery Plug-in or the Backup Exec System Recovery Linux Edition Plug-in

See "Installing the Backup Exec System Recovery Plug-in on computers" on page 46.

- Install Backup Exec System Recovery 2010, Backup Exec System Recovery 2010 Linux Edition, or LightsOut Restore 2010
  See "About installing Backup Exec System Recovery 2010, Backup Exec System Recovery 2010 Linux Edition, or LightsOut Restore 2010 on client computers " on page 49.

After the necessary agent and plug-in are deployed, you can define and assign backup policies to resource targets.

See "Creating a basic backup policy" on page 88.

Discovering client computers on the network

Before you can use Backup Exec System Recovery 2010 Management Solution to manage the back ups 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 Altiris Agent on them.

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

See "Installing the Altiris Agent on client computers" on page 44.

See "About preparing to manage the backups of client computers" on page 42.

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 Backup Exec System Recovery 2010 Management Solution 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 Backup Exec System Recovery 2010 Management Solution 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 Altiris Agent on client computers

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

The amount of time required to install the Altiris Agent varies depending on the number of computers on which you want to install it.

See "About installing the Backup Exec System Recovery Plug-in on client computers" on page 45.

See "About preparing to manage the backups of client computers" on page 42.

To install the Altiris Agent on client computers

1. On the Backup Exec System Recovery 2010 Management Solution Home tab, in the Getting Started Web part, click **Install the Altiris Agent**.
2. Do one of the following:

To install the Altiris Agent on computers where Backup Exec System Recovery for Windows will run	Do the following: ■ Select one or more computers. ■ On the **Install Altiris Agent** tab, click **Installation Settings**. ■ In the **Altiris Agent Installation Options** panel, select the options you want to apply to the agent. ■ Click **OK**. ■ Click **Install Altiris Agent**. Review the installation options and make changes if necessary. ■ Click **Proceed with Install**.

To install the Altiris Agent on computers where Backup Exec System Recovery 2010 Linux Edition will run	Do the following: ■ Select one or more computers. ■ On the **Install Altiris 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 Altiris Agent**. ■ Click **OK** to proceed with the installation.

About installing the Backup Exec System Recovery Plug-in on client computers

Using Symantec Management Platform policies, you can install the Backup Exec System Recovery Plug-in or the Backup Exec System Recovery Linux Edition Plug-in to computers on your network. You can also use policies to upgrade (excluding Backup Exec System Recovery Linux Edition) and uninstall the plug-in.

See "Installing the Backup Exec System Recovery Plug-in on computers" on page 46.

Note: To use roll out policies, the Altiris 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 required to install Backup Exec System Recovery varies depending on the number of computers on which you want to install it.

See "About preparing to manage the backups of client computers" on page 42.

Table 3-2 describes the Backup Exec System Recovery Plug-in policies that are included with your installation of Backup Exec System Recovery 2010 Management Solution.

Table 3-2 Predefined Backup Exec System Recovery Plug-in policies

Backup Exec System Recovery Plug-in policy	Description
Backup Exec System Recovery Plug-in Backup Exec System Recovery Linux Edition Plug-in	A software delivery policy that is installed on resource targets with no Backup Exec System Recovery Plug-in installed. You can also use the uninstall program with the software delivery policy to uninstall the plug-in. The Backup Exec 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 backup policies or Independent Backup tasks, and backup status). That information is published back to Notification Server. The Backup Exec System Recovery Plug-in accepts and applies backup configuration changes from Notification Server.
Backup Exec System Recovery Plug-in Upgrade	A software delivery policy that upgrades the previously installed Backup Exec System Recovery Plug-in on resource targets requiring an upgrade to the plug-in.
Backup Exec System Recovery Plug-in Uninstall Backup Exec System Recovery Linux Edition Plug-in Uninstall	A software delivery policy that uninstalls the previously installed Backup Exec System Recovery Plug-in on resource targets with the plug-in.

Installing the Backup Exec System Recovery Plug-in on computers

Using Symantec Management Platform policies, you can deploy the Backup Exec System Recovery or Backup Exec System Recovery Linux Edition Plug-in to computers on your network. You can also use policies to upgrade and uninstall the plug-in.

The amount of time required to install Backup Exec System Recovery varies depending on the number of computers on which you want to install it.

See "About installing the Backup Exec System Recovery Plug-in on client computers" on page 45.

To uninstall the Backup Exec System Recovery Plug-in from client computers

To install the Backup Exec System Recovery Plug-in on client computers

1 Do one of the following:

To install the Backup Exec System Recovery for Windows Plug-in	Do one of the following: ■ On the Backup Exec System Recovery 2010 Management Solution **Home** tab, in the **Getting Started** Web part, click **Install the plug-in for Backup Exec System Recovery**. In the Install Backup Exec System Recovery Plug-in panel, in the upper-right corner, make sure **On** is selected from the list to enable the software delivery policy. ■ On the Backup Exec System Recovery 2010 Management Solution **Packages and Policies** tab, in the **Install Policies** list in the left pane, under **Agent Plug-in**, click **Backup Exec System Recovery**. In the right pane, near the upper-right corner, make sure **On** is selected from the list to enable the software delivery policy.
To install the Backup Exec System Recovery Linux Edition Plug-in	Do the following: ■ On the Backup Exec System Recovery 2010 Management Solution **Packages and Policies** tab, in the **Install Policies** list in the left pane, under **Agent Plug-in**, click **Install Plug-in for Backup Exec System Recovery Linux**. ■ In the right pane, near the upper-right corner, click **On** to enable the software delivery policy.

2 Set the deployment options.

See "Deployment options" on page 48.

3 Click **Save changes**.

To uninstall the Backup Exec System Recovery Plug-in from client computers

1 Do one of the following:

To uninstall the Backup Exec System Recovery for Windows Plug-in	Do the following: ■ On the Backup Exec System Recovery 2010 Management Solution **Packages and Policies** tab, in the **Uninstall Policies** list in the left pane, under **Agent Plug-in**, click **Plug-in for Backup Exec System Recovery Uninstall**. ■ In the right pane, near the upper-right corner, make sure **On** is selected from the list to enable the software delivery policy.
To uninstall the Backup Exec System Recovery Linux Edition Plug-in	Do the following: ■ On the Backup Exec System Recovery 2010 Management Solution **Packages and Policies** tab, in the **Uninstall Policies** list in the left pane, under **Agent Plug-in**, click **Plug-in for Backup Exec System Recovery for Linux Uninstall**. ■ In the right pane, near the upper-right corner, click **On** to enable the software delivery policy.

2 Set the deployment options.

See "Deployment options" on page 48.

3 Click **Save changes**.

Deployment options

You can set various options during a deployment, upgrade, or uninstall.

See "Installing the Backup Exec System Recovery Plug-in on computers" on page 46.

Table 3-3 Deployment options

Options	Description
Program name	Identifies the name of the program that you want to run.

Table 3-3 Deployment options *(continued)*

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

About installing Backup Exec System Recovery 2010, Backup Exec System Recovery 2010 Linux Edition, or LightsOut Restore 2010 on client computers

Besides installing the predefined Backup Exec System Recovery Plug-in on computers, you also need to deploy installation packages of Backup Exec System Recovery or Backup Exec System Recovery Linux Edition. Optionally, you can also deploy installation packages of LightsOut Restore for the ability to recover drives remotely.

For complete system requirements for Backup Exec System Recovery 2010 (including LightsOut Restore) or Backup Exec System Recovery 2010 Linux Edition, see the respective user's guide in PDF, available on the Backup Exec System Recovery 2010 Management Solution DVD.

See the *Altiris Software Management Solution User's Guide* and the *Altiris Software Management Framework User's Guide* for more information about software delivery on the Symantec Management Platform.

Note: Backup Exec System Recovery 2010 Management Solution currently supports only the Independent Backup task (one-time backup) for Linux-based computers with Backup Exec System Recovery Linux Edition installed. Recovery of Linux computers must also occur on the local computer. For more information about using Backup Exec System Recovery Linux Edition locally on a computer, see the *Backup Exec System Recovery 2010 User's Guide Linux Edition*.

See "Creating an Independent Backup task" on page 115.

See "Installing Backup Exec System Recovery 2010 or Backup Exec System Recovery 2010 Linux Edition on client computers" on page 50.

See "Configuring and installing LightsOut Restore on client computers" on page 55.

See "Adding or deleting Backup Exec System Recovery license policies" on page 79.

See "Assigning or unassigning Backup Exec System Recovery licenses" on page 80.

See "Uninstalling Backup Exec System Recovery-related products from the Symantec Management Platform" on page 65.

Installing Backup Exec System Recovery 2010 or Backup Exec System Recovery 2010 Linux Edition on client computers

You can deploy Backup Exec System Recovery 2010, 8.5, 8.0 or Backup Exec System Recovery 2010 Linux Edition software delivery packages to computers. You can also choose to install Backup Exec System Recovery with a user interface to allow user interaction with the software from the desktop of the client computer.

For complete system requirements for Backup Exec System Recovery 2010 or Backup Exec System Recovery 2010 Linux Edition, see the respective user's guide in PDF, available on the Backup Exec System Recovery 2010 Management Solution DVD.

Note: Backup Exec System Recovery 2010 Management Solution currently supports only the Independent Backup task (one-time backup) for Linux-based computers with Backup Exec System Recovery Linux Edition installed. Recovery of Linux computers must also occur on the local computer. For more information about using Backup Exec System Recovery Linux Edition locally on a computer, see the *Backup Exec System Recovery 2010 User's Guide Linux Edition*.

See "Creating an Independent Backup task" on page 115.

Note: Following the installation of Backup Exec System Recovery 2010 for Windows, the client computer is automatically restarted. The restart is necessary to ensure that the necessary Backup Exec System Recovery services are started and running. A restart is not necessary following the installation of Backup Exec System Recovery 2010 Linux Edition.

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

See "About installing Backup Exec System Recovery 2010, Backup Exec System Recovery 2010 Linux Edition, or LightsOut Restore 2010 on client computers " on page 49.

See "Installing Backup Exec System Recovery 2010 or Backup Exec System Recovery 2010 Linux Edition on client computers" on page 50.

To install Backup Exec System Recovery 2010 or Backup Exec System Recovery 2010 Linux Edition on client computers

1. Do one of the following:
   - If you chose to install the **Backup Exec System Recovery 2010 Package** or the **Backup Exec System Recovery 2010 Linux Edition Package** at the time you installed Backup Exec System Recovery 2010 Management Solution, go to step 3.
   - If you chose not to install the **Backup Exec System Recovery 2010 Package** or the **Backup Exec System Recovery 2010 Linux Edition Package** at the time you installed Backup Exec System Recovery 2010 Management Solution, continue to the next step.
2. Use the Symantec Installation Manager to install the **Backup Exec System Recovery 2010 package** or the **Backup Exec System Recovery 2010 Linux Edition package**.
3. Do one of the following:

To install Backup Exec System Recovery 2010 that includes a user interface that is accessible from the desktop on client computers	Do one of the following: ■ On the Backup Exec System Recovery 2010 Management Solution **Home** tab, in the **Getting Started** Web part, click **Install Backup Exec System Recovery**. In the Install Backup Exec System Recovery panel, in the upper-right corner, click **On** to enable the software delivery policy. ■ On the Backup Exec System Recovery 2010 Management Solution **Packages and Policies** tab, in the **Install Policies** list in the left pane, under **Backup Exec System Recovery 2010**, click **Install With User Interface**. In the right pane, near the upper-right corner, click **On** to enable the software delivery policy.
To install Backup Exec System Recovery 2010 that does not include a user interface on the desktop of client computers	Do the following: ■ On the Backup Exec System Recovery 2010 Management Solution **Packages and Policies** tab, in the **Install Policies** list in the left pane, under **Backup Exec System Recovery 2010**, click **Install Without User Interface**. ■ In the right pane, near the upper-right corner, click **On** to enable the software delivery policy.
To install Backup Exec System Recovery 2010 Linux Edition	Do the following: ■ On the Backup Exec System Recovery 2010 Management Solution **Packages and Policies** tab, in the **Install Policies** list in the left pane, under **Backup Exec System Recovery 2010 Linux Edition**, click **Install Without User Interface**. ■ In the right pane, near the upper-right corner, click **On** to enable the software delivery policy.

4 Set the deployment options.

See "Deployment options" on page 48.

5 Click **Save changes**.

To install Backup Exec System Recovery 8.5 or 8.0 on client computers

1 Insert the Backup Exec System Recovery 8.5 or 8.0 product CD into the media drive of the computer on which Notification Server is installed.

2 Browse to the root of the Backup Exec System Recovery CD.

3 Copy the Install folder.

4 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\Backup Exec System Recovery Management Solution\Web\SoftwareDelivery\BESR\8.5\. If you copy the Install folder from Backup Exec System Recovery 8.0, paste it in the 8.0 folder.

5 On the Backup Exec System Recovery 2010 Management Solution **Manage Tasks** tab, in the left pane, expand the **Update Packages** list.

6 Under **Backup Exec System Recovery**, under **8.5** or **8.0**, click **Install Without User Interface Package** or **Install With User Interface Package**.

7 In the bottom of right pane, click **Update Distribution Points** to make the Notification Server aware of the package location that you just added.

8 Do one of the following:

To install Backup Exec System Recovery 8.5 or 8.0 that includes a user interface that is accessible from the desktop on client computers	Do the following: ■ On the Backup Exec System Recovery 2010 Management Solution **Packages and Policies** tab, expand the **Install Policies** list in the left pane. ■ Under **Backup Exec System Recovery**, under 8.5 or 8.0, click **Install With User Interface**. ■ In the right pane, near the upper-right corner, click **On** to enable the software delivery policy.

To install Backup Exec System Recovery 8.5 or 8.0 that does not include a user interface on the desktop of client computers	Do the following: ■ On the Backup Exec System Recovery 2010 Management Solution **Packages and Policies** tab, expand the **Install Policies** list in the left pane. ■ Under **Backup Exec System Recovery**, under 8.5 or 8.0, click **Install Without User Interface**. ■ In the right pane, near the upper-right corner, click **On** to enable the software delivery policy.

9 Set the deployment options.

See "Deployment options" on page 48.

10 Click **Save changes**.

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

Uninstalling Backup Exec System Recovery-related products and components from client computers

You can use uninstall policies in Backup Exec System Recovery 2010 Management Solution to remove the following from client computers:

- Backup Exec System Recovery Plug-in
- Backup Exec System Recovery 2010 Linux Edition Plug-in
- Backup Exec System Recovery 2010, 8.5, or 8.0
- Backup Exec System Recovery 2010 Linux Edition
- LightsOut Restore 2010, 8.5, or 8.0

See "Uninstalling Backup Exec System Recovery-related products from the Symantec Management Platform" on page 65.

See "Installing Backup Exec System Recovery 2010 or Backup Exec System Recovery 2010 Linux Edition on client computers" on page 50.

To uninstall Backup Exec System Recovery or Backup Exec System Recovery Linux Edition from client computers

1 Do one of the following:

To uninstall the Backup Exec System Recovery	Do one of the following: ■ On the Backup Exec System Recovery 2010 Management Solution **Packages and Policies** tab, in the **Uninstall Policies** list in the left pane, under Backup Exec System Recovery, click the version you want. ■ In the right pane, near the upper-right corner, make sure **On** is selected from the list to enable the software delivery policy.
To uninstall the Backup Exec System Recovery Linux Edition	Do the following: ■ On the Backup Exec System Recovery 2010 Management Solution **Packages and Policies** tab, in the **Uninstall Policies** list in the left pane, under **Backup Exec System Recovery Linux Edition**, click **2010 Uninstall**. ■ In the right pane, near the upper-right corner, click **On** to enable the software delivery policy.

2 Set the deployment options.

See "Deployment options" on page 48.

3 Click **Save changes**.

Configuring and installing LightsOut Restore on client computers

If you followed the instructions for installing Backup Exec System Recovery 2010 Management Solution, then LightsOut Restore 2010 was also installed and made available in the solution.You can configure and install LightsOut Restore 2010 on client computers. To install LightsOut Restore 8.5 or 8.0, you must use the Symantec Recovery Disk CD or a custom Symantec Recovery Disk CD that you have created yourself.

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 GB of memory on the client computer to run properly.

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

See "About installing Backup Exec System Recovery 2010, Backup Exec System Recovery 2010 Linux Edition, or LightsOut Restore 2010 on client computers " on page 49.

To uninstall LightsOut Restore from client computers

See "About LightsOut Restore on computers" on page 158.

To configure and install LightsOut Restore on client computers

1 Do one of the following:

To install LightsOut Restore 2010	Skip to step 2.
To install LightsOut Restore version 8.5 or 8.0	Copy LightsOut Restore from Symantec Recovery Disk to the default package location on the Notification Server 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 of 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 Backup Exec System Recovery 2010 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 8.5 is the following: c:\Program Files\Altiris\Backup Exec System Recovery Management Solution\web\softwaredelivery\lor\8.5\ The default location for LightsOut Restore 8.0 is the following: c:\Program Files\Altiris\Backup Exec System Recovery Management Solution\web\softwaredelivery\lor\8.0\ ■ Continue with the next step.

For purposes of this task, the remaining steps assume that you are installing LightsOut Restore 2010. If you install LightsOut Restore 8.5 or 8.0 instead, adjust the steps for the correct version.

2 On the Backup Exec System Recovery 2010 Management Solution **Packages and Policies** tab, expand the **Install Policies** list in the left pane.

3 Under **LightsOut Restore**, under **2010**, click **Configure Policy**.

4 In the right pane, set the configuration options.

See "LightsOut Restore configuration options" on page 57.

5 In the right pane, near the upper-right corner, click **On** to enable the software delivery policy.

6 Set the deployment options.

See "Deployment options" on page 48.

7 Click **Save changes**.

To uninstall LightsOut Restore from client computers

1 On the Backup Exec System Recovery 2010 Management Solution **Packages and Policies** tab, in the **Uninstall Policies** list in the left pane, click the LightsOut Restore version you want.

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

3 Set the deployment options.

See "Deployment options" on page 48.

4 Click **Save changes**.

LightsOut Restore configuration options

You can set various configuration options that affect how you use LightOut Restore.

Note: The LightsOut Restore feature requires a minimum of 1 GB of memory on the client computer to run properly.

See "Configuring and installing LightsOut Restore on client computers" on page 55.

Table 3-4 LightsOut Restore configuration options

Option	Description
Use the default language that is specified in Symantec Recovery Disk (English)	Uses English as the display language in the recovery environment.

Table 3-4 LightsOut Restore configuration options *(continued)*

Option	Description
Choose language	Uses the display language that you prefer to use in the recovery environment.
Time Zone	Runs the recovery environment in the specified time zone. **Note:** This option is not available in LightsOut Restore 8.0.
Keyboard layout	Use the specified keyboard layout while in the recovery environment. **Note:** This option is not available in LightsOut Restore 8.0.
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. **Note:** This option is not available in LightsOut Restore 8.0.
Automatically start network services	Starts 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 no DHCP is server (or the DHCP server is not available) when you recover.

Table 3-4 LightsOut Restore configuration options *(continued)*

Option	Description
Automatically start Symantec pcAnywhere	Allows the Symantec pcAnywhere thin host to start automatically when you start the recovery environment (LightsOut Restore). This option is useful for troubleshooting a system recovery.

Updating the settings of a package

The various packages available in Backup Exec System Recovery 2010 Management Solution are already pre-defined 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 on each package is contained in an XML file that is stored with the package. This information must be updated each time you edit 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 to update the package information on all of its distribution points immediately.

To update the settings of package

1. On the Backup Exec System Recovery 2010 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	See "Package tab settings" on page 60.
Programs	See "Programs tab settings" on page 61.
Package Servers	See "Package Servers tab settings" on page 63.
Advanced	See "Advanced tab settings" on page 64.

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

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

Package tab settings

The Package tab lets you specify basic package information such as the package name, version, and source file location.

See "Updating the settings of a package" on page 59.

Table 3-5 Package tab settings

Setting	Description
Name	The package name.
Description	A user-friendly description of the package.
Publisher	The package publisher.
Language	The package language.
Version	The package version.
Package Source	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	The location at which the package is stored. This can be a local directory on the Notification Server computer, a UNC path, or a URL location, depending on the package source option specified above.

Table 3-5 Package tab settings *(continued)*

Setting	Description
Package files will be deleted from the client computer if unused for	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

The Programs tab lets you configure the programs that are included in the package.

See "Updating the settings of a package" on page 59.

Table 3-6 Settings on the Programs tab

Setting	Description
Name	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	A user-friendly description of the selected program. This field is optional.
Command Line	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	The directory where files that are needed by the program are temporarily stored during deployment. 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, but typically a zero value is used for success and a non-zero value for failure. These fields are optional.

Table 3-6 Settings on the Programs tab *(continued)*

Setting	Description
Estimated Disk Space	The estimated amount of disk space that the program requires to run on the target computer. The Altiris Agent ensures that at least one physical drive with the specified space is available before executing the program. This field is optional.
Estimated Run Time	The estimated time in minutes that the program requires to run on the target computer. This field is optional.
Terminate After	The time-out 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	The action that is performed when the program finishes running: ■ No action required ■ Restart computer ■ Log off user
Starting window	The status of the command window that runs the program on a managed computer: ■ Normal ■ Hidden ■ Minimized ■ Maximized
Run with rights	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 in the following box.
Program can run	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.

Table 3-6 Settings on the Programs tab *(continued)*

Setting	Description
Minimum connection speed	Specifies the minimum connection speed for software delivery programs to be executed. Before the program is run, the connection speed from the Altiris Agent to Notification Server is tested. If the connection speed is less than the specified minimum speed, the program will not run. The options are as follows: ■ No network connection required There is 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

The Package Servers tab lets you assign the package to the appropriate package servers and specify the location at which the package files are stored.

See "Updating the settings of a package" on page 59.

Table 3-7 Settings on the Package Servers tab

Setting	Description
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*\Altiris\Altiris Agent\Agents\SoftwareManagement\Software Delivery*package_GUID*\cache

Table 3-7 Settings on the Package Servers tab *(continued)*

Setting	Description
Assign packages to	Specifies the package servers to which the package is assigned. The options are as follows: ■ **All Package Servers** Assign the package to all package servers. ■ **Package Servers Individually** Assign the package to selected package servers. ■ **Package Servers by Site** Assign sites to packages from a list of sites that is configured 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** This assignment occurs when a task that requires the package is assigned to a resource target. All the computers that are identified by the resource target require 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

The Advanced tab lets you specify additional package settings. You can specify the agent display name and description, enable the sending of package status events to Notification Server, and specify an alternate download destination managed computers.

See "Updating the settings of a package" on page 59.

Table 3-8 Settings on the Advanced tab

Setting	Description
Agent display name	The package name to be displayed on the Altiris 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 end user. The name that is specified on the **Package** tab may make sense only to an administrator.
Agent display description	Agent display description to inform the end user. This description can be different than the package description that is specified on the **Package** tab. This setting lets you supply a package description that tells the end user what the package does on the managed computer.

Table 3-8 Settings on the Advanced tab *(continued)*

Setting	Description
Enable verbose reporting of Package Status events	Enable the sending of package status events to Notification Server. Disabling events for the package prevents Altiris Agents from sending AeX SWD Package events to Notification Server. The Notification Server Event Capture settings in the Global Altiris Agent Settings policy take precedence to the Enable Verbose Reporting setting here. Events are sent only if they are enabled in the Global Altiris 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. Copied package files are never deleted by the Altiris Agent. They are copied each time the task is run so, if the task is running on a recurring schedule, the files are copied repeatedly. This 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*\Altiris\Altiris Agent\Agents\SoftwareManagement\Software Delivery*package_GUID*\cache

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

You can uninstall Backup Exec System Recovery 2010 Management Solution or Backup Exec System Recovery-related products from the Symantec Management Platform by using Symantec Installation Manager. If you uninstall the Backup Exec System Recovery 2010 Management Solution, the solution and any other related installed Backup Exec System Recovery products are also uninstalled.

If you choose to uninstall Backup Exec System Recovery 2010 Management Solution, be aware that Backup Exec System Recovery, the Backup Exec System Recovery Plug-in, and LightsOut Restore are not uninstalled from any managed client computers that you added to the console.

To uninstall Backup Exec System Recovery and related components from client computers, you must use the Backup Exec System Recovery 2010 Management Solution. You should run the uninstall policies for the following products and components, in the following order:

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

See "Uninstalling Backup Exec System Recovery-related products and components from client computers" on page 54.

Following the uninstallation of the above items, you can use Symantec Installation Manager to uninstall Backup Exec System Recovery 2010 Management Solution.

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

1. Start Symantec Installation Manager.
2. In the **Installed Products** page, select the Backup Exec System Recovery 2010 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. In the **Uninstallation Complete** page, click **Finish**.

About the recovery point password store

For each backup policy or an 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.

When you create a backup policy or an Independent Backup task, any password you assign to the respective policy or task is automatically added to the password store.

See "Adding recovery point passwords to the password store" on page 67.

See "Removing all recovery point passwords from the password store" on page 67.

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.

When you create a backup policy or an Independent Backup task, any password you assign to the respective policy or task is automatically added to the password store.

See "About the recovery point password store" on page 66.

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

See "Creating an Independent Backup task" on page 115.

To add recovery point passwords to the password store

1. On the Backup Exec System Recovery 2010 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 text field, type a password that you have used in a backup policy or 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.

See "About the recovery point password store" on page 66.

To remove all recovery point passwords from the password store

1. On the Backup Exec System Recovery 2010 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 as seen 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 recovery point destination network credentials" on page 72.

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 72.

You can also select a computer and assign it the exclusive 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 73.

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 are backing up.

See "About managing recovery point destinations" on page 68.

See "About Offsite Copy" on page 100.

See "Configuring a Dedicated Offsite Copy task" on page 73.

To create default recovery point destinations

1. On the Backup Exec System Recovery 2010 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. In the middle pane, on the toolbar above the table, click **Create**.
4. Depending on the destination type you selected in the left pane, do one of the following:

Local	In the Backup Destinations panel, do the following: ■ 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 offsite destination by selecting it from the Offsite drop-down list in a backup policy. USB is not supported as an offsite location.

Network Shares	In 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 offsite destination by selecting it from the Offsite drop-down list in a backup policy.
FTP	In the Backup Destinations panel, do the following: ■ 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 offsite destination by selecting it from the Offsite drop-down list in a backup policy.

ESX	In 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** buttons 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** buttons 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. See "ESX Server Location options" on page 136.
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

5 Click **Apply**.

Editing recovery point destination network credentials

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 68.

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

To edit recovery point destination network credentials

1. On the Backup Exec System Recovery 2010 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 whose network credentials you want to edit.
4. In the middle pane, on the toolbar above the table, 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 119.

See "About managing recovery point destinations" on page 68.

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 Backup Exec System Recovery 2010 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 select a computer and assign it the exclusive 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 to process an entire offsite copy task.

See "About Offsite Copy" on page 100.

See "About managing recovery point destinations" on page 68.

To configure a dedicated Offsite Copy task

1 On the Backup Exec System Recovery 2010 Management Solution **Monitor Tasks** tab, right-click Backup Exec System Recovery Tasks, and then click **New > Task**.

2 In the Client Tasks tree, click **Backup Exec 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:

- In the **Offsite Destination** drop-down list, select the destination where you want the recover point sets copied to.
- Select **Create new destination**, and then specify local folder path, UNC path to a network share, or an FTP path.

If you typed a UNC path or an FTP path, 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:

- Click **New Schedule**.
  Click **Now** or click **Schedule** at the bottom of the panel to run the task as soon as possible.
- 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

Backup Exec System Recovery 2010 Management Solution includes numerous predefined filters that you can use to roll out Backup Exec System Recovery policies to client computers.

Table 3-9 describes a few of the predefined filters that are installed with Backup Exec System Recovery 2010 Management Solution.

Table 3-9 Predefined filters

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

Table 3-9 Predefined filters *(continued)*

Filter	Description
Linux	Linux filters include the following: ■ Computers with Backup Exec System Recovery 2010 Linux Edition installed ■ Red Hat Enterprise Linux Server 5 with Backup Exec System Recovery 2010 Linux Edition Plug-in installed ■ SUSE Linux Enterprise Server 10 with Backup Exec System Recovery 2010 Linux Edition Plug-in installed
All computers with Backup Exec System Recovery installed	Lists the managed client computers that have Backup Exec System Recovery 2010, 8.5, 8.0, or Backup Exec System Recovery 2010 Linux Edition installed.
Windows computers with LightsOut Restore installed	Lists the managed Windows client computers that have LightsOut Restore 2010 installed.

When you are in the Manage Tasks tab of Backup Exec System Recovery 2010 Management Solution, you can filter the displayed results in the table. You use the **Filter results** bar directly above the table in the middle pane. If desired, 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 allowing you to get to specific data quickly.

See "Viewing Backup Exec System Recovery 2010 Management Solution filters" on page 75.

See "Viewing the filters and policies that are assigned to a client computer" on page 76.

See "Adding a filtered results path in the Manage Tasks tab to Favorites" on page 77.

Viewing Backup Exec System Recovery 2010 Management Solution filters

You can view a variety of predefined Backup Exec System Recovery 2010 Management Solution filters.

See "About viewing filters" on page 74.

To view Backup Exec System Recovery 2010 Management Solution filters

1. In the Symantec Management Console, on the toolbar, click **Manage > Filters**.
2. In the Filters tree, click **Computer Filters > Backup Exec 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 74.

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 > Backup Exec 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 Backup Exec System Recovery 2010 Management Solution

1. On the Backup Exec System Recovery 2010 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:
   - Under **Group**, click a computer group name.
   - Click **Computers**.
     If necessary, in the middle pane, use the **Filter results** bar above the table 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 above the table.

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.

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

1 On the Backup Exec System Recovery 2010 Management Solution **Manage Tasks** tab, in the left pane, select any specific filter.

2 In the middle pane, above the data table, on the **Filter results** bar, 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 managing Backup Exec System Recovery license policies

You can add or delete Backup Exec System Recovery license policies. When you add a license policy, the information that is found in a license key is stored in the Backup Exec System Recovery 2010 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 any resource target with an unlicensed version or trial version of Backup Exec System Recovery installed.

See "Adding or deleting Backup Exec System Recovery license policies" on page 79.

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

After you add a license policy, you can assign it to any resource target that has an unlicensed version or trial version of Backup Exec System Recovery installed. When you assign licenses, you activate Backup Exec System Recovery on the client computers and remove the 60-day trial.

Unassigning licenses from client computers returnsBackup Exec System Recovery to a 60-day trial version. If you choose to delay installation of the license, all features in Backup Exec 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 Backup Exec 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.
  Backup Exec 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 Backup Exec System Recovery 2010 Management Solution database.

See "Assigning or unassigning Backup Exec System Recovery licenses" on page 80.

You can review the license status of Backup Exec System Recovery on computers by using the Backup Exec System Recovery 2010 Management Solution Home tab.

Note: A computer is considered managed by Backup Exec System Recovery 2010 Management Solution when the Altiris Agent, Backup Exec System Recovery Plug-in, and Backup Exec System Recovery are installed.

Table 3-10 describes the different license status information that is available

Table 3-10 Backup Exec System Recovery license status

Backup Exec System Recovery license status	Description
Licensed	The number of computers that have a current license assigned. Computers with Backup Exec System Recovery Linux Edition do not require a license and therefore always have the status of Licensed.
Not licensed	The number of computers on which an expired trial version of Backup Exec System Recovery is installed or on which no license was activated.
Trial licensed	The number of computers that have a trial version of Backup Exec System Recovery installed.

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

Adding or deleting Backup Exec System Recovery license policies

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

Note: Computers with Backup Exec System Recovery Linux Edition do not require a license and therefore always have the status of Licensed.

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

To add Backup Exec System Recovery license policies

1. On the Backup Exec System Recovery 2010 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 you want to associate with the Backup Exec System Recovery license policy.
5. Enter a valid Backup Exec System Recovery license key.
6. Click **Save changes**.
7. You may need to click **Refresh** on the table filter toolbar to see the changes.

To delete Backup Exec System Recovery license policies

1. On the Backup Exec System Recovery 2010 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.
6. You may need to click **Refresh** on the table filter toolbar to see the changes.

Assigning or unassigning Backup Exec System Recovery licenses

You can assign or unassign Backup Exec System Recovery licenses to or from computers.

Note: Computers with Backup Exec System Recovery Linux Edition do not require a license and therefore always have the status of Licensed.

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

To assign Backup Exec System Recovery licenses to client computers

1. On the Backup Exec System Recovery 2010 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 Backup Exec 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**.
8. You may need to click **Refresh** on the table filter toolbar to see the changes.

To unassign Backup Exec System Recovery licenses from client computers

1. On the Backup Exec System Recovery 2010 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 > OK**.
   - On the tables's toolbar, click **Disable**.
5. You may need to click **Refresh** on the table filter toolbar to see the changes.

Checking the license status of Backup Exec System Recovery on client computers

You can review the license status of Backup Exec System Recovery on computers by using the Backup Exec System Recovery 2010 Management Solution portal.

A computer is considered managed by Backup Exec System Recovery 2010 Management Solution when the Altiris Agent, Backup Exec System Recovery Plug-in, and Backup Exec System Recovery are installed.

Note: Computers with Backup Exec System Recovery Linux Edition do not require a license and therefore always have the status of Licensed.

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

To check the license status of Backup Exec System Recovery on client computers

1. On the Backup Exec System Recovery 2010 Management Solution Home tab, in the upper-right corner, click **Edit**.
2. In the left pane, in the Web Parts tree, click **Backup Exec System Recovery 2010 Management Solution**.
3. Select **License Status**.
4. Click **Add** to add license status to the list of Web parts that are displayed on Backup Exec System Recovery Home page.

   If **Add** is dimmed (unavailable), the Web part is already added to the Backup Exec System Recovery 2010 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 Backup Exec System Recovery 2010 Management Solution Home tab, in the License Status Web part, click **Licensed**, **Not Licensed**, or **Trial License**.
To view license status from the Alerts and Failures on the Manage Tasks tab	Do the following: ■ On the Backup Exec System Recovery 2010 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 above the table in the right pane. There must be two or more rows in the table to enable the **Filter results** bar. If desired, you can add the filtered results path to the Favorites area in the left pane by clicking 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 (instead of an independent recovery point), 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 security settings (encryption and password protection) and search engine support for Google and Backup Exec Retrieve, and many other options that let you customize each backup according to your business needs.

While the client computer must be turned on to create a recovery point at the scheduled time, 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 Backup Exec System Recovery 2010 Management Solution portal page to check backup status information, or review the Recovery Points report in the Reports folder of the Backup Exec System Recovery 2010 Management Solution tree.

Note: Backup Exec System Recovery 2010 Management Solution supports recovery point files saved directly to a network hard disk or to a local hard disk on the client computer (including USB or FireWire drives). Backup Exec System Recovery 2010 Management Solution does not support saving recovery point files directly to CD or DVD.

See "Creating a basic backup policy" on page 88.

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.

Note: Backup policies apply to Windows-based computers only. If you want to backup a Linux-based computer using Backup Exec System Recovery Linux Edition, you must create a one-time backup task.

See "Creating an Independent Backup task" on page 115.

You can back up databases.

See "About backing up VSS-aware databases" on page 197.

See "About backing up non-VSS-aware databases" on page 199.

See "Ways to work with recovery points" on page 85.

See "Tips for creating recovery points" on page 86.

See "About backing up dual-boot systems" on page 87.

Ways to work with recovery points

Table 4-1 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 files are missing, the recovery point becomes invalid and you cannot restore the data.

Table 4-1 Types of scheduled recovery points

Type	Advantages and disadvantages
Recovery point set	■ A recovery point set is the same as an Independent recovery point except that it has incremental tracking enabled for the selected drive. ■ This type of backup creates a base recovery point with additional recovery points that 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. ■ If you use recovery point sets, 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 to the point in time that the fourth incremental 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.
Independent recovery point	■ 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 are recovery point sets. You can take an Independent recovery point of a drive (using a one-time backup task) even if that drive is tracked with a Recovery point set. See "Creating an Independent Backup task" on page 115. See "Deploying an existing backup policy as soon as possible" on page 117. ■ This backup type typically requires more storage space.

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 Backup Exec System Recovery 2010 Management Solution portal page.
- All backup policies are saved in the Backup Exec System Recovery 2010 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.
- Do not run a disk defragmentation program on the managed client computer when a recovery point is being created. 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, you should include both drives in the same backup policy. With Backup Exec System Recovery 2010 Management Solution, you can 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.
- You should avoid storing recovery points on the Backup Exec System Recovery 2010 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, or systems 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 it is bootable 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 for 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 if Backup Exec 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 Backup Exec System Recovery LightsOut Restore or Backup Exec 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 (instead of an independent recovery point), you can also specify that certain events, like logging on or off of a computer, create incremental recovery points.

Note: Backup policies apply to Windows-based computers only. If you want to backup a Linux-based computer using Backup Exec System Recovery Linux Edition, you must create a one-time backup task.

See "Creating an Independent Backup task" on page 115.

See "About backup policies" on page 83.

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

To create a basic backup policy

1. On the Backup Exec System Recovery 2010 Management Solution **Manage Tasks** tab, expand the **Backup Policies** list in the left pane.
2. In the left pane, select the type of recovery point that you want the backup policy to create.

Recovery Point Set	Schedule a base recovery point with additional recovery points that contain only incremental changes that were made to your computer since the previous recovery point. Incremental recovery points are created faster than the base recovery point. They also use less storage space than an independent recovery point. **Note:** You can only have one recovery point set defined for each drive. The **Recovery Point Set** option is not available if you have already assigned a selected drive to an existing backup and specified **Recovery Point Set** as the recovery point type. This option also is unavailable if you select an unmounted drive that cannot be part of a recovery point set.
Independent Recovery Point	Creates a complete, independent copy of the drives that you select. This backup type typically requires more storage space, especially if you run the backup multiple times.

3. In the middle pane, click **Create** on the toolbar.
4. In the **Name** text field, type a descriptive name for the new backup policy.
5. In the Drives field, click the hyperlink.
6. Do one of the following, and then click **Apply**:
   - Click **All drives on selected computers** to protect all drives, including those that are hidden or unmouinted, that exist on the client computers.
   - If you are defining a backup policy that backs up certain drive letters on the selected client computers, click **By Drive Letter**, and then select the drive letters that you want.
     If you chose to create a recovery point set, hidden drives are not displayed in the **By Drive** listing.

   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 Backup Exec System Recovery was

installed. In such cases, when the recovery point is created, it does not include the drive.

7 In the Schedule field, click the hyperlink.

8 Set the scheduling options for how you want the backup policy to run when it is assigned to computers. The available scheduling options depend on the recovery point type that you selected.

See "Scheduling options for creating recovery points " on page 92.

If the backup type is recovery point sets	On the Schedule tab, click **Schedule**, and then specify the frequency and time for creating a new recovery point set. You can also apply the following progressive scheduling options to the backup policy: ■ Specify options to have the policy run more than once per day. ■ Specify the amount of time to distribute the creation of recovery points from all the computers where the backup policy is being deployed. ■ Specify how frequently a new recovery point set should be started. For example, if you select **Monthly**, a new base recovery point is created the first time the backup runs during each new month. Click the **Triggers** tab if you want to use different event triggers to automate the creation of incremental recovery points. Click the **ThreatCon** tab and set the desired threat level. If the level is reached or exceeded, a back up will occur. When you are finished selecting scheduling options, click **Apply**, and then continue to the next step.

If the backup type is independent recovery points	Select **No schedule** from the drop-down list if you intend to run the backup policy on computers by creating a client task and using **Run Now**. See "Creating an Independent Backup task" on page 115. See "Deploying an existing backup policy as soon as possible" on page 117. Otherwise, select the backup frequency from the drop-down list, and time for creating new independent recovery points. When you are finished, click **Apply**, and then continue to the next step.

9 Select the destination where you want to store the recovery points by doing one of the following:

- In the Destination list, select a local target folder on the client computer, and then click **Apply**. If a local target folder is not available from the drop-down list, click **Define destination** to specify the path to the folder.
- In the Destination list, select a target folder on a network share.
  You also have the option to create a subfolder for each computer's recovery points at the network destination (checked by default). If you uncheck this option, all recovery points for all computers assigned to the backup policy are stored at the root of the network destination.
  If a network share is not available from the drop-down list, click **Define destination** to specify the UNC path to the folder. You need to specify the user name and password to access the location with create, read, and write privileges.
  If there is not be enough space at the destination where the recovery point is stored, the backup fails and an error is reported on the Backup Exec System Recovery 2010 Management Solution Home tab.

You should avoid storing recovery points on the Backup Exec System Recovery 2010 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, it eliminates this problem.

See "About managing recovery point destinations" on page 68.

10 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.

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

- In the Offsite list, select an offsite destination.
- In the Offsite list area, click **Define Destination**. Specify the path to an external drive, a network server, or an FTP server, and then click **Apply**.
  See "About Offsite Copy" on page 100.

12 Click **Save changes**.

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

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

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

Scheduling options for creating recovery points

Table 4-2 describes the schedule options that are available.

Table 4-2 Scheduling options for creating recovery points

Tab	Description
Schedule (Recovery Point Set policies)	If you selected Recovery Point Set as the backup policy type, you can specify how frequently a new recovery point set should be started. Such frequency lets you control the size of a recovery point set. If you specify Monthly and the backup is scheduled to run daily, more recovery points are created. However, the amount of required disk space depends on the amount of data that is written to the hard drive during that time. If you selected Recovery point set as the backup policy type, you have the following scheduling options to choose from: ■ **Schedule** Runs the backup policy automatically, according to a schedule. ■ **Start time** Specify the time of day when the backup should occur. ■ Days of the week Select the days you want the back policy to run.

Table 4-2 Scheduling options for creating recovery points *(continued)*

Tab	Description
	■ **Run more than once per day** Protects a system or data that changes frequently. ■ **Time between backups** Select the maximum amount of time to elapse before the next backup. ■ **Number of times** Specify the number of times that you want the backup to occur, beginning from the start time. ■ **Automatically optimize** Helps you to manage the hard disk of the backup destination. This is useful if you chose to create more than one incremental recovery point per day. Recovery points, especially independent recovery points, can use up disk space. Automatic optimization is a way to minimize the use of disk space. **Never** No deletion of incremental recovery points is performed. **Every four hours** 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** 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 4-2 Scheduling options for creating recovery points *(continued)*

Tab	Description

Table 4-2 Scheduling options for creating recovery points *(continued)*

Tab	Description
	Your options for starting new recovery point sets include the following: ■ **Start a new recovery point set (base)** ■ **Weekly** Created a new recovery point set on the first scheduled or manual backup of the week. If you clicked **Custom**, it creates a new recovery point set at the specified time on each day of the week that you checked. ■ **Monthly** Creates a new recovery point set on the first scheduled or manual back of the month. If you clicked **Custom**, it creates a new recovery point set at the specified time on each day of the month that you checked. ■ **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** A new recovery point set is created on the first scheduled or manual backup of the year, once a year on the date that you selected this option. ■ **Custom** Lets you set specific weekly or monthly options for starting a new recovery point set. ■ **Distribute strategy randomly across (minutes)** If you are saving recovery points to a network destination, you have the option to distribute the policy randomly across a specified number of minutes (0-1440) to all computers assigned to the policy. For example, suppose you want to distribute a backup 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 you avoid having to run the policy at the same start time for all computers which can sometimes cause a denial of service condition on the network, the recovery point destination, or both.

Table 4-2 Scheduling options for creating recovery points *(continued)*

Tab	Description
	Note: If you choose to archive recovery points, you might consider creating recovery point sets more frequently to keep the size of your recovery point sets smaller.
Schedule (Independent Recovery Point policies)	If you selected Independent recovery point as the backup type, your 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, it can require large amounts of disk storage space. ■ **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. ■ **Distribute strategy randomly across (minutes)** See the description in the row above. You can also create a single, independent recovery point once, with no schedule. See "Creating an Independent Backup task" on page 115.

Table 4-2 Scheduling options for creating recovery points *(continued)*

Tab	Description
Triggers	If you selected Recovery point set as the backup type, you can select the events that can trigger the automatic creation of incremental recovery points. For example, at the time you log off of a client computer or install an application, you can have Backup Exec System Recovery create an incremental recovery point. You can specify when a backup occurs for the following types of events: ■ **Any application is installed** Creates an incremental recovery point at the time users begin to install a software application on their computer. ■ **Specified applications are launched** Creates an incremental recovery point at the time users run a specified software application on their computer. ■ **Any user logs on to the computer** Creates an incremental recovery point when users log on to Windows on their computer. ■ **Any user logs off from the computer** Creates an incremental recovery point at the moment users log off from Windows on their computer (but does not turn off Windows). ■ **Data added to the drive exceeds** Creates an incremental recovery point when the added data on a drive exceeds an amount (in megabytes) that you specify.

Table 4-2 Scheduling options for creating recovery points *(continued)*

Tab	Description
ThreatCon	ThreatCon is 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. This option lets you set the Symantec ThreatCon trigger for a selected backup policy. Backup Exec System Recovery detects changes in the threat level, assuming that the computers are online at the time. When Backup Exec System Recovery detects that the ThreatCon level you chose is either reached or exceeded, the backup policy in which you enabled Symantec ThreatCon is started automatically. You then have a recovery point to use to recover data should a computer become affected by the latest threat. If a computer is not online, then it is not susceptible to online threats. But if a desktop user connects the computer to the Internet at any time, it becomes vulnerable. A desktop user does not have to enable or disable Symantec ThreatCon when they go on or offline. It works if they are online, but does nothing if they are off line.

See "Creating a basic backup policy" on page 88.

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 click Browse to navigate to the appropriate network share.

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

See "About managing recovery point destinations" on page 68.

Because 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 you have created in the console.

The user name that you enter needs read/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 Backup Exec System Recovery 2010 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 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.

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.

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 Backup Exec System Recovery 2010 Management Solution console.

About Offsite Copy

Backing up data to a secondary hard disk is a critical first step to protect your information assets. But 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 either 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 is important in the event that 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 Backup Exec System Recovery 2010 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 73.
- 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 88.
- 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 119.

When you enable Offsite Copy through a backup policy, you specify up to two Offsite destinations. After the backup policy finishes creating recovery points, Offsite verifies that the Offsite 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 6 p.m. and configured an external drive as an Offsite Copy destination. However, when you leave the office at 5:30 p.m., you take the drive with you for safe keeping. When the backup policy completes at 6:20 p.m., Backup Exec System Recovery detects that the Offsite Copy destination drive is not available and the copy process aborted. The following morning, you plug the drive back in to the computer. Backup Exec System Recovery detects the presence of the Offsite Copy destination drive and copies your recovery points.

See "About using external drives as your Offsite Copy destination" on page 102.

See “About using a network share as the Offsite Copy destination” on page 103.

See “About using an FTP server as your Offsite Copy destination” on page 104.

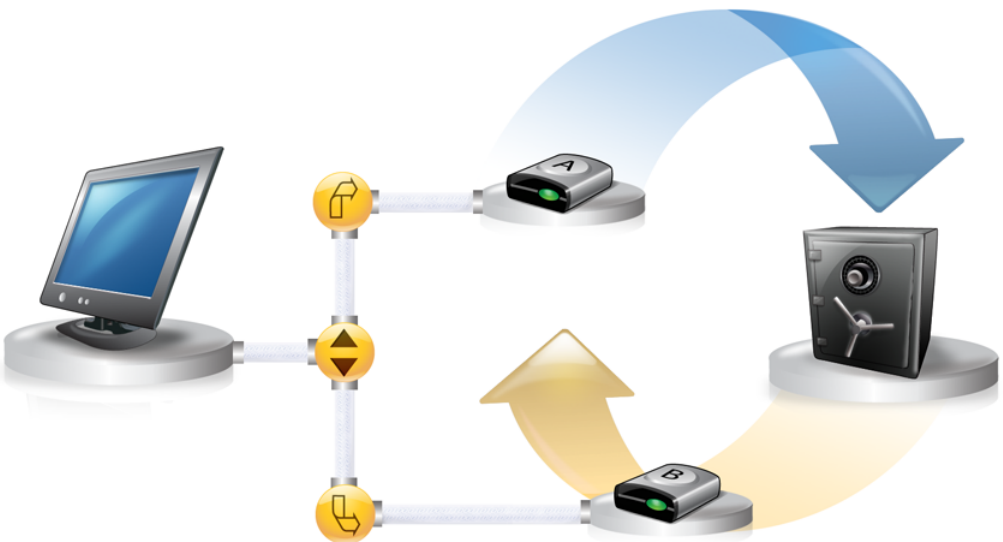
About using external drives as your Offsite Copy destination

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

See “About Offsite Copy” on page 100.

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



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

On Wednesday morning, the user brings drive B to the office and plugs it in. Backup Exec System Recovery detects that drive B is an Offsite Copy destination. The next time the backup policy runs, Backup Exec 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 multiple copies of recovery points that are stored at two separate, physical locations. The original recovery points that are stored on their backup destinations at the office. And copies of those same recovery points that are 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 gives them 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 user's have a copy of their backup data stored at two separate, physical locations.

Backup Exec 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 back policy is assigned, the backup policy is marked as supported in the Backup Exec System Recovery 2010 Management Solution user interface.

About using a network share as the Offsite Copy destination

See "About Offsite Copy" on page 100.

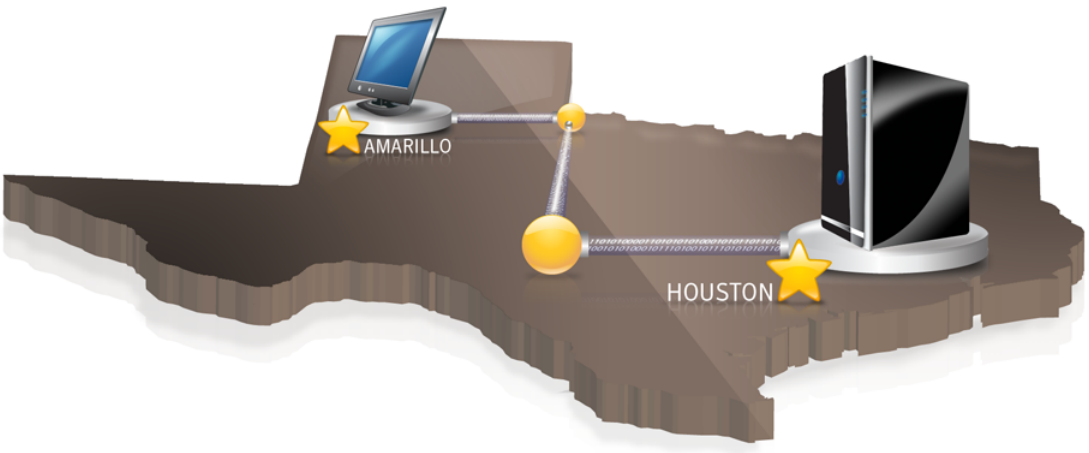
You can specify a local area network share as an Offsite Copy destination. You must be able to access the server that you plan to use. You must either map a local drive to the server, or provide a valid UNC path.

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 Backup Exec System Recovery. You can review the error information in Backup Exec System Recovery 2010 Management Solution by viewing the details of a client computer.

See "About viewing Backup Exec System Recovery details for a client computer" on page 122.



About using an FTP server as your Offsite Copy destination

See "About Offsite Copy" on page 100.

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 Backup Exec System Recovery 2010 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 Backup Exec System Recovery. You can review the error information in Backup Exec System Recovery 2010 Management Solution by viewing the details of a client computer.

See "About viewing Backup Exec System Recovery details for a client computer" on page 122.

Creating an advanced backup policy

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

Note: Backup policies apply to Windows-based computers only. If you want to backup a Linux-based computer using Backup Exec System Recovery Linux Edition, you must create a one-time backup task.

See "Creating an Independent Backup task" on page 115.

See "Creating a basic backup policy" on page 88.

To create an advanced backup policy

1. Make sure you have already created a basic backup policy.
2. On the Backup Exec System Recovery 2010 Management Solution **Manage Tasks** 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 above the Backup Policies table.
6. In the displayed panel, click **Advanced Options**.

7 In the Advanced Options panel, in the Compression drop-down list, set the compression level for the recovery points.

See "Compression level options" on page 107.

When a recovery point of a drive is created, compression results may vary, depending on the types of files on the drive.

8 Set the recovery point options.

See "Advanced recovery point options" on page 107.

9 Click **Apply**.

10 Optionally, click **Password and data encryption settings** hyperlink, and then set the password options you want.

See "Password and data encryption options" on page 110.

11 If appropriate, click **Command file settings**.

12 Specify a command file (.exe, .bat) to run during a particular stage in the recovery point creation process, and then specify the amount of time (in seconds) that you want the command to run before it is stopped.

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

See "Creating cold, warm, and hot recovery points" on page 200.

13 Do one of the following:

- Select **Use command file package to deliver command files to the local machine** if you intend to deploy the Backup Exec System Recovery command file package that is stored on Notification Server.
  See "Deploying the command files package to client computers for use during a backup" on page 114.
- Deselect **Use command file package to deliver command files to the local machine**, and then specify a folder on a network share (be sure you specify the user name and password to the share) where the command files are stored for deployment.

14 Click **Apply**.

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

16 Set the deployment options.

See "Deployment options" on page 48.

17 Click **Save changes**.

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

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

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

Compression level options

You can set a compression level for recovery points.

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

Table 4-3 Compression level options

Option	Description
None	Select this option if storage space is not an issue. If the recovery point is saved to a busy network drive, the use of high compression may be faster than no compression because less data needs to be written across the network.
Standard (recommended)	(Default) Uses low compression for a 40% average data compression ratio on recovery points.
Medium	Uses medium compression for a 45% average data compression ratio on recovery point files.
High	Uses high compression for a 50% average data compression ratio on recovery point files. High compression 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.

Advanced recovery point options

When you create an advanced backup policy, you can set a variety of options that affect how recovery points are created.

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

Table 4-4 Advanced recovery point options

Option	Description
Active backup policy	Activates (or turn on) 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, and then the oldest, previously created recovery point or set is deleted (including all associated incrementals, if applicable) from the same storage location. Be sure 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 Backup Exec 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 there are bad sectors on the hard drive. Although most drives do not have bad sectors, the potential for problems increases during the lifetime of the hard drive.

Table 4-4 Advanced recovery point options *(continued)*

Option	Description
Perform full VSS backup	For VSS-aware applications, such as Microsoft Exchange Server 2003 or Microsoft SQL, this option does two things. It performs a full backup on the VSS storage. And, after the backup, it sends a request for VSS to review its own transaction log. 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, back ups 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 Backup Exec 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 Backup Exec 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, by splitting the recovery point into smaller segments, it 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.

Table 4-4 Advanced recovery point options *(continued)*

Option	Description
Enable search engine support for Google Desktop and Backup Exec Retrieve	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. Client computers can have a search engine already installed on their computer, such as Google Desktop, to search their recovery points. See *Appendix A: Using a search engine to search recovery points* in the *Backup Exec System Recovery User's Guide* for information about using Google Desktop to retrieve files. **Note:** This option does not apply to Backup Exec 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 Backup Exec System Recovery Linux Edition.

Password and data encryption options

You can set various recovery point password and data encryption options for added security.

When you create a backup policy or an Independent Backup task, the password that you enter in this option is also automatically added to the recovery point password store.

See "About the recovery point password store" on page 66.

See "Creating an Independent Backup task" on page 115.

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

Table 4-5 Password and data encryption options

Options	Description
Enable password protection	Sets a password on the recovery point that is created. Passwords can only use standard characters, not extended characters, or symbols. (Use characters with an ASCII value of 128 or lower.) Store the password in a secure place. When you access or restore a password-encrypted recovery point, the Backup Exec System Recovery prompts you for the case-sensitive password. If you do not enter the correct password or you forget the password, you cannot open the recovery point. **Warning:** Symantec has no method for opening encrypted recovery points. User's type this password before they can restore a backup. They must also type the password to delete recovery points within a recovery point set. For greatest security, recovery point passwords should adhere to the following general rules: ■ Do not use consecutive characters that repeat (for example, BBB or 88). ■ Do not use common words you would find in a dictionary. ■ Use at least one number. ■ Use both uppercase and lowercase alpha characters. ■ Use at least one special character like ({}[],.<>;:'"?/|\`~!@#$%^&*()_-+=). ■ Change the password of an existing encrypted recovery point file after a set period of time with the Archive Recovery Point File feature in the Recovery Point Browser. See the Backup Exec System Recovery product documentation for more information about the Recovery Point Browser.

Table 4-5 Password and data encryption options *(continued)*

Options	Description
Enable AES encryption	Enhances the security of your data by enabling AES (Advanced Encryption Standard) to encrypt recovery points that you create or archive. This encryption level is especially useful if you store recovery points on a network share and need a high level of security protection against unauthorized access and use. You must enter the correct password before you can access or restore an encrypted recovery point, or delete recovery points within a recovery point set. Besides bit strength, the makeup of the password can improve the security of your data. Encryption strengths are available for the following levels: ■ Standard (password length is 8 characters or longer) ■ Medium (password length is 16 characters or longer) ■ High (password length is 32 characters or longer) While higher strengths require longer passwords, the result is greater security for your data.

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. Command files can be used 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. These command files can run in the following three different stages during the creation of a recovery point:

- Before data capture
- After data capture
- After recovery point creation

You can also specify the amount of time (in seconds) that a command file should be allowed to run.

The most common use for running command files is to stop and restart non-VSS-aware databases (such as Windows 2000) that you want to back up with Backup Exec System Recovery.

See "About backing up non-VSS-aware databases" on page 199.

Any command files that you specify in the Command File Settings window 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 114.

When you deploy the backup policy to client computers, any command files you specified are also assigned to the backup. Be sure 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 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 Backup Exec System Recovery, before using them during a backup.

When the backup begins, the command file runs during the stage you selected. If an error occurs while a command file runs, or the command file does not finish in the time you specified (regardless of the stage), the entire backup is stopped, the command file is ended (if necessary), and the error information is logged and displayed.

Table 4-6 describes the three stages of recovery point creation.

Table 4-6 Recovery point creation stages

Stage	Description
Before data capture	This stage occurs after a backup has started and before the recovery point is created. When you run a command during this stage, it lets you prepare for the recovery point creation process by stopping (or notifying) any open applications that the drive uses. **Note:** If you use this stage option, be sure that the command file has an error recovery mechanism that is 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 entire recovery point creation process to end immediately; no other command files can run.
After data capture	This stage occurs after the "virtual disk snapshot" is created. When you run a command during this stage, you can allow services to safely resume normal activity on the drive while continuing the recovery point creation process. Because the virtual disk snapshot takes only a few seconds to create, the database is in the backup state momentarily, and results in a minimal number of created log files.
After recovery point creation	This stage occurs after the actual recovery point file is created. When you run a command during this stage, it lets you act on the recovery point, itself, by copying it to an offline location.

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** at the time you create an advanced backup policy that uses command files, you need to deploy the Backup Exec System Recovery Command File Delivery package to client computers.

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

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

1. On the Backup Exec System Recovery 2010 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

   See "Deployment options" on page 48.
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 Backup Exec 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.

Note: A backup policy, as opposed to a one-time, independent backup task, applies to Windows-based computers only.

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 88.

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

See "Deploying a backup policy" on page 117.

To run an Independent Backup task

1. On the Backup Exec System Recovery 2010 Management Solution **Monitor Tasks** tab, right-click Backup Exec System Recovery Tasks, and then click **New > Task**.
2. In the Client Tasks tree, click **Backup Exec System Recovery Tasks > Independent Backup**.
3. On the **Create New Task** page, in the right pane, type a name for the task.
4. Specify the backup options you want.
5. Click **Advanced**, and then click the General tab to set specific backup options.

   The options found on the Security Option tab, the Command File tab, and the Task Options tab are optional.

   If you choose to use the Security Option tab to assigned a password to the recovery point, the password that you enter is also automatically added to the recovery point password store.

   An addition tab is available when you save the task, and then edit it by going into **Advanced** again. The additional tab is **Image File Name** and it is only available if you are backing up by drive letter.

   The Command File tab does not apply to Backup Exec System Recovery Linux Edition.
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:
   - Click **Quick Run**.
     Select the computer on which you want the task to run, and then click **Run**.
   - Click **New Schedule**.
     Click **Now** and then select the computers that you want the task applied to. Or, click **Schedule** to run the task as soon as possible.
   - Click **New Schedule**.
     Click **Schedule**. Specify the date and time to run the task, and then select the computers that you want the task applied to. 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 resource targets with Backup Exec System Recovery installed.

See "Disabling a backup policy" on page 120.

See "Creating a basic backup policy" on page 88.

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

See "Deploying an existing backup policy as soon as possible" on page 117.

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, when two backup policies with recovery point set options pointing to the same drives are assigned to the client computer, the policy fails with no generated error.

To deploy a backup policy

1. On the Backup Exec System Recovery 2010 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

   See "Deployment options" on page 48.
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. Within the Client Task you can use Quick Run to create–on demand–an independent recovery point, a recovery point set, or an incremental recovery point of the drive's most recent changes. A manual backup starts immediately if there are no other tasks or policies in the queue.

See "Deploying a backup policy" on page 117.

To deploy an existing backup policy as soon as possible

1. On the Backup Exec System Recovery 2010 Management Solution **Monitor Tasks** tab, right-click Backup Exec System Recovery Tasks, and then click **New > Task**.
2. In the Client Tasks tree, click **Backup Exec 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 drop-down list, and then click **OK**.
5. In the Task Status field, do one of the following:
   - Click **Quick Run**.
     Select the computer on which you want the policy to run, and then click **Run**.
   - Click **New Schedule**.
     Click **Now**, and then select the computers that you want the backup policy applied to. Or, click **Schedule** to run the task as soon as possible.
   - Click **New Schedule**.
     Click **Schedule**. Specify the date and time to run the task, and then select the computers that you want the backup policy applied to. 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.

To view the status of computers within a backup policy

1. On the Backup Exec System Recovery 2010 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 "Editing the schedule of a backup policy" on page 119.

See "Viewing the status of computers within a backup policy" on page 118.

See "Creating a basic backup policy" on page 88.

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

To edit a backup policy

1. On the Backup Exec System Recovery 2010 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.
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. The settings include the following:

- Check (enable) or uncheck (disable) the schedule
- Backup schedule
- Recovery point set schedule
- Event triggers that automate the creation of recovery points (for recovery point set backup policies only)

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

See "Creating a basic backup policy" on page 88.

To edit the schedule of a backup policy

1. On the Backup Exec System Recovery 2010 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**.

6 Click **Save changes**.

Renaming a backup policy

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

To rename a backup policy

1 On the Backup Exec System Recovery 2010 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 or "turn on" the backup later when you want recovery point creation to resume.

To disable a backup policy on resource targets

1 On the Backup Exec System Recovery 2010 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 or "turns off" the backup policy on client computers. The policy, however, remains on client computers.

5 Click **Save changes**.

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 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 Backup Exec System Recovery 2010 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**.

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 Backup Exec System Recovery 2010 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**.

About viewing Backup Exec System Recovery details for a client computer

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

Among the details that you can view include the following:

- 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.
- Backup Exec System Recovery license status.

Table 4-7 describes the tab and the details within that tab that you can view.

Table 4-7 Backup Exec System Recovery details

Tab	Description
Status	

Table 4-7 Backup Exec 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 backup. For example, suppose you have a C:\, D:\, and E:\ volume on a client computer, but only a backup of C:\ exists. While Backup Exec System Recovery 2010 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, it 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 Altiris Agent is not installed. ■ **Unknown** The status is not yet calculated, or the computer has an unsupported version of Backup Exec System Recovery. ■ **Not Installed** A computer does not have the Backup Exec System Recovery Plug-in installed. See "Creating a basic backup policy" on page 88. License status types include the allowing: ■ **License** The number of computers that have a current license assigned.

Table 4-7 Backup Exec System Recovery details *(continued)*

Tab	Description
	■ **Not Licensed** The number of computers on which an expired trial version of Backup Exec System Recovery is installed or on which no license was activated. ■ **Trial License** The number of computers that have a trial version of Backup Exec System Recovery installed. The Status tab also shows you the Backup Exec System Recovery version, license model used, and the license expiration date.
Events	View 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	View 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 that are taken of selected drives (even if the recovery point has been deleted from the storage location). The picture icon next to each drive letter gives you a quick visual indication about the type of recovery point that is created (a recovery point set, or an independent recovery point).
Volume Status	View 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.

Table 4-7 Backup Exec System Recovery details *(continued)*

Tab	Description
Client Configuration	View the selected computer's Backup Exec System Recovery client settings. For example, you can view the Backup Exec 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 150.
Recovery History	View 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.

See "Viewing Backup Exec System Recovery details for a client computer" on page 126.

Viewing Backup Exec System Recovery details for a client computer

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

See "About viewing Backup Exec System Recovery details for a client computer" on page 122.

To view Backup Exec System Recovery details for a client computer

1. On the Backup Exec System Recovery 2010 Management Solution **Manage Tasks** tab, in the left pane, expand the **Computers** area.
2. In the left pane, do one of the following:
   - Under **Group**, click a computer group name.
   - Click **Computers** in the **Computers** tree.
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.

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 127.

You can also delete recovery points within a set.

The base recovery point and all of its incrementals that are taken up to a point in time are required whenever you want to restore to a specific point in time. Depending on the duration of the backup, there can be a large accumulation of incremental recovery points. You can 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 recovery points within a set consolidates the data only, it does not delete data.

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.

See "Deleting recovery points within a set" on page 128.

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 88.

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 127.

See "Deleting recovery points within a set" on page 128.

To delete a recovery point set

1. On the Backup Exec System Recovery 2010 Management Solution **Monitor Tasks** tab, right-click Backup Exec System Recovery Tasks, and then click **New > Task**.
2. In the Client Tasks tree, click **Backup Exec 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:
   - Click **Now**, and then click **Schedule** to run the task as soon as possible.
   - 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 that you defined includes the assignment of 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 127.

See "Deleting a recovery point set" on page 127.

To delete recovery points within a set

1. On the Backup Exec System Recovery 2010 Management Solution **Monitor Tasks** tab, right-click Backup Exec System Recovery Tasks, and then click **New > Task**.
2. In the Client Tasks tree, click **Backup Exec 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

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

Chapter 5

Managing the conversion of recovery points to virtual disks

This chapter includes the following topics:

About convert to virtual

You can use Backup Exec System Recovery 2010 Management Solution to schedule the conversion of the latest recovery points of a physical computer to VMware Virtual Disk, Microsoft Virtual Disk, or a VMware ESX Server. When you convert recovery points to virtual disks, it has the following benefits:

- It is useful in the event that 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).
- It is excellent for testing and evaluation purposes.

The following platforms support virtual disks created from recovery points:

- VMware Workstation 4, 5, and 6
- VMware ESX Server 2.0, 3.0, 3.5, 3.5i, 4.0, and 4.0i
- VMware Server 1
- VMware GSX Server 3.x (replaced by VMware Server)
- Microsoft Virtual Server 2005 R2 and later
- Microsoft Hyper-V

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 132.

See "Configuring a Convert to Virtual by Destination task" on page 140.

See "Configuring a one-time convert to virtual task" on page 143.

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, they must first be unlocked using the specified password.

To help automate the conversion process, you can specify these existing passwords in the Passwords Store. When you configure and run a convert to virtual task, the client computers use the list of passwords to unlock the recovery points at the time of conversion.

See "About the recovery point password store" 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.

The convert to virtual by computer task is only available from the Monitor Tasks tab area. You can apply the task to multiple computers at a time. The convert to

virtual by computer 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 "Configuring a Convert to Virtual by Destination task" on page 140.

See "Configuring a one-time convert to virtual task" on page 143.

To configure a Convert to Virtual by Computer task

1. On the Backup Exec System Recovery 2010 Management Solution **Monitor Tasks** tab, right-click Backup Exec System Recovery Tasks, and then click **New > Task**.
2. In the Client Tasks tree, click **Backup Exec 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, if necessary, select the version that you want to create.
5. Do one of the following:
   - If you want to configure a conversion task for two or more computers, click **All drives on the selected computers** to convert the latest recovery points of all drives, including hidden, that exist on the selected computers (excludes unmounted drives).
   - If you want to configure a convert to virtual task that converts 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 Backup Exec 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**, 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 Backup Exec System Recovery 2010 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 Backup Exec System Recovery 2010 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.

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: ■ Click the **ESX Setup** tab, and then 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 server, upload, or import locations to choose from, click the ESX Server Location tab, and set the appropriate options. See "ESX Server Location options" on page 136. ■ Select **Remove files from temporary location after conversion** if you want the temporary files removed after the virtual disk is created.

9 Click the **Conversion Options** tab, and then set the options you want.

See "Conversion options" on page 137.

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 Do one 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. The reason for this is because if the computers to which you want a schedule to apply are in a target, there is no need to change the schedule as 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.

15 Click **Schedule** at the bottom of the page.

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

ESX Server Location options

Use the ESX Server Location options if you are configuring a convert to virtual task for an ESX server.

See "Configuring a Convert to Virtual by Computer task" on page 132.

Table 5-1 ESX Server Location options

Option	Description
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 buttons 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 button to configure the import folder path you want.

Conversion options

You can set various conversion options when you convert a recovery point to a virtual disk.

See "Configuring a Convert to Virtual by Computer task" on page 132.

Table 5-2 Conversion options

Option	Description
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.

Table 5-2 Conversion options *(continued)*

Option	Description
Run Windows Mini-Setup	Select this option (default) to run 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 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, entering the Product Key, user name, and company name are automatically applied by Mini-Setup which uses the answer file. Deselect this option if you want any of the following to occur at the time of recovery instead: ■ Run Windows Welcome instead 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 ensures that the computer is recovered to its original state prior to recovery. For more detailed information about Mini-Setup. you can perform a search for "Mini-Setup" on the Microsoft Help and Support Web site.

Table 5-2 Conversion options *(continued)*

Option	Description
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.

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 a recovery point is created by Backup Exec System Recovery, 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 132.

See "Configuring a one-time convert to virtual task" on page 143.

To configure a Convert to Virtual by Destination task

1. On the Backup Exec System Recovery 2010 Management Solution **Monitor Tasks** tab, right-click Backup Exec System Recovery Tasks, and then click **New > Task**.
2. In the Client Tasks tree, click **Backup Exec 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, if necessary, select the version that you want to create.

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 Backup Exec System Recovery 2010 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 Backup Exec System Recovery 2010 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: ■ Click the **ESX Setup** tab, and then 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 server, upload, or import locations to choose from, click the ESX Server Location tab, and set the appropriate options. See "ESX Server Location options" on page 136. ■ Select **Remove files from temporary location after conversion** if you want the temporary files removed after the virtual disk is created.

11 Click the **Conversion Options** tab, and then set the options you want.

See "Conversion options" on page 137.

12 Click **OK** to return to the task page.

13 Click **OK**.

14 In the Task Status field, do one of the following:

15 ■ Click **New Schedule**.
Click **Now**, or click **Schedule** at the bottom of the page to run the task as soon as possible.

■ Click **New Schedule**.
Click **Schedule**. Specify the date and time to run the task, and then click **Schedule** at the bottom of the page.

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

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 is run only once on the computer that you have selected (it is run 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 132.

See "Configuring a Convert to Virtual by Destination task" on page 140.

To configure a one-time convert to virtual task

1. On the Backup Exec System Recovery 2010 Management Solution **Monitor Tasks** tab, right-click Backup Exec System Recovery Tasks, and then click **New > Task**.
2. In the Client Tasks tree, click **Backup Exec 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 will do the conversion.
5. Click the virtual disk type and, if necessary, select the version that you want to create.
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.	■ 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 are using 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 was 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 Backup Exec System Recovery 2010 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 Backup Exec System Recovery 2010 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: ■ Click the **ESX Setup** tab, and then 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 server, upload, or import locations to choose from, click the ESX Server Location tab, and set the appropriate options. See "ESX Server Location options" on page 136. ■ Select **Remove files from temporary location after conversion** if you want the temporary files removed after the virtual disk is created.

10 Click the **Conversion Options** tab, and then set the options you want.

See "Conversion options" on page 137.

11 Click the **Drives to Include** tab, and then set the options you want.

See "Drives to Include options" on page 147.

12 Click **OK** to return to the task page.

13 Click **OK**.

14 In the Task Status field, do one of the following:

15 ■ Click **New Schedule**.
Click **Now**, or click **Schedule** at the bottom of the panel to run the task as soon as possible.

■ Click **New Schedule**.
Click **Schedule**. Specify the date and time to run the task, and then click **Schedule** at the bottom of the panel.

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

Drives to Include options

When you do a one time conversion of a recovery point to a virtual disk, you can set the drives within the recovery point that you want to convert. You can also choose to rename the resulting virtual disk file.

See "Configuring a one-time convert to virtual task" on page 143.

Table 5-3 Drives to Include options

Option	Description
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.)

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 just 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 convert to virtual" on page 131.

To edit a convert to virtual task

1. On the Backup Exec System Recovery 2010 Management Solution **Monitor Tasks** tab, expand the **Backup Exec System Recovery Tasks** folder.
2. Do one of the following:
   - In the **Backup Exec System Recovery Tasks** tree, click a convert to virtual task name.
   - Click the **Backup Exec System Recovery Tasks** folder, and then in the right pane, double-click the highlighted convert to virtual task name that 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 convert to virtual" on page 131.

To delete a convert to virtual task

1. On the Backup Exec System Recovery 2010 Management Solution **Monitor Tasks** tab, expand the **Backup Exec System Recovery Tasks** folder.
2. Do one of the following:
   - In the **Backup Exec System Recovery Tasks** tree, right-click a convert to virtual task name.
   - Click the **Backup Exec System Recovery Tasks** folder, and then in the right pane, right-click the highlighted convert to virtual task name that you want to delete.
3. Click **Delete**.
4. Click **OK** to confirm the deletion.

Chapter 6

Monitoring computers and processes

This chapter includes the following topics:

About viewing reports

You can use the **Reports** tool to generate various predefined reports with detailed information about your backup management system.

See "Viewing reports" on page 150.

See "Viewing the status of computers within a backup policy" on page 118.

Table 6-1 describes the predefined reports that you can generate.

Table 6-1 Available reports

Report	Description
Backup policies	Displays a detailed overview of all backup policies that are available in Backup Exec System Recovery 2010 Management Solution.
Backup Status of Managed Computers	Displays the backup status of client computers that Backup Exec System Recovery 2010 Management Solution manages.
License Policies	Displays all available Backup Exec System Recovery license policies.
License Status of Managed Computers	Displays the Backup Exec System Recovery license status on computers.

Table 6-1 Available reports *(continued)*

Report	Description
Managed Computers with Backup Exec System Recovery	Displays a list of client computers that Backup Exec System Recovery 2010 Management Solution manages with the Backup Exec System Recovery plug-in installed.
Managed Computers with Backup Exec System RecoveryLinux Edition	Displays a list of client computers that Backup Exec System Recovery 2010 Management Solution manages with the Backup Exec System Recovery Linux Edition plug-in installed.
Managed Computers with Recovery Points	Displays detailed information about available recovery points. Deleted recovery points are not included in the report.
Managed Computers with Unsupported Backup Exec System Recovery	Displays computers that have an installed version of Backup Exec System Recovery that Backup Exec System Recovery 2010 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.

Viewing reports

You can use the Reports tab to generate various predefined reports with detailed information about your backup management system.

See "About viewing reports" on page 149.

See "Viewing the status of computers within a backup policy" on page 118.

To view reports

1. On the Backup Exec System Recovery 2010 Management Solution, click the **Report Tasks** tab.
2. In the Backup Exec 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 Backup Exec System Recovery 2010 Management Solution **Manage Tasks** tab, expand the **Configuration Policies** list in the left pane.
2. Do any one of the following:

To edit the default client configuration policy	Do the following: ■ In the left pane, select a client configuration policy name (Event Log, FTP, Log Files, Performance, SMTP Notification, SNMP Notification, Tray Icon, or Volume Alert). ■ 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 (Event Log, FTP, Log Files, Performance, SMTP Notification, SNMP Notification, Tray Icon, or Volume Alert) . ■ 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. In the displayed page, near the upper-right corner, 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.

   See "Client configuration policy options" on page 152.
5. In the **Applied to** field, select a resource target, and then select the filtering rules that you want applied to the policy.
6. Click **Save Changes**.

Client configuration policy options

You can set a variety of options that affect one computer or entire groups of computers.

See "Configuring a client option policy for computers" on page 150.

Table 6-2 Client configuration policy options

Option	Description
Event Log	Sets the minimum priority level and error message types that you want added to the Windows application log regarding Backup Exec System Recovery on the computer.
FTP	Sets the default FTP connection settings if you use FTP as an offsite copy destination. Your options are the following: ■ Passive (Recommended) Passive (sometimes written "PASV") mode 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 Active mode when connections or transfer tries fail in Passive mode, or when you receive data socket errors. When an FTP client connects using 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 Backup Exec System Recovery on the client computer tries to connect to an FTP server before giving up. Backup Exec System Recovery can try a maximum of 100 times. ■ Stop trying to connect after Specifies the number of seconds Backup Exec System Recovery on the client computer tries to connect to an FTP server before giving 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.

Table 6-2 Client configuration policy options *(continued)*

Option	Description
Log File	Sets the following log file options: ■ Priority Level Choose the minimum priority level and error message types that you want logged to a file regarding Backup Exec System Recovery on the computer. ■ Log file location Specify the path that you want to use for storing log files. ■ Maximum file size Specify 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 Backup Exec System Recovery 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 Backup Exec System Recovery, you can improve the performance of other software programs that may be running on the computer. When Backup Exec System Recovery (with a user interface) is installed, the throttle value that you set in Backup Exec System Recovery 2010 Management Solution takes precedence over the throttle value that a remote user may set. If you save recovery points to a network storage location, you can also set a network throttle 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.

Table 6-2 Client configuration policy options *(continued)*

Option	Description
SMTP Notification	Configures a user to receive SMTP email notification messages. Choose the minimum priority level and error message types that you want to send regarding Backup Exec 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. Backup Exec System Recovery 2010 Management Solution does not check the server name or the email address for validity. You can increase the security of the email that is sent by specifying an authentication level (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. When you change an existing SMTP Notification setting policy from On (enabled) to Off (disabled), it does not prevent resource targets with Backup Exec 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 SNMP traps from Backup Exec System Recovery when install and configure the Windows SNMP system service. By default, Backup Exec System Recovery is not enabled to send traps to NMS managers.
Tray Icon	Shows or hides the Backup Exec System Recovery system tray icon on computers. Hiding the tray icon is useful for the following reasons: ■ You want the actions of Backup Exec 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 Backup Exec System Recovery on critical computers such as product servers. Backup Exec System Recovery and the Backup Exec 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, regardless of whether the system tray icon is visible or hidden.

Table 6-2 Client configuration policy options *(continued)*

Option	Description
Volume Alert	Changes how Backup Exec System Recovery 2010 Management Solution reports the status of a particular drive on a client computer. For example, if 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 Backup Exec System Recovery 2010 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 of each drive on a client computer is reported throughout the software, wherever the drive is listed. When you customize status reporting for a drive, the status is reflected anywhere that the drive is listed in Backup Exec System Recovery 2010 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 to it. You can set the status reporting level that you want 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.

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, if 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 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 Backup Exec 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 "About LightsOut Restore on computers" on page 158.

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 (you must start the computer from the Symantec Recovery Disk CD).

As an additional option, when the recovery environment starts as part of LightsOut Restore, you can set it to automatically start a pcAnywhere thin host. To enable or disable this feature, you must edit the LightsOut Restore Configuration options as found in the LightsOut Restore Install Policies tree. You can then use pcAnywhere to connect to the thin host and remotely use the recovery environment to assist you with troubleshooting or other issues.

See "Configuring a remote Recover Drive task" on page 160.

About LightsOut Restore on computers

You must install LightsOut Restore (using the LightsOut Restore 2010 installation policy) before you can perform a remote recovery of a primary (or system) drive using the LightsOut Restore capability.

See "About setting up and using LightsOut Restore" on page 159.

Note: To run the LightsOut Restore feature you need a minimum of 1 GB of memory on the client computer.

The following is an overview of how to install LightsOut Restore on client computers:

- Edit the LightsOut Restore Configuration policy in Backup Exec System Recovery 2010 Management Solution.
- Edit the LightsOut Restore install policy.
- Deploy the LightsOut Restore policy to client computers.

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 Symantec recovery environment boot menu option is selected, the computer starts LightsOut Restore by using the files that are installed on the system partition.

LightsOut Restore uses Symantec pcAnywhere technology, the Windows boot menu, and hardware devices such as RILO and DRAC to let an administrator remotely control a system during the boot process.

When the custom recovery environment starts as part of LightsOut Restore, you can enable it to automatically start a pcAnywhere thin host. You can then use Symantec pcAnywhere from your remote location to connect to the thin host.

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 and go 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 "About installing Backup Exec System Recovery 2010, Backup Exec System Recovery 2010 Linux Edition, or LightsOut Restore 2010 on client computers " on page 49.

See "Configuring and installing LightsOut Restore on client computers" on page 55.

About setting up and using LightsOut Restore

Before you set up and configure LightsOut Restore, you should review the following information:

- Install a licensed version of Symantec pcAnywhere on a central computer that you use for management (for example, a help desk computer).
- Ensure that all of your servers can be managed remotely through a hardware device such as RILO or DRAC.
- Install Backup Exec System Recovery on the client computers that you want to protect, and then define and run backups to create recovery points.
- Install LightsOut Restore directly to the client computer's local file system.
- Use the RILO or 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.
- 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. A pcAnywhere thin host automatically starts if you configured it to do so in the LightsOut Restore Configuration policy.

- Use Symantec pcAnywhere to connect to the pcAnywhere thin host that waits on the remote server.
- Use the recovery environment to restore individual files, or entire drives with the help of pcAnywhere.

Additional information to help you successfully use LightsOut Restore includes the following:

- The LightsOut Restore feature requires at least 1 GB of memory to run.
- 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 CD.
- 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 "About installing Backup Exec System Recovery 2010, Backup Exec System Recovery 2010 Linux Edition, or LightsOut Restore 2010 on client computers " on page 49.

See "Configuring and installing LightsOut Restore on client computers" on page 55.

Configuring a remote Recover Drive task

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.

If the remote drive cannot be locked to perform the recovery under Windows (typically, because the drive is in use by a program), it starts the recovery environment 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 are unable to save the Recover Drive task.

See "About installing Backup Exec System Recovery 2010, Backup Exec System Recovery 2010 Linux Edition, or LightsOut Restore 2010 on client computers " on page 49.

See "About setting up and using LightsOut Restore" on page 159.

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 of the data on the drive you want to restore is replaced by 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 "Configuring a remote Recover Computer task" on page 163.

To configure a remote Recover Drive task from the Monitor Tasks tab

1. Inform the user of the client computer. They should close any applications and files that may be running or open on the drive that you want to recover.
2. On the Backup Exec System Recovery 2010 Management Solution **Monitor Tasks** tab, right-click Backup Exec System Recovery Tasks, and then click **New > Task**.
3. In the **Client Tasks** tree, click **Backup Exec 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 are using 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 In 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 In the **Options** tab, set the restore options.

See "Restore options" on page 162.

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:

- Click **New Schedule**.
  Click **Now** or click **Schedule** at the bottom of the page to run the task as soon as possible.
- Click **New Schedule**.
  Click **Schedule**. Specify the date and time to run the task, and then click **Schedule** at the bottom of the page

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

Restore options

You can select from a variety of options when you recover a drive.

See "Configuring a remote Recover Drive task" on page 160.

Table 7-1 Restore options

Option	Description
Verify recovery point before restore	Determines whether a recovery point is valid or corrupt before restoring it. 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.

Table 7-1 Restore options *(continued)*

Option	Description
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, which is a drive other than the one where the Windows operating system is installed, do not check this option.
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.

Configuring a remote Recover Computer task

You can use a Recover Computer task to restore one, multipe, or all drives on a selected computer, based on the recovery point you have selected..

See "About recovering a drive remotely" on page 157.

See "Configuring a remote Express Recovery task" on page 165.

See "About recovering a computer locally" on page 174.

To configure a remote Recover Computer task

1. Inform the user of the client computer. They should close any applications and files that may be running or open on the drive that you want to recover.
2. On the Backup Exec System Recovery 2010 Management Solution **Monitor Tasks** tab, right-click Backup Exec System Recovery Tasks, and then click **New > Task**.
3. In the Client Tasks tree, click **Backup Exec 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 are using 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. In 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. In the **Options** tab, set the restore options.

    See "Restore options" on page 162.
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:

- Click **New Schedule**.
  Click **Now** or click **Schedule** at the bottom of the page to run the task as soon as possible.
- Click **New Schedule**. Click **Schedule**, and then specify the date and time to run the task. Click **Schedule** at the bottom of the page.

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

Configuring a remote Express Recovery task

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 "Configuring a remote Recover Computer task" on page 163.

To configure a remote Express Recovery task

1 On the Backup Exec System Recovery 2010 Management Solution **Monitor Tasks** tab, right-click Backup Exec System Recovery Tasks, and then click **New > Task**.

2 In the Client Tasks tree, click **Backup Exec System Recovery Tasks > Express Recovery**.

3 In the right pane of the Create New Task page, type a name for the task.

4 Do one or more of the following:

- Click **Verify recovery point before recovery** to ensure 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.
- Click **Check for file system errors** to check the recovered drive for errors after the recovery point is restored.

5 Do one of the following:

- Click **Use the computer's latest recovery point**.

- Click **Use the computer's latest recovery point available on or before the specified date**, and then use the calendar to select a date.
  If the recovery point is missing (deleted) at the primary destination, the Offsite Copy destination is checked for a copy of the same recovery point. If the recovery point is found, then the express recovery task is performed. Otherwise, the task fails.
- Click **Use the selected recovery point**.
  Optionally, click **Display recovery points from local and network Offsite locations**.
  This option only applies if you are using 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 table list, select the recovery point that you want to restore.
  If the recovery point is password-protected, enter the correct password in the text field.

6 Click **OK**.

7 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.

8 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. The reason for this is because if the computers to which you want a schedule to apply are in a target, there is

no need to change the schedule as 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.

9 Click **Schedule** at the bottom of the page.

10 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

Backup Exec 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, the backup data must be at least as current as the changes that were made to the lost file or folder.

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: File and folder backups or file and folder restore are only possible if it is set up directly in Backup Exec System Recovery on the client computer, not from Backup Exec System Recovery 2010 Management Solution. If you installed Backup Exec System Recovery without a user interface, on client computers, file and folder backup is not possible.

If you cannot find the files or folders that you want to restore by browsing through a recovery point, you can use the Backup Exec 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 170.

See "Recovering files and folders locally by using a recovery point" on page 172.

Recovering files and folders locally by using file and folder backup data

If you defined a file and folder backup and need to recover files, you can recover them from a recent file and folder backup.

Note: File and folder backups or file and folder restore are only possible if it is set up directly in Backup Exec System Recovery on the client computer, not from Backup Exec System Recovery 2010 Management Solution. If you installed Backup Exec System Recovery without a user interface, on client computers, file and folder backup is not possible.

Backup Exec 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 169.

To recover files and folders locally by using file and folder backup data

1. On the client computer, in the Backup Exec System Recovery Home or Tasks page, click **Recover My Files**.
2. In the left pane of the Recover My Files window, select **File and Folder** as the search method.
3. Do one of the following:
   - In the Find files to recover search 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 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:
   - Click **Original folders** to restore the files to the same folder where they existed when they were backed up.
     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.

     Caution: The Overwrite existing files option replaces the original files (or the files of the same names that are currently stored at that location) with the files that you want to restore.
   - Click **Recovered Files folder on the desktop** to restore the files to a Recovered Files folder on the Windows desktop.
     Backup Exec System Recovery creates this folder during the restore.
   - Click **Alternate folder** and 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** if you are certain that the file you want to recover is the file that you want.
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: File and folder backups or file and folder restore are only possible if it is set up directly in Backup Exec System Recovery on the client computer, not from Backup Exec System Recovery 2010 Management Solution. If you installed Backup Exec System Recovery without a user interface, on client computers, file and folder backup is not possible.

See "About recovering lost data locally" on page 169.

To recover files and folders locally by using a recovery point

1. On the client computer, on the Home or Tasks page in Backup Exec System Recovery, click **Recover My Files**.
2. In the left pane of the Recover My Files window, select **Recovery Point** as the search method.
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 Backup Exec 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.

   See "View by options" on page 173.
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 Files to restore list, select the files that you want to restore.
7. Click **Recover Files**.
8. In the Recover My Files dialog box, do one of the following:

   - Click **Original folders** to have the files restored in the original folder where they existed when they were backed up.

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 remains unchanged.

Caution: Checking Overwrite existing files replaces the original files (or the files of the same names that are currently stored at that location) with the files you want to restore.

- Click **Recovered Files folder on the desktop** to have the files restored to a new folder that is created on the Windows desktop called Recovered Files.
- Click **Alternate folder** and specify the path to an alternate location where you want the files restored.

9 Click **Recover**.

10 If you are prompted to replace the existing file, and you are certain that the file you want to recover is the correct one, click **Yes**.

11 Click **OK**.

View by options

To help you restore the right files and folders, you can view recovery points by date, file name, or system.

See "Recovering files and folders locally by using a recovery point" on page 172.

Table 8-1 View by options

Option	Description
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	Browse to another location, such as an external (USB) drive, removable media, or to a network location (with proper network credentials) to select a recovery point (.v2i) file.

Table 8-1 View by options *(continued)*

Option	Description
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.

About 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 (which is any drive other than the system drive, or the drive where your operating system is installed), you can restore the drive within Windows.

The Symantec Recovery Disk lets you run a recovery environment that provides temporary access to Backup Exec System Recovery 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 Backup Exec 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 8-2 Process for recovering a computer locally

Order	Action	Description
Step 1	Configure a client computer to start from a CD	Set up the computer so that it can start from the Symantec Recovery Disk CD. See "Configuring a computer locally to start from a CD" on page 177.

Table 8-2 Process for recovering a computer locally *(continued)*

Order	Action	Description
Step 2	Start the client computer using the Symantec Recovery Disk CD	Start the computer by using the Symantec Recovery Disk CD. See "About starting a computer locally by using Symantec Recovery Disk" on page 175.
Step 3	Optionally scan a hard disk for errors	Scan the computer's hard disk to check for errors before you perform a recovery. See "Checking a hard disk for errors" on page 178.
Step 4	Recover a computer locally	Recover the computer using Symantec Recovery Disk. See "About recovering locally to a computer with different hardware" on page 185. See "Recovering files and folders locally by using Symantec Recovery Disk" on page 187.

About 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. Symantec Recovery Disk is included with Backup Exec System Recovery. When you start a computer using the Symantec Recovery Disk CD, a simplified version of Windows starts that runs a recovery environment. In the recovery environment, you can access the recovery features of Backup Exec System Recovery.

Note: Depending on which version of the product you have purchased, Symantec Recovery Disk is either included on the product CD, or as a separate CD. You should store the original CD in a safe place. Should you lose the CD, you can create a new one if you have a CD burner. See *If driver validation fails* in the *Backup Exec System Recovery User's Guide*.

The recovery environment requires a minimum of 512 MB of RAM to run. If a computer's video card is configured to share the computer's RAM, you might need more than 512 MB of RAM. Also, if you install a multilingual version of the product, you must have a minimum of 768 MB of RAM to run Symantec Recovery Disk.

See "Starting a computer locally by using Symantec Recovery Disk" on page 176.

Starting a computer locally by using Symantec Recovery Disk

You can use the Symantec Recovery Disk CD to start a client computer locally that can no longer run the Windows operating system.

See "About starting a computer locally by using Symantec Recovery Disk" on page 175.

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, and external hard drive).

   As a best practice, you should attach the device before you restart the computer using the Symantec Recovery Disk CD.

2. On the client computer, insert the Backup Exec System Recovery CD into its media drive.

   If a computer manufacturer installed Backup Exec 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 CD, you might need to change the startup settings on the computer.

   See "Configuring a computer locally to start from a CD" on page 177.

4 As soon as you see the prompt “Press any key to boot from CD”, 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

To run Symantec Recovery Disk, you must be able to start the computer using a CD.

See “Starting a computer locally by using Symantec Recovery Disk” on page 176.

To configure a computer locally to start from a CD

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 setup 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 CD into the CD drive, and then restart the computer.

Depending on which version of the product you have purchased, Symantec Recovery Disk is either included on the product CD, or as a separate CD. You should store the original CD in a safe place. Should you lose the CD, you can create a new one if you have a CD burner.

6 Save the changes and 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 with the Symantec Recovery Disk CD in the drive, you see a prompt telling you to “Press any key to boot from CD”. If you do not press a key within five seconds, the computer attempts to start from the next startup 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.

About preparing to recover a computer locally by using Symantec Recovery Disk

Before you start the recovery process, you should scan the hard disk to check it for corrupted data or surface damage.

See “Checking a hard disk for errors” on page 178.

Checking a hard disk for errors

If you suspect that a hard disk is damaged, you can examine it for errors.

See “Check hard disk for errors options” on page 178.

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.

See “Check hard disk for errors options” on page 178.

4 Click **Start**.

Check hard disk for errors options

You can use the Analyze panel in Symantec Recovery Disk to check the hard disk on the client computer for bad sectors or system errors.

See “Checking a hard disk for errors” on page 178.

Table 8-3 Check hard disk for errors options

Option	Description
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.

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 or other hard drive back to the state it was in when the recovery point was created.

If you intend to use the Restore Anyware feature to restore a computer that uses different hardware, you must save the recovery point file that you want to use for the restore to a location that you can access (for example, to a location that you can browse to). During a recovery in which you have enabled the Restore Anyware option, you might be prompted to supply disk drivers, service packs, hotfixes, and so forth. You should have your Windows media CD available.

See "About recovering locally to a computer with different hardware" on page 185.

See "How to use Restore Anyware" on page 186.

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 "Configuring a remote Recover Computer task" on page 163.

See "Recovering files and folders locally by using Symantec Recovery Disk" on page 187.

See "Starting a computer locally by using Symantec Recovery Disk" on page 176.

To recover a computer locally by using Symantec Recovery Disk

1. Start the managed client computer by using the Symantec Recovery Disk CD.
2. On the **Home** panel, click **Recover My Computer**.

   Note: If recovery points are stored on a CD or DVD and you only have one CD/DVD drive, you can eject the Symantec Recovery Disk CD now. Insert the CD or DVD that contains the recovery points.

3. On the **Welcome** panel of the wizard, click **Next**.
4. Do one of the following:
   - If Symantec Recovery Disk located recovery points, proceed to step 6
   - If Symantec Recovery Disk did not locate any recovery points, proceed to the next step.
5. In the View recovery points by list, set the option you want.

   See "View recovery point by options" on page 181.
6. Click **Next**.
7. In the **Drives to Restore** pane, check each recovery point that you want to recover.

   If necessary, add or remove recovery points from the list.

   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 that is based on its label, the name that is assigned to it, or by browsing the files and folders in the recovery point.
8. Optionally, in the **Drives to Restore** panel, **Source drive** column, select a drive whose recovery options you want to change and make effective during the recovery process, and then click **Edit**.
9. In the **Edit Target Drive and Options** panel, set the recovery options you want.

   See "Edit target drive options" on page 182.
10. Click **OK**.
11. In the **Drives to Recover** panel, set the options you want.

    See "Drives to recover options" on page 184.

12 Click **Next** to review the recovery options that you selected.

13 Select **Reboot when finished** if you want the computer to restart automatically after the recovery process finishes.

14 Click **Finish**.

15 Click **Yes** to begin the recovery process.

View recovery point by options

You can select how you want to list the available recovery points that you want to use for recovery from within Symantec Recovery Disk.

See "Recovering a computer locally by using Symantec Recovery Disk" on page 179.

Table 8-4 View recovery points by options

Option	Description
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. You can view a list of all available recovery points that may exist on your computer's local drives. Or, you can browse to locate a recovery point on a local drive or a shared network folder.
File name	Browse to another location to select a recovery point file (.V2i). See "About convert to virtual" on page 131. See "Configuring a one-time convert to virtual task" on page 143. If necessary, you can map a network drive to browse to a shared network folder for the file you want.

Table 8-4 View recovery points by options *(continued)*

Option	Description
System	Restore a computer that has multiple drives by using a system index file (.sv2i). A system index file reduces the amount of time that is needed to restore the drives. 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 Select this option, and then click **Browse**. Locate and select a system index file (.sv2i), and then click **Open**. If you select a network location, type your network credentials.

Edit target drive options

You can optionally set recovery options for a selected drive that you want to restore from within Symantec Recovery Disk.

See "Recovering a computer locally by using Symantec Recovery Disk" on page 179.

Table 8-5 Edit target drive options

Option	Description
Delete Drive	Delete a selected drive in the list to make space available to restore your recovery point. When you click Delete Drive, the drive is only marked for deletion. The actual deletion of the drive takes place after you click Finish in the wizard.
Undo Delete	If you delete a drive and then change your mind, click **Undo Delete** to return the drive to the list.

Table 8-5 Edit target drive options *(continued)*

Option	Description
Resize drive after recover (unallocated space only)	Select a disk (or volume label) that you want to resize after the recovery point is restored. Then, select this option and specify the new size in megabytes. The size must be greater than the identified size of the disk that you selected in the list.
Partition type	Sets the partition type as follows: ■ 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 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 Backup Exec System Recovery 2010 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.

Table 8-5 Edit target drive options *(continued)*

Option	Description
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 physical 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 from within the recovery environment. Select this option if any of the following situations are true: ■ You 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.

Drives to recover options

You can use the Drive to recover panel in the Recovery My Computer wizard to verify a recovery point before it is restore. You can also choose to use Restore Anyware if you recover to different hardware.

See "Recovering a computer locally by using Symantec Recovery Disk" on page 179.

Table 8-6 Drive to recover options

Option	Description
Verify recovery point before restore	Verifies 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	Select this option if any of the following are true: ■ You recover a system drive only (the drive on which Windows is installed; usually the C drive), or both a system drive and one or more data drives to new computer hardware. ■ You upgrade to new computer hardware from an older computer. ■ The motherboard on the computer has failed. If you recover a data drive only to new computer hardware, it is not necessary to select this option. See "About recovering locally to a computer with different hardware" on page 185. See "How to use Restore Anyware" on page 186.

About recovering locally to a computer with different hardware

The Backup Exec System Recovery Restore Anyware feature lets administrators restore a system drive of a Windows 2000/2003/XP/Vista/7 client computer. You can restore the system drive even if it has different hardware than was found in 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 on which the recovery point was originally made, you do not need to select Restore Anyware.

See "Recovering a computer locally by using Symantec Recovery Disk" on page 179.

How to use Restore Anyware

Restore Anyware lets you restore a recovery point onto new hardware. 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; it cannot be used to recover at a file and 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 use 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 hotfixes 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.
- Backup Exec 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 "About recovering locally to a computer with different hardware" on page 185.
  See "Recovering a computer locally by using Symantec Recovery Disk" on page 179.

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 176.

To recover files and folders locally by using Symantec Recovery Disk

1. Start the client computer by using the Symantec Recovery Disk CD.
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 and share that holds the recovery points. For example, \\computer_name\share_name.

If you still have problems, try entering the computer's IP address.

About using the networking tools in Symantec Recovery Disk.

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 to expand it.
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 recovery points on a network, you need access to the network to restore a computer or the files and folders from the recovery environment.

Note: Additional computer memory might be required to recover a computer across a network.

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 "About mapping a network drive from within Symantec Recovery Disk" on page 191.

About using the pcAnywhere thin host for a remote recovery

The Symantec Recovery Disk includes a pcAnywhere thin host, which lets you remotely access a computer in the recovery environment. The pcAnywhere thin host contains the minimum settings that are needed to support a single-use remote control session. The thin host requires an IP address for hosting a remote control session.

Note: You cannot deploy a thin host to the recovery environment. The thin host can only be started from Symantec Recovery Disk to host a remote control session in the recovery environment. The thin host in Symantec Recovery Disk does not support file transfers and cannot be used to add drivers for network or storage devices.

After you start the thin host from Symantec Recovery Disk, it waits for a connection from a remote computer. You can connect to the thin host to remotely manage a recovery or to perform other tasks in the recovery environment. You must use Symantec pcAnywhere to connect to the thin host.

See "About starting a computer locally by using Symantec Recovery Disk" on page 175.

See "Starting the pcAnywhere thin host for a remote recovery" on page 190.

Starting the pcAnywhere thin host for a remote recovery

You can use the pcAnywhere thin host from within Symantec Recovery Disk to perform a remote recovery of a computer.

See "About using the pcAnywhere thin host for a remote recovery" on page 189.

To start the pcAnywhere thin host for a remote recovery

- On either the Home or Network panels in the recovery environment, click **Start the pcAnywhere Thin Host**.

  The networking services are started if necessary. The thin host waits for a connection.

Remotely connecting to the pcAnywhere thin host

Symantec pcAnywhere lets you remotely connect to a computer that is running in the recovery environment. The computer must be running the pcAnywhere thin host that is included with Symantec Recovery Disk. The computer must also be waiting for a connection. After it is connected, the client computer can remotely manage a recovery or perform other tasks that are supported in the recovery environment.

Note: The client computer cannot transfer files or add additional drivers for network or storage devices on the computer that runs the thin host.

To remotely connect to the pcAnywhere thin host

1. Ensure that the computer to be remotely managed (the host) has started in the recovery environment. Also, ensure that the pcAnywhere thin host waits for a connection.
2. Obtain the IP address of the thin host computer.
3. On the client computer, in Symantec pcAnywhere, configure a remote connection item.

   For more information, see the *Symantec pcAnywhere User's Guide*.

   Note: You do not need to choose to automatically logon to the host on connection.

   ---

4. When you configure the connection in pcAnywhere, do the following:

- Select TCP/IP as the connection type.
- Specify the IP address of the host computer.
- Choose to automatically logon to the host on connection.
  If you do not include the logon information, you are prompted for it when you connect to the thin host.
- Type the following logon name:
  symantec
- Type the following password:
  recover

The thin host shuts down when there is an attempt to connect by using any incorrect configuration settings.

To prevent unauthorized users from tampering with the settings or launching a session without your permission, set a password for your remote connection item.

This option is available in the Remote Properties window on the Protect Item tab. The thin host does not support encryption.

5 In pcAnywhere, start the remote control session.

If the connection attempt is unsuccessful, the thin host must be restarted on the host computer before you make another attempt to connect.

6 Remotely perform the necessary tasks on the host computer.

The remote control session ends when the thin host is closed, when the thin host computer is restarted, or when the remote control session is ended.

After the host computer starts Windows, the client computer can deploy and connect a thin host on the computer to verify the success of tasks that were performed in the recovery environment.

About 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 for the computer on which you run Symantec Recovery Disk.

See "Configuring network connection settings" on page 192.

After you provide the static IP address and subnet mask address, you can enter the recovery environment. However, because 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.

The ability to map a network drive from within Symantec Recovery Disk is available from the following two locations:

- Symantec Recovery Disk **Home** page.
- The **Select a Recovery Point to Restore** panel in the **Recover My Computer** wizard.

If you chose not to start networking services at the time you started the recovery environment, you can still start the services from the **Network** page of Symantec 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

If you want to restore a recovery point that is located on a network drive or share, but you cannot map a drive or browse to the drive or share on the network (usually caused by the lack of an available DHCP service), 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 **Network Adapter Configuration** box, click **Use the following IP address**.
2. 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.

3 Click **OK**.

4 Click **Close** to return to the recovery environment's main menu.

5 In the **Network** pane, click **Ping a Remote Computer**.

6 Type the address of the computer that you want to ping on the network segment.

7 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 from the computer that you pinged.

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.

Getting a static IP address if pinging is unsuccessful

If you ping an address and the address does not respond, you can use the **ipconfig /all** command to determine the correct IP address.

To get an IP address if pinging is unsuccessful

1 On the computer that contains the recovery point that you want to restore, at a DOS prompt, type the following command, and then press **Enter**.

ipconfig /all

2 Write down the IP address that is displayed.

3 Return to the computer that is running the recovery environment and run the utility **Ping Remote Computer with this IP address**.

Viewing the properties of a recovery point

You can view various properties of a recovery point by using the Recovery Point Browser, a component of Backup Exec 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**.

See "Recovery point properties" on page 194.

Recovery point properties

You can view various properties of a recovery point by using the Recovery Point Browser, a component of Backup Exec System Recovery.

See "Viewing the properties of a recovery point" on page 193.

Table 8-7 Recovery point properties

Property	Description
Description	A user-assigned comment that is associated with the recovery point
Size	The total size (in megabytes) of the recovery point
Created	The date and time that the recovery point file was created
Compression	The compression level that is used in the recovery point
Spanned	Whether the entire recovery point file is spanned over several files
Password-protected	The password protection status of the selected drive
Encryption	The encryption strength that is used with the recovery point
Format	The format of the recovery point
Computer name	The name of the computer on which the recovery point was created
Restore Anyware	If 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 (Backup Exec System Recovery) 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 hard drive within a recovery point by using the Recovery Point Browser, a component of Backup Exec System Recovery.

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. Do one of the following:
   - On the menu bar, click **File** > **Properties**.
   - Right-click the recovery point, and then click **Properties**.

   See "Drive properties within a recovery point" on page 195.

Drive properties within a recovery point

You can view various properties of a hard drive within a recovery point by using the Recovery Point Browser, a component of Backup Exec System Recovery.

See "Viewing the properties of a drive within a recovery point" on page 195.

Table 8-8 Drive properties within a recovery point

Property	Description
Description	A user-assigned comment that is associated with the recovery point.
Original drive letter	The original drive letter that was assigned to the drive.
Cluster size	The cluster size (in bytes) that is used in a FAT, FAT32, or NTFS drive.
File system	The file system type that is used within the drive.
Primary/Logical	The selected drive's drive status as either the primary partition or the logical partition.
Size	The total size (in megabytes) of the drive. This total includes used and unused space.

Table 8-8 Drive properties within a recovery point *(continued)*

Property	Description
Used space	The amount of used space (in megabytes) within the drive.
Unused space	The amount of unused space (in megabytes) within the drive.
Contains bad sectors	Indicates if there are any bad sectors on the drive.

About the Support Utilities

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.

Appendix A

About backing up databases

This appendix includes the following topics:

About backing up VSS-aware databases

Backup Exec System Recovery 2010 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 2003 or later
- SQL Server 2005 or later
- Windows Server 2003-based domain controller or later

Note: Licensing Backup Exec 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 199.

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, Backup Exec 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. (Backup Exec 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, and Backup Exec 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 being created from the snapshot, the databases and 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 affecting productivity.

Additional points for backing up and restoring VSS-aware databases include the following:

- Backup Exec System Recovery supports Exchange Server 2003 or later, which implements VSS technology. If the database load is heavy, the VSS request might be ignored.
- Run backups during the lightest load time.
- Additional backup applications are not needed to run Backup Exec System Recovery with Exchange databases.
- Be sure that you have installed the latest service packs for your given database.
- Backup Exec System Recovery prevents VSS snapshots from occurring during the time the Backup Exec System Recovery is creating 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 Backup Exec 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 Backup Exec System Recovery recovery point, a VSS snapshot that was taken before the date and time of the Backup Exec System Recovery snapshot can no longer 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, and you should not rebuild or restore the database at the same time that you are backing it up. Finally, to avoid possible conflict, Backup Exec System Recovery does not let you take VSS snapshots and Backup Exec System Recovery snapshots at the same time.

About backing up non-VSS-aware databases

With Backup Exec System Recovery, you can create cold recovery point manually, warm recovery points automatically, or hot recovery points of non-VSS-aware databases.

Because the Backup Exec System Recovery 2010 Management Solution server also includes a database, you 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 do this, you can use Backup Exec System Recovery by way of the Backup Exec System Recovery 2010 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 Backup Exec System Recovery to create the recovery point, and then restart the database.

See "Creating cold, warm, and hot recovery points" on page 200.

When you automate the creation of a warm recovery point of a non-VSS-aware database, you run a command file in the backup policy, before data capture, to stop (quiesce) the database momentarily and commit all transaction logs to the hard disk. Backup Exec System Recovery instantaneously 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.

Because the virtual volume snapshot takes only a few seconds to create, the database is in the recovery point state momentarily, resulting in a minimal number of created log files.

See "To create a warm recovery point automatically" on page 200.

If a cold or warm recovery point is not possible in your organization, the next available option for backing up non-VSS-aware databases is a hot (or online) recovery point. Backup Exec 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 201.

See “Backing up Notification Server and the database” on page 201.

See “About backing up VSS-aware databases” on page 197.

Creating cold, warm, and hot recovery points

You can create cold recovery points manually, or warm recovery point 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 199.

See “Backing up Notification Server and the database” on page 201.

See “Creating an Independent Backup task” on page 115.

To create a cold recovery point manually

1. Stop the database manually.
2. Use Backup Exec System Recovery 2010 Management Solution to run a backup immediately using the Run Backup Policy task or the Independent Backup task.

   Backup Exec 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 already being 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 Backup Exec System Recovery to run the backup policy that includes the command files.

To create a hot recovery point

- Use Backup Exec System Recovery to create a recovery point without stopping or restarting the database.

  Backup Exec 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 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 Backup Exec System Recovery by way of the Backup Exec System Recovery 2010 Management Solution to create a "cold" recovery point.

See “To create a warm recovery point automatically” on page 200.

To back up Notification Server and the database

1. Install the Backup Exec System Recovery Install Plug-in and Backup Exec System Recovery.

   See “About installing the Backup Exec System Recovery Plug-in on client computers” on page 45.

   See “About installing Backup Exec System Recovery 2010, Backup Exec System Recovery 2010 Linux Edition, or LightsOut Restore 2010 on client computers ” on page 49.

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 2:00 A.M., the backup policy for the Backup Exec System Recovery 2010 Management Solution server should run earlier than 2:00 A.M. (or later if you prefer).

See "Scheduling options for creating recovery points " on page 92.

3 Make sure that the Backup Exec System Recovery 2010 Management Solution server computer is not assigned to any Groups that you may have defined in the console. This ensures that backup policies intended for other computers, do not get assigned to the server.

Appendix B

About Active Directory

This appendix includes the following topics:

About the role of Active Directory

When protecting a domain controller with Backup Exec System Recovery 2010 Management Solution, be aware of the following:

- If your domain controller is Windows Server 2003, it supports VSS. Backup Exec System Recovery 2010 Management Solution will automatically call VSS 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 prior to using Backup Exec System Recovery 2010 Management Solution to protect the full system. This process can be automated using an external command that is called by Backup Exec System Recovery 2010 Management Solution. When configuring a backup job, you have the option to enter external commands. This provides a simple process for protecting domain controllers that do not support VSS.
  See "About running command files during a backup" on page 112.
- In order 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. But a trust token contained in a recovery point cannot be updated by the domain controller automatically. Therefore, when a computer is recovered using a recovery point that contains an out dated token, the recovered computer cannot participate in the domain until it has been added to the domain by someone who has the required credentials.

In Backup Exec System Recovery 2010 Management Solution, this trust token can be re-established automatically if the computer is currently participating in the domain at the time the recovery process is started.

- In most cases, domain controllers should be restored non-authoritatively. This will prevent outdated objects in the Active Directory from being restored. Outdated objects are referred to as tombstones. Active Directory will 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 will prevent tombstone conflicts.

For additional details about protecting non-VSS aware domain controllers, see the white paper titled "Protecting Active Directory," located on the Web.

http://sea.symantec.com/protectingdc

You can also refer to the Symantec Knowledge Base

http://entsupport.symantec.com/umi/V-269-16

Appendix C

About backing up Microsoft virtual environments

This appendix includes the following topics:

About backing up Microsoft virtual hard disks

Microsoft Windows 7 and Windows 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 Backup Exec System Recovery 2010 Management Solution. You cannot back up a physical disk and its VHD counterpart in the same backup job using Backup Exec System Recovery 2010 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.

Microsoft Windows 7 now supports 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 Backup Exec System Recovery 2010 Management Solution. You cannot back up a physical disk and its VHD counterpart in the same backup job using Backup Exec System Recovery 2010 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 you do not include the VHD as another volume in the same backup. If you backup a physical

disk that hosts a VHD, 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 Web site.

http://technet.microsoft.com/en-us/library/dd440865(WS.10).aspx

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. To do this, 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 when the guest operating system on the virtual machine is not running (cold backup) or the Hyper-V VSS integration component is not installed in the virtual machine.

Note: Backup Exec System Recovery 2010 Management Solution is unable to back up clustered 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 Backup Exec System Recovery 2010 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 machine must be running Windows Server 2003 or later.
  If the guest machine is running Win 2000, Win XP 32- or 64-bit, 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, you must first uninstall the Virtual Server 2005 integration component from the virtual machine before installing the Hyper-V VSS integration component.

- The guest virtual machine should be configured to only use basic disks, not dynamic disks.
  This is the default for installing a Windows virtual machine.
- All the volumes on the fixed disks must support the creation of snapshots.

If you attempt to perform a backup when the conditions above are not met, Backup Exec System Recovery 2010 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.

To restore a virtual machine, you must restore the recovery point of the host computer. The host computer recovery point must include the volume that holds the virtual machine you want to restore. You cannot restore a specific virtual machine.

http://entsupport.symantec.com/umi/V-306-2

Appendix D

About Backup Exec System Recovery 2010 Management Solution and Windows Server 2008 Core

This appendix includes the following topics:

About Backup Exec System Recovery 2010 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 Backup Exec System Recovery 2010 can be installed on Windows Server 2008 Core, it is an agent only install. Windows Server 2008 Core does not support .NET. Because of this, the Backup Exec System Recovery GUI cannot be installed. Backup Exec System Recovery is supported on Windows Server 2008 Core via a headless agent only. You can install Backup Exec System Recovery 2010 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 machine. This means that after installing the agent on a Windows Server 2008 Core machine, you must connect to it from a remote machine running Backup Exec System Recovery 2010 or Backup Exec System Recovery 2010 Management Solution Management Solution in order to back it up or restore it.

Prior to installing the agent remotely and managing backup and restore functions on a Windows Server 2008 Core machine, 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 machine, see the Microsoft Web site.

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 machine, you must reinstall it before installing Backup Exec System Recovery 2010.

Installing Backup Exec System Recovery 2010 on Windows Server 2008 Core using commands

Three options exist for installing Backup Exec System Recovery 2010 on a Windows Server 2008 Core system. They are

- Full silent install with logging
- Agent only silent install with logging

To run a full install with GUI support

1. On the Backup Exec System Recovery 2010 CD, browse to and run AutoRun.exe.

   This will launch a graphical environment (GUI) where you complete the remainder of the installation.

2. Complete the installation process by following the steps in the installation wizard.

   Even though the full Backup Exec System Recovery is installed, only the agent is needed and used on Windows Server 2008 Core.

To run a full silent install with logging

1. On the Backup Exec System Recovery 2010 CD, change to the Install directory.
2. Run the following command:

   ```
   Setup.exe /s /v"/qn /l*v %temp%\BESRInstall.log"
   ```

   Even though the full Backup Exec System Recovery is installed, only the agent is needed and used on Windows Server 2008 Core.

To run an agent-only silent install with logging

1. On the Backup Exec System Recovery 2010 CD, change to the Install directory.
2. Run the following command:

   Setup.exe /s /v"/qn AddLocal=Agent,Shared,BESRSecurityShortCut /l*v %temp%\BESRInstall.log"

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

Backup Exec System Recovery supports the use of Google Desktop for searching file names in recovery points.

Note: Backup Exec Retrieve is also supported, but it must be installed by your company's IT department. When they install it, there is nothing you have to do to enable it. Ask your IT department for details.

When a backup runs, Backup Exec 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, Backup Exec 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 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 files that are required by search engines for generating searchable indexes are appended to recovery points as they are created. 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.

To use this feature 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 215.
Enable Google Desktop support	A Google plug-in for Backup Exec 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 "To enable Google Desktop support" on page 215.
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. See "To enable search engine support for a backup policy" on page 215.

See "Recovering files using Google Desktop's Search Desktop feature" on page 216.

See "If a file cannot be found using Google Desktop" on page 216.

Enabling search engine support in recovery points

You turn on search engine support in recovery points by installing Google Desktop, enabling Google Desktop support, and enabling search engine support in a backup policy.

See "About using a search engine to search recovery points" on page 213.

See "Recovering files using Google Desktop's Search Desktop feature" on page 216.

To install Google Desktop

1. Start Backup Exec 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 Backup Exec System Recovery Options window.

   For more information, visit desktop.google.com.

To enable Google Desktop support

1. Start Backup Exec System Recovery on the client computer.
2. Click **Tasks > Options > Google Desktop**.
3. Check **Enable Google Desktop File and Folder Recovery**.
4. Click **OK**.

   This option is not available if you do not have Google Desktop installed. Install Google Desktop, and then repeat this procedure.
5. Click **OK** to install the Google plug-in.

To enable search engine support for a backup policy

- In Backup Exec System Recovery 2010 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.

  See "Advanced recovery point options" on page 107.

Recovering files 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 located and recover files using Google Desktop.

See "If a file cannot be found using Google Desktop" on page 216.

See "About using a search engine to search recovery points" on page 213.

See "Enabling search engine support in recovery points" on page 215.

To recover files 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. When the file opens in the associated application, click **File > Save As** to save the recovered file.

   You can also right-click the search result and click Open to open the recovery point in the Recovery Point Browser.

If a file cannot be found using Google Desktop

If you are certain that the file is included in a recovery point that has search engine support enabled, but the file is not found, do the following:

- 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.
- 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. This option must be checked or 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 on 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 you are connected and logged on with the correct credentials.
- Adding **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. When you add the extension to the search string, it eliminates search results that are not found in a recovery point.

- 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 using Google Desktop's Search Desktop feature" on page 216.

Index

D

E

F

P

R

S

T

U

V