VERITAS™

Storage Exec 5.3

Administrator's Guide

Windows

N159628

December 2004

Disclaimer

The information contained in this publication is subject to change without notice. VERITAS Software Corporation makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. VERITAS Software Corporation shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual.

VERITAS Legal Notice

VERITAS Software Corporation
350 Ellis Street
MountainView, CA 94043
USA
Phone 650-527-8000
Fax 650-527-2908
www.veritas.com

Contents

Preface

Welcome to the *Storage Exec Administrator's Guide*. This document contains the instructions you will need to install and use Storage Exec.

The Preface includes the following topics:

What's in This Manual

The following table summarizes the chapters in this document.

Chapters in This Manual

Chapter	Description
Preface	The preface summarizes the contents of this document and provides information about how to get technical support.
"Introduction" on page 1	Introduces you to Storage Exec and the benefits it provides, and describes the features new to version 5.3.
"Installing Storage Exec" on page 11	Provides installation and upgrade instructions. Also lists the requirements needed to install and run Storage Exec.
"Getting Started" on page 33	Provides instructions for performing common tasks with Storage Exec.
"Managed Resources" on page 45	Provides an overview of what managed resources are, and how to create and use them.

Chapters in This Manual (continued)

Chapter	Description
"Space Allocation" on page 63	Contains material related to the Storage Exec space allocation feature.
"File Blocking" on page 83	Contains material related to the Storage Exec file blocking feature.
"File Groups" on page 97	Provides an overview of what file groups are, and how to create and use them.
"Report Queries" on page 103	Describes how to define the content and appearance of a report.
"Reports" on page 121	Documents how to run reports that come with Storage Exec and how to create reports.
"Integration with Backup Exec" on page 139	Describes how Storage Exec works with VERITAS Backup Exec for Windows Servers via SmartLink.
"Audit Trail" on page 147	Documents how to use and interpret the audit data that Storage Exec can store.
"Preferred Computers and Groups" on page 153	Provides an overview of what preferred computers and groups are, and how to create and use them.
"Storage Exec Enterprise Administration Option" on page 159	Provides instructions for using Storage Exec with the Active Directory.
"Working with Network Appliance Filers" on page 173	Provides instructions for using Storage Exec to manage storage on Network Appliance Filers.
"Remote Server Agent" on page 185	Documents the installation and use of the Storage Exec Remote Server Agent.
"Remote Workstation Agent" on page 197	Documents the installation and use of the Storage Exec Remote Workstation Agent.
"Command Line Interface" on page 209	Documents the Storage Exec commands you can use with the Storage Exec command line interface.
"Cluster Support in Storage Exec" on page 221	Provides information about cluster support in Storage Exec.

Chapters in This Manual (continued)

Chapter	Description
"Permissions" on page 229	Describes the permissions that different classes of users need to run Storage Exec.
"Accessibility and Storage Exec" on page 243	Documents the Storage Exec accessibility features, such as keyboard navigation.

Getting Help

VERITAS offers you a variety of support options.

- The VERITAS Support Web Site (http://support.veritas.com) allows you to:
  - contact the VERITAS Support staff and post questions to them
  - get the latest patches, upgrades, and utilities
  - view the Storage Exec frequently asked questions (FAQ) page
  - search the knowledge base for answers to technical support questions
  - receive automatic notice of product updates
  - find out about Storage Exec training
  - read current white papers related to Storage Exec
- Subscribe to the VERITAS email notification service to be informed of software alerts, newly published documentation, Beta programs, and other services. Go to http://support.veritas.com. Select a product and click **E-mail Notifications** on the right side of the page. Your customer profile ensures you receive the latest VERITAS technical information pertaining to your specific interests.
- Telephone support for Storage Exec is only available with a valid support contract. To contact VERITAS for technical support, go to http://support.veritas.com. Specify Storage Exec as the product and click **Contact Support** on the right side of the page. Find the appropriate phone number in the list that displays.

Storage Exec Manuals

The table below lists other resources VERITAS provides to help you learn about Storage Exec.

Related VERITAS Documentation

Item	Description
Storage Exec Quick Installation Guide	Provides the instructions needed to install Storage Exec.

Related Resources

As explained in "Integration with Backup Exec" on page 139, Storage Exec integrates with VERITAS Backup Exec for Windows Servers. To learn more about Backup Exec, read the *Backup Exec for Windows Servers Administrator's Guide*.

Conventions

The following conventions apply throughout the documentation set.

Typographical Conventions

Convention	Description
GUI Font	Depicts graphical user interface (GUI) objects, such as fields, listboxes, and menu commands. For example: Enter your password in the **Password** field.
Italics	Used for placeholder text, book titles, new terms, or emphasis. Replace placeholder text with your specific text. For example: Replace *filename* with the name of your file.
`Code`	Shows what commands you need to type, to identify pathnames where files are located, and to distinguish system or application text that is displayed or that is part of a code example.
Key+Key	Shows that you must hold down the first key while pressing the second key. For example: Ctrl+S means hold down the Ctrl key while you press S.

Tips, notes, and cautions are used to emphasize information. The following samples describe when each is used.

Tip Used for nice-to-know information, like a shortcut.

Note Used for important information that you should know, but that shouldn't cause any damage to your data or your system if you choose to ignore it.

Caution Used for information that will prevent a problem. Review cautions carefully to determine if they will impact your environment.

Introduction 1

This chapter explains the benefits of using VERITAS Storage Exec™ and lists the features of the new release. The topics in this chapter include:

Introduction to Storage Exec

Welcome to Storage Exec, a comprehensive Windows file blocking, quota management, and storage reporting solution. Storage Exec addresses the following key storage management areas: controlling and monitoring disk space usage, and reporting on storage content.

Storage Exec can solve immediate storage problems with minimal setup and planning. It includes features like auto detection, detailed reporting, and policies. Storage policies can be established and enforced with a minimum of administrative intervention. Storage reporting allows storage problems to be quickly isolated and resolved on a real-time basis.

Storage Exec:

- Limits the users' disk space by monitoring and enforcing disk usage policies in real time.
- Generates detailed reports of space consumption for administrators and end users.
- Warns users—in real time—as they approach maximum storage limits or attempt to store blocked file types.
- Prevents unwanted files from being saved on the servers.

Product Benefits

Control: Storage Exec controls the users' storage habits and prevents runaway disk consumption. Simply select the appropriate disk space allocations by user, workgroup, or enterprise.

Enforcement: Storage Exec enforces pre-configured storage policies that have been set.

Continuity: Storage Exec eliminates or reduces system crashes, downtime, and loss of productivity due to lack of disk space or unnecessary space upgrades.

User Awareness: Storage Exec notifies the users who attempt to violate a certain storage policy and educates them about appropriate disk space usage.

Efficiency: Storage Exec maximizes disk space usage and prolongs the performance of disk space investment, lowering overall storage total cost of ownership.

Recovery: Storage Exec reclaims wasted disk space and identifies files that are not backed up.

What's New in Storage Exec

Storage Exec 5.3 has a variety of new features and capabilities.

What's New in Storage Exec

New Feature	Description
Licensing and deployment	Storage Exec™ is now available in multiple editions that can be purchased to fit your environment: • *Storage Exec* offers storage quota management, file auditing, file blocking, and basic reporting capabilities. Add-on options allow you to extend the functionality of Storage Exec to remote Windows computers. • *Storage Exec Small Business Server Edition* offers the same functionality as the full product, but is installed on and works with Microsoft Small Business Server Premium and Standard Editions only. • *Storage Exec QuickStart Edition* is designed for single server environments and includes standard Storage Exec functionality, such as storage quota management, file auditing, file blocking, and basic reporting capabilities. Add-on options and remote agents are not supported.
Enhanced installation	With a completely redesigned installation program, Storage Exec makes it easier than ever to configure your systems. In addition, you can install the remote agents from the Administration Console to remote Windows computers across the network.
Information Desk-based Administration Console	Storage Exec now provides a new overview page that guides you through various Storage Exec tasks. The Storage Exec Information Desk offers links to commonly asked questions, configuration dialog boxes, and configuration wizards.
Advanced configuration wizards	Storage Exec includes new configuration wizards that are designed to simplify the configuration of Storage Exec in complex environments. • With the Enterprise Administration Wizard, you can configure a centralized repository for policy definitions and management. The Storage Exec Enterprise Administration Option leverages Microsoft Active Directory to enable the application of storage policies across the enterprise. • Using the Cluster Configuration Wizard, you can add Storage Exec resources to existing resource groups to provide high availability.

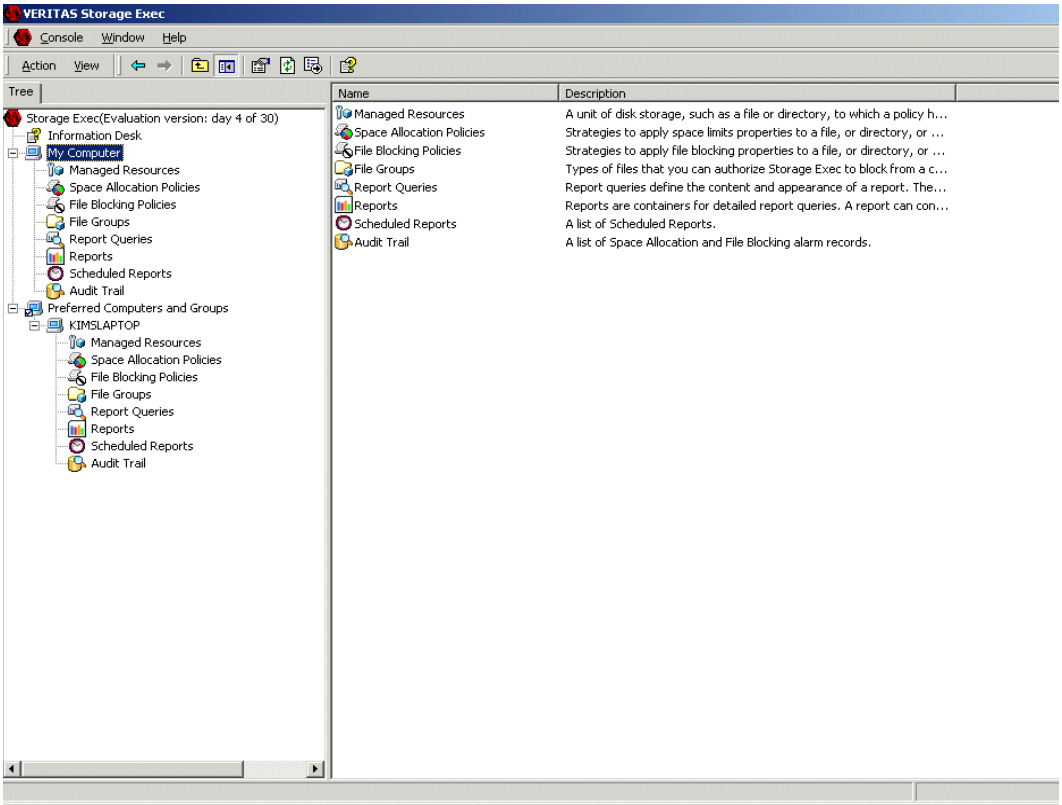
What's New in Storage Exec (continued)

New Feature	Description
Integration with Backup Exec for Windows Servers	When using Backup Exec 9.1 or 10.0 for Windows Servers in your environment, Storage Exec seamlessly integrates with Backup Exec via Backup Exec ™ SmartLink. This integration enables you to immediately back up or archive data from Storage Exec reports using Backup Exec.
Microsoft certified	Storage Exec 5.3 is now fully Microsoft Windows certified by Veritest, ensuring that Storage Exec works in supported Microsoft environments.
New options and agents	With new Storage Exec add-on options and agents, you can enhance the functionality of Storage Exec, as well as extend Storage Exec functionality to remote Windows computers. ◆ **Storage Exec Enterprise Administration Option** provides integration with Microsoft's Active Directory, which enhances reporting and enables global policies on multiple computers. ◆ **Storage Exec Advanced Reporting Option** offers additional reports that are not available in Storage Exec, while also providing advanced report writing tools. ◆ **Storage Exec Network Appliance Option** integrates with and uses ONTAP qtrees to provide quota management and reporting for Network Appliance Filers. ◆ **Storage Exec Remote Server Agent**™ adds quota management, content filtering and file blocking to a remote server. When used in conjunction with a Storage Exec Server, it allows administration from a remote console. ◆ **Storage Exec Remote Workstation Agent**™ offers content filtering and file blocking for remote workstations running Microsoft Windows 2000 Professional and Microsoft Windows XP operating systems. When used in conjunction with Storage Exec Server, it allows administration from a remote console.
Quick Installation Guide	The *Storage Exec Quick Installation Guide* is a printed manual that is shipped with Storage Exec. It provides the information you need to install Storage Exec. The *Storage Exec Quick Installation Guide* does not replace the *Storage Exec Administrator's Guide*, which is available in electronic (PDF) format on the Storage Exec installation CD and in printed format from the VERITAS WebStore.

Overview of the Administration Console

The Administration Console is divided into two panes.

Storage Exec Administration Console



- The left pane is the management pane and includes the **Tree** tab, which is also known as the console tree. The console tree displays items that are available in a given console.
- The right pane is the details pane. The details pane displays information about items selected in the console tree.

The management pane for Storage Exec contains the following items:

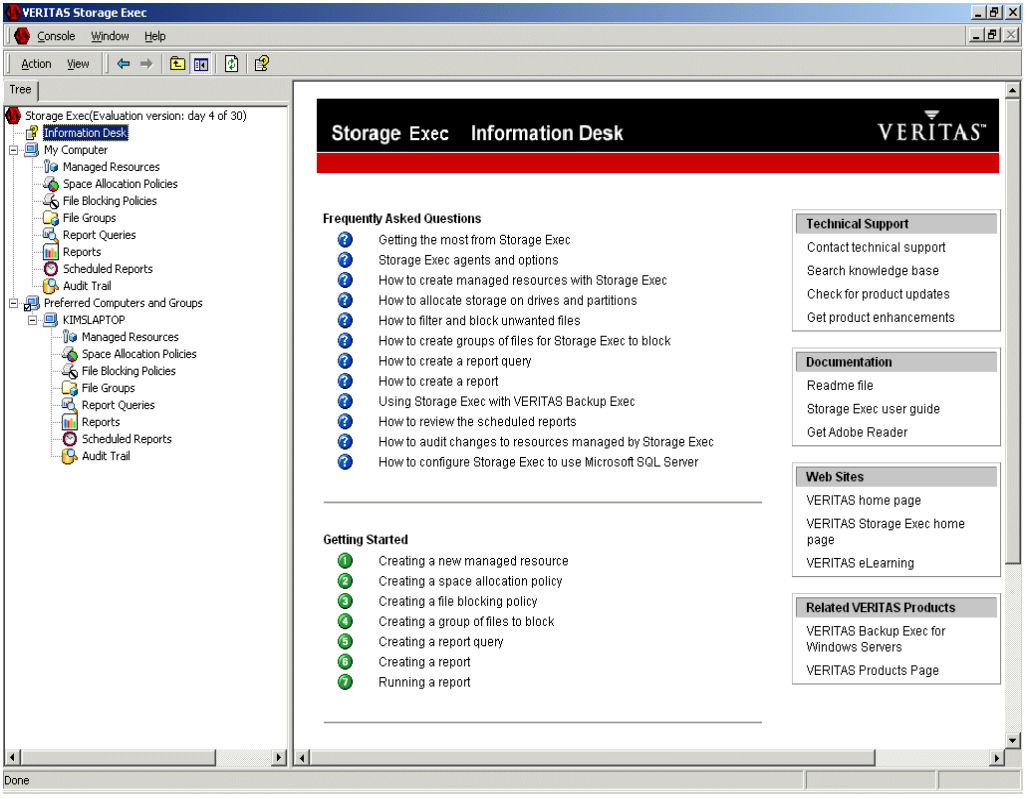
- **My Computer**. Storage Exec is a Storage Resource Management system that provides disk space quota monitoring and control in real time. Use the following tools to monitor and control disk space:
  - **Managed Resources**. Configure resources, such as files, directories, shares, or partitions, to manage and control space allocation and file blocking settings. Create new managed resources, delete existing managed resources, and view or modify the properties of the managed resources.
  - **Space Allocation Policies**. Set policies to limit the amount of data stored in resources that Storage Exec manages.
  - **File Blocking Policies**. Set policies to block users from creating and copying certain types of files.
  - **File Groups**. Set up and manage groups of files that you want to block or allow.
  - **Report Queries**. Define the content and appearance of reports.
  - **Reports**. Run reports that help you manage space effectively.
  - **Scheduled Reports**. View a list of reports that are scheduled to run.
  - **Audit Trail**. View space allocation and file blocking actions.
- **Preferred Computers and Groups**. Group commonly used computers in one place.

If you are running the Storage Exec Enterprise Administration Option, you will see additional entries on the management pane. For more information, see "Introduction to the Enterprise Administration Option" on page 159.

Overview of the Information Desk

The Information Desk has links to the list of new features in this release and tasks such as running wizards. The information desk also provides links to the ReadMe file, the online documentation, the technical support web site, and the VERITAS company web site.

Information Desk



Best Practices for Storage Exec

This section identifies and explains general best practices.

- Establish corporate Storage Resource Management (SRM) policies.
  - Decide how much space to give each user. The space limits are determined based on the result of a storage audit. The audit should show how much space the users currently have, and whether the disk space is being used appropriately (business data vs. personal or illicit data). Space limits are also based on available capacity.

    The space limit alarms may take many forms based on an individual need and the political nature of limiting disk space. Some organizations prefer to monitor all users and enforce limits only for certain offenders. Most organizations will use at least passive limits with alarms. This encourages users to participate in storage management. More strict environments, such as a university, would enforce all users and use alarms to warn of the space limit. A typical alarm includes the notification message and specifies how the message will be delivered (screen pop-up or email) and who will receive the message.
  - Determine alarm thresholds. Alarm thresholds allow you to specify actions to occur when a threshold value (a percentage of the space allocation) is exceeded. Although multiple alarm settings can be configured, usually only two or three alarms are enough with the thresholds set at 80, 90, and 100 percent. A threshold is activated only once until the percentage of used space drops below the threshold.

    For example, if threshold 3 is set at 70 percent and threshold 2 is set at 80 percent and 71 percent of the space limit is used, threshold 3 is activated. Threshold 3 will not be activated again, unless the value first drops below 70 percent. Threshold 2 will be activated if more files are saved and the value increases to above 80 percent.

    For more information about the space allocation alarm thresholds, read the section “Setting Up Space Allocation Alarm Notification” on page 74.
  - Determine notification messages to users. A customized notification message can be sent to a user when a space allocation or file blocking alarm is activated,

    For a space allocation alarm, the following message could be sent to the user: “You are approaching the disk space quota on managed resource ‘C:\Users\MGold.’ Delete or archive unneeded files from this managed resource to free additional space." For more information about the space allocation notification messages, read the section “Setting Up Space Allocation Alarm Notification” on page 74.

For a file blocking alarm, the following message could be sent to the user: "You may have attempted to save media files on [SERVER NAME]. These files are not permitted. Contact John Smith at extension 1234 with questions." For more information about the file blocking notification messages, read the section "Setting Up File Blocking Alarm Notification" on page 90.

- Determine which file types to block. Consider that some executable files with extensions such as .exe and .vbs could be harmful viruses. Illegal .mp3 and .mpg files may take up valuable disk space or expose your company to unnecessary legal risks. Include unwanted file types in the list of unauthorized files when creating a new file group. For more information about the unauthorized files and file groups, read "Introduction to File Groups" on page 97.

- Tell users that Storage Resource Management (SRM) is beginning. Specify when the SRM will start and what is being monitored. Explain the benefits to the organization and let the users know whom to contact if they have questions or issues (for example, whom to ask when they want to increase a space allocation).

  For example, you may send the following email to all users in your organization or in a certain department: "As part of our organization's storage resource management policy, limits on users' disk space will be set on the company server to conserve space. The disk space quota per user is X. If you require additional disk space, contact HelpDesk@company.com."

- Create managed resources and apply policies during off hours. Most managed resource-policy relationships are created when new managed resources are created. We suggest that the initial application of space allocation policies should be done during off hours because creating managed resources requires a disk scan.

  Although the persistent monitoring of disk I/O for policy enforcement adds less than one percent to overall system overhead, the initial application of a space allocation policy requires a one-time scan of the managed resource to determine current space consumption. The processing required to perform this scan depends on the number of files stored in the resource. If it is a large folder, the scan can take some time and the processing will be reflected primarily in the system process and the QuotaAdvisor Server service (the Storage Exec service, which manages space limits and sends alarms).

- Monitor overall disk consumption. Storage Exec provides detailed disk consumption information in a format that allows administrators to take corrective actions.
  - Storage Exec ships with pre-configured policies for monitoring disk consumption. For example, when the "Partition Alert" policy is applied to a partition, it calculates the size of the partition and sets the space allocation value to that amount.
  - When you create space allocation policies or managed resources, you may configure multiple alarm thresholds to customize to your needs.
  - You may generate certain reports that allow you to monitor space by partition. For example, the Disk Drive Summary report lists all partitions and their capacity, free space and type.

  This practice saves the organization money by reducing wasted space on storage media and helps avoid down time associated with insufficient disk space. Administrators will be notified when disks approach their capacity so that they can take corrective actions before disk consumption reaches critical levels.
- Identify user reports. A user report is typically implemented in a space allocation policy that directly affects a user. When the user's space consumption reaches critical levels based on SRM policies, the user should be notified and provided with detailed reports that help him or her recover wasted space. Storage Exec uses Active HTML controls within Internet Explorer, which allows administrative actions to be taken against files listed in the report.

  For example, a file can be launched, copied, moved, or deleted directly from the browser. This enables system administrators to delegate file management back to the users who own the data.

  Informed users can take a corrective action themselves, decreasing the burden on the system administrator.

Installing Storage Exec 2

This chapter contains the following sections:

- "System Requirements" on page 12 provides a list of the minimum hardware and software requirements that should in place before you install and run Storage Exec.
- "Storage Exec Installation Overview" provides an overview of the installation requirements that must be considered before beginning the Storage Exec installation.
- "Installing Storage Exec Server" on page 16 provides the instructions necessary for installing Storage Exec using the installation program provided on the Storage Exec CD.
- "Installing Storage Exec Server from the Command Line" on page 21 provides the instructions necessary for installing Storage Exec from a Windows command prompt using command line syntax.
- "Starting Storage Exec" on page 18 provides the instructions necessary for starting Storage Exec after you complete the installation.
- "Installing the Storage Exec Remote Administration Console on Remote Computers" on page 19 provides the instructions necessary for installing the Storage Exec Remote Administration Console on remote computers.
- "Upgrading from Previous Versions of Storage Exec and Storage Manager" on page 28 provides instructions for upgrading previous versions of Storage Exec.
- "Repairing Storage Exec" on page 24 provides the instructions for repairing a Storage Exec installation.
- "Uninstalling Storage Exec" on page 25 provides the instructions necessary for uninstalling Storage Exec.
- "Configuring Microsoft SQL Server as the Centralized Storage Exec Database" on page 30 provides the steps necessary for configuring Storage Exec to use Microsoft SQL Server as its repository for audit and trending data.

Installation instructions for the Storage Exec Remote Server Agent and the Storage Exec Remote Workstation Agent can be found in their respective appendixes in this user guide. For more information, see "Remote Server Agent" on page 185 and "Remote Workstation Agent" on page 197.

System Requirements

The following are the minimum system requirements for running this version of Storage Exec. Following the installation of Storage Exec, a reboot may be required.

Storage Exec minimum system requirements

Operating System	Microsoft Windows 2003 Server family. Microsoft Windows Storage Server 2003 Standard or Enterprise. Microsoft Windows 2000 Server family. Microsoft Windows XP Professional Service Pack 1 or later. Microsoft Windows NT 4 Workstation or Server; Service Pack 6a or later. Microsoft Small Business Server 2003 Standard. Microsoft Small Business Server 2003 Premium. Microsoft Small Business Server 2000. **Note** Please refer to the Storage Exec Software Compatibility List (http://support.veritas.com/rd/se-compatibility.htm) for a complete list of supported environments.
For the Network Appliance Options	ONTAP 6.4 or later.
Internet Browser	Internet Explorer 6.0 or later.
Processor	Intel Pentium, Xenon, or compatible.
Memory (RAM)	Storage Exec Server • Required: 256 MB RAM • Recommended: 521 MB (or more for better performance) **Note** RAM requirements may vary depending on operations performed, the options installed, and the specific system configuration.

Storage Exec minimum system requirements

Virtual Memory Recommendations	20 MB above the Windows recommended size for a total paging file size (total for all disk volumes). To view or set the paging file size: On Windows 2000: Point to **Settings**, and then click **Control Panel**. Double-click **System**, click the **Advanced** tab, and then click **Performance Options**. Click **Change** to reset the paging file size for all drives. On Windows Server 2003 and Windows XP: Go to **Control Panel** and double-click **System**. Click the **Advanced** tab, and then in **Performance**, click **Settings**. Click the **Advanced** tab, and then in **Virutal memory**, click **Change** to reset the paging file size for all drives.
Installation Disk Space	70 MB (typical installation). 90 MB (includes all options). **Note** Disk space requirements may vary depending on operations performed, the options installed, and the specific system configuration.
Other Hardware	Network interface card or virtual adapter device CD-ROM drive Mouse (recommended) Printer (optional for printing reports).

Related Topics:

- "Storage Exec Installation Overview" on page 14
- "Installing Storage Exec Server" on page 16
- "Installing the Storage Exec Remote Administration Console on Remote Computers" on page 19

Storage Exec Installation Overview

When installing Storage Exec Server, use the installation program on the Storage Exec CD, or install it from the command line, which is referred to as *Silent Mode Installation*. The silent mode installation uses the **setup.exe** program on the Storage Exec CD. If you are installing an evaluation version of Storage Exec, you can also install the Storage Exec remote agents and the Storage Exec Remote Administration Console, all of which will be active until the evaluation period expires. Note the following information before installing Storage Exec:

Storage Exec installation requirements

Rights	To install Storage Exec, Administrator rights are required, or the account must belong to an Administrator-equivalent group.
The Storage Exec Service Account	All Storage Exec services on the Windows computer run in the context of an existing user account configured for the Storage Exec system services. To use an existing user account as a service account, enter the name and password of an Administrator account when prompted during installation. If this computer is in a domain, enter a Domain Administrators account, or an equivalent account that is part of the Domain Administrators group. In the Domain list, select or enter the Domain name. If this computer is in a workgroup, enter an Administrators account, or an equivalent account that is part of the Administrators group on the computer. In the Domain list, select or enter the computer name. The account designated for Storage Exec services - whether it is a new account or an existing user account - will be assigned the following rights: ◆ Authenticate as any user and gain access to resources under any user identity. ◆ Create a token object, which can then be used to access any local resources. ◆ Log on as a service. ◆ Administrative rights (provides complete and unrestricted rights to the computer). ◆ Backup operator rights (provides rights to restore files and directories). ◆ Manage auditing and security log.

Storage Exec installation requirements (continued)

	Due to security implementations in Microsoft Small Business Server, the service account must be *Administrator*. On a computer running Windows Server 2003 or Windows XP, you cannot install Storage Exec using a service account that has a blank password. If you attempt to do so, the following error message displays when Storage Exec services are created: "The given password is not correct for account [server]\[username]." You can configure Windows to allow for blank passwords. For more information, see your Windows documentation.

Related Topics:

- "System Requirements" on page 12
- "Installing Storage Exec from the Installation CD" on page 16
- "Installing Storage Exec Server from the Command Line" on page 21

Installing Storage Exec from the Installation CD

The Storage Exec CD includes an installation program that guides you through the installation process for Storage Exec Server and its Remote Administration Console. You will be prompted for a serial number for Storage Exec Server during the installation process.

Note If you are installing Storage Exec through Terminal Services and the installation media is on a shared drive (CD-ROM or network share), Storage Exec must be installed using a UNC path. Installation using mapped drives is not supported.

Related Topics:

- "Installing Storage Exec Server from the Command Line" on page 21
- "Installing the Storage Exec Remote Administration Console on Remote Computers" on page 19

Installing Storage Exec Server

Use the following steps to install Storage Exec Server on a local computer.

▼ **To install Storage Exec Server using the installation CD:**

1. At the local computer, place the Storage Exec CD in the local computer's CD drive.

   The Windows Autorun feature automatically launches the Storage Exec Browser.

   Note If the Storage Exec Browser does not automatically start, start the Windows Explorer and navigate to the CD drive containing the Storage Exec CD media. Double-click **Browser.exe** to start the Storage Exec browser.

2. Select a language and then click **OK**.
3. Click **Install Storage Exec**.
4. Click **Next** to continue with the installation.
5. Select **I accept the terms of the license agreement**, and then click **Next**.
6. On the VERITAS Storage Exec Install Menu, select **Local Install**, which installs both Storage Exec Server software and user-selected options on the computer where you are running the Storage Exec installation program.

If you are installing on a computer where Storage Exec was previously installed, and you did not remove all Storage Exec-related data during the previous uninstall process, click the additional check box to enable the restoring of existing Storage Exec data to your new Storage Exec installation.

7. Clear the check box for **Remote Agent Install**, if it is selected.

8. Click **Next**.

9. Type the serial numbers for Storage Exec and any options. You can also import an existing scsernum.xml file to enter the serial numbers.

   - To manually enter the serial numbers for Storage Exec Server and any additional options, type the serial numbers into the field, and then click **Add**. When finished, click **Next**.

     Note After clicking **Next**, the serial numbers you entered are saved to a file named scsernum.xml, which is located in the Windows directory.

   - To import the serial numbers from a file, click **Import**, and then browse the Windows directory. Select an existing scsernum.xml file and then click **Next**.

     A serial number is not required to install an evaluation version. Clicking **Next** without entering a serial number displays a message informing you that an evaluation version of Storage Exec Server will be installed.

10. Review the local options to be installed.

    Options that will not be installed have a red "X" displayed in the option icon. To enable any of these options, click the icon to clear the X, and then follow the prompts to install it. If the option icon is gray, the option is not available.

11. To accept the local options for installation, and to accept the default destination folders for both the Storage Exec program files and the Storage Exec databases, click **Next**.

    Note To select a different destination folder for either the Storage Exec program files or the Storage Exec databases, click **Change**, and follow the prompts.

    If you are reinstalling Storage Exec or upgrading from previous versions of StorageCentral, the Change buttons do not appear, as the original installation folders are used.

12. Provide a user name, password and domain name for the Storage Exec system services to use and then click **Next**. For more information, see "The Storage Exec Service Account" on page 14.

13. Review the Storage Exec Installation Summary screen and then click **Next**.

    The Storage Exec installation begins.

    When the installation finishes, you can review the installation log file, which is named `scinst.log`. The log file is created in the Windows directory on the computer where Storage Exec is installed. This file lists any errors that may have occurred during installation.

14. Click **Finish** and restart the computer.

Related Topics:

- "Installing the Storage Exec Remote Administration Console on Remote Computers" on page 19
- "Uninstalling Storage Exec using Windows Add/Remove Programs" on page 25

Starting Storage Exec

▼ **To start Storage Exec:**

❖ To start the Storage Exec, click **Start**, point to **Programs**, and then click **VERITAS Storage Exec**.

If you selected the option to add an icon to your desktop when you installed Storage Exec, you can also double-click the icon to start Storage Exec.

Installing the Storage Exec Remote Administration Console on Remote Computers

This section provides the steps necessary for installing the Storage Exec Remote Administration Console on remote Windows computers on your network.

Note The Storage Exec Remote Administration Console cannot be installed on a remote computer running Windows NT 4.0.

▼ **To install the Storage Exec Remote Administration Console on a remote computer:**

1. At a computer running Storage Exec Server, click **Start**, point to **Settings**, click **Control Panel**, and then double-click **Add or Remove Programs.**
2. On the Add or Remove Programs dialog box, select **VERITAS Storage Exec**, and then click **Change.**
3. On the Welcome screen, click **Next.**
4. On the Program Maintenance screen, clear the check box for **Local Install**.
5. Click the check box for **Remote Agent Install** and then click **Next.**
6. Under Destination Systems, right-click **Windows Options/Agents** to display a shortcut menu for selecting the remote computer or computers that you want to install to.
7. On the shortcut menu, do one of the following:
   a. Click **Add Remote Computer**, and then browse the list to select all of the remote computers that you want to install to, and then click **Next.**
   b. Click **Add Remote Computer Manually**, and then type the Domain and Computer Name, and then click **OK**.

      You can add as many remote computers as you want; the Remote Administration Console will be installed on all that computers that appear in the Destinations Systems pane.
8. Type the user name, password, and domain credentials of an account that has administrative rights on the remote computers, and then click **OK**.

   The remote computers selected appear in the Destination Systems pane.

9. Click a computer name and then select **Remote Administration Console**.

10. Click **Next.**

11. Review the Storage Exec Installation Summary screen and then click **Next**.

    The Remote Installation Status screen appears, and the Remote Administration Console is installed on the remote computer.

12. Click **Next** when the Remote Installation Status screen reports a successful installation.

13. Click **Finish** to exit the install wizard.

Related Topics:

- "Uninstalling Storage Exec" on page 25
- "Uninstalling the Storage Exec Remote Administration Console" on page 27

Installing Storage Exec Server from the Command Line

Installing Storage Exec Server using the command line is referred to as Silent Mode Installation. This installation method uses the program, Setup.exe, which is found on the Storage Exec CD, along with a series of command switches, and the -S switch.

If you use the switches without the -S parameter, the Storage Exec silent install program prompts you for values for each of the switches you specify on the command line. Using the -S parameter forces the silent install program to accept the switch values you provide, without prompting you for them during the installation process. In the above example, had -S not been used, the Storage Exec installation program would have prompted you for the user name, domain, and password, even though you already provided the required information on the command line.

Note Silent mode installation is only supported if Storage Exec is being installed on a computer for the first time.

To perform a command line installation, you must have:

- Storage Exec installation CD.
- Administrator privileges on the computer where you want to install or configure Storage Exec.

The following switches can be used during the command line installation of Storage Exec.

Silent install command line switches

Switch	Description
/USER:<user name> **/DOM:<domain name>** **/PASS:<password>**	*Required*. Specifies an existing user, domain, and password to be used by the Storage Exec service account. Silent mode installation will not create a user profile.
/DEST:<destination folder>	Specifies a user-defined folder where Storage Exec will be installed. If you do not specify a folder, the default path and folder are used: `\Program Files\VERITAS\Storage Exec`.
/DBDEST:<destination path>	Specifies the path where the Storage Exec Database will be installed. If you do not specify a path, the default path will be used: `\Program Files\VERITAS\Storage Exec\DB`
/DOM:<domain>	Specifies the name of the domain in which the Storage Exec service account resides.

Silent install command line switches (continued)

Switch	Description
/NODOCS:	Excludes the Storage Exec documentation from being installed.
/NOREBOOT:	Specifies that the computer will not be restarted after the silent installation finishes. The default is to restart the computer.
/NORESTORE:	Specifies that previous Storage Exec data found on the system will be ignored during the installation of Storage Exec. Running the silent install operation without this switch will add the previous Storage Exec data to the new Storage Exec database.
/PASS:<password>	Specifies the Storage Exec service account password. The parameter /PASS must be used if you use the /DOM parameter.
/PROFILE:	The Microsoft Exchange profile to be used when the address book is required.
/PROFILEPASS:	The Microsoft Exchange profile password, if required.
/S	Forces the silent install program to accept the switch values you provide on the command line, without prompting you for them during the installation process.
/SMTP:	The name of the SMTP server that sends the email alerts and reports.
/SMTPSENDER:	The sender's logon ID or email address.
/SMTPPASS:	Email account password.
/SNO:<serial number>	Specifies one or more serial numbers to use for installing Storage Exec and other additional options. Use the following examples as a guide when using this switch: Example 1: `c:\setup /SNO:<s/n>` Example 2: `c:\setup /SNO:<s/n 1> <s/n2> <s/n 3>` Example 3: `c:\setup /SNO:<s/n1> /SNO:<s/n2> /SNO:<s/n3>` If you do not enter a serial number using the /SNO: switch, an evaluation version of Storage Exec will be installed.
/USER:	Specifies the user name for the Storage Exec services account.

Silent install command line switches (continued)

Switch	Description
/UNINSTALL:	Specifies the removal of only the Storage Exec program files. All accumulated Storage Exec data files remain.
/REMOVEALL:	Specifies a complete uninstallation of Storage Exec. All Storage Exec folders, program files and data files are removed.

▼ To install Storage Exec Server using the command line:

1. Move to a Windows computer where you want to install Storage Exec.
2. Place the Storage Exec CD in a CD-ROM drive.

   Note If the Windows Autorun feature launches the Storage Exec Browser, select a language and then click **Exit** when the main installation screen appears.

3. Open a Windows Command Prompt.
4. Change to the drive containing the Storage Exec CD.
5. Change directories to `\WINNT\INSTALL`.
6. Type setup along with the following required switches. For example:

   ```
   c:\>setup /USER:<user> /DOM:<domain> /PASS:<password> -S
   ```

7. Press **ENTER**.

   An installation job log named scinst.log is created in the Windows directory on the computer where Storage Exec is installed. This file lists any errors that may have occurred during installation process, and is the only source of feedback when running setup.exe.

Related Topics:

- "Uninstalling Storage Exec from the Command Line" on page 26

Repairing Storage Exec

If you have missing or corrupted Storage Exec files or registry keys on the local Windows computer, run the **Repair** option. The program stops all Storage Exec services, reinstalls corrupted files and registry keys, and then restarts the services. The Storage Exec databases are not reinstalled.

Any changes made to Storage Exec program files and registry keys will be reset to the original settings.

▼ To run the Storage Exec Repair option:

1. Close the Storage Exec application.
2. Click **Start**, point to **Settings**, click **Control Panel**, and then double-click **Add or Remove Programs**.
3. At the Add or Remove Programs dialog box, select **VERITAS Storage Exec**, and then click **Change.**
4. On the Welcome screen, click **Next.**
5. On the Program Maintenance screen, select **Local Install and Repair**, and then click **Next.**

   Note Make sure the option **Remote Agent Install** is not selected.

6. Select **Install**.
7. Select **Finish**.

Related Topics:

- "Storage Exec Installation Overview" on page 14
- "Uninstalling Storage Exec" on page 25

Uninstalling Storage Exec

This section provides the information necessary for uninstalling Storage Exec from a local computer using either **Windows Add/Remove Programs**, or from a command line using a Windows command prompt and the Storage Exec command line program, Setup.exe.

Related Topics:

- "Uninstalling Storage Exec using Windows Add/Remove Programs" on page 25
- "Uninstalling Storage Exec from the Command Line" on page 26
- "Uninstalling the Storage Exec Remote Administration Console" on page 27

Uninstalling Storage Exec using Windows Add/Remove Programs

Use the following steps to uninstall Storage Exec using Windows **Add/Remove Programs**.

▼ To uninstall the Storage Exec application using Add/Remove Programs:

1. Move to a computer where Storage Exec is installed.
2. Close the Storage Exec application.
3. Click **Start, point to Settings, click Control Panel, and then double-click Add/Remove Programs.**
4. At the Add/Remove Programs dialog box, select **VERITAS Storage Exec**, and then click **Remove.**
5. When prompted to confirm the deletion of Storage Exec from your computer, click **Yes.**
6. When prompted to remove Storage Exec program files or all data, click **Yes**; click **No** to retain user-created data such as managed resources, file groups, report sets and report definitions, preferred computers, audit and trend databases, reports and quarantine directories, and the Network Appliance Filer registry.
7. When the uninstall is completed, click **Finish.**
8. If the uninstall program fails, click the **View Installation Log File button**.
9. Restart the computer after uninstalling Storage Exec.

Related Topics:

- "Installing Storage Exec Server" on page 16

Uninstalling Storage Exec from the Command Line

Storage Exec can be uninstalled from the command line using the Storage Exec install/uninstall program, Setup.exe.

To perform a command line uninstall, you must have:

- Storage Exec installation CD.
- Administrator privileges on the computer where you want to uninstall Storage Exec.

▼ To uninstall Storage Exec using the command line:

1. Move to a Windows computer where you want to uninstall Storage Exec.
2. Place the Storage Exec CD in a CD-ROM drive.

   Note If the Windows Autorun feature launches the Storage Exec Browser, select a language and then click **Exit** when the main installation screen appears.

3. Open a Windows Command Prompt.
4. Change to the drive containing the Storage Exec CD.
5. Change directories to `\WINNT\INSTALL`.
6. Type `setup` along with either of the following switches:

   ```
   c:\>setup /UNINSTALL
   ```

   or

   ```
   c:\>setup /REMOVEALL
   ```

The following switches can be used during the command line uninstall of Storage Exec.

Silent install command line switches

Switch	Description
/UNINSTALL	Specifies the removal of only the Storage Exec program files. All accumulated Storage Exec data remains.
/REMOVEALL	Specifies a complete uninstallation of Storage Exec. All Storage Exec folders, program files and data files are removed.

7. Press **ENTER**.

   An uninstall job log named scuninst.log is created in the Windows directory on the computer where Storage Exec is being uninstalled. This file lists any errors that may have occurred during uninstall process, and is the only source of feedback when running setup.exe.

Related Topics:

- "Uninstalling Storage Exec using Windows Add/Remove Programs" on page 25

Uninstalling the Storage Exec Remote Administration Console

Use the following steps to uninstall the Storage Exec Remote Administration Console from remote computers.

▼ **To uninstall the Storage Exec Remote Administration Console:**

1. Move to a computer running the Storage Exec Remote Administration Console.
2. If it is running, close the Storage Exec Remote Administration Console.
3. Click **Start**, point to **Settings**, click **Control Panel**, and then double-click **Add/Remove Programs**.
4. Select **VERITAS Storage Exec Remote Agent**, and then click **Remove.**
5. When prompted to confirm the deletion of the Storage Exec Remote Administration Console from your computer, click **Yes.**

6. After the uninstall operation finishes, close Add/Remove Programs.

   The Storage Exec Remote Administration Console uninstallation is now complete.

Upgrading from Previous Versions of Storage Exec and Storage Manager

This version of Storage Exec replaces Storage Exec versions 4.x and 5.x, formerly known as StorageCentral. It also replaces Storage Manager 2.0 for Server Appliances and Storage Manager 1.01 for Server Appliances.

During the upgrade process, each of the previous products will be uninstalled and replaced with Storage Exec. In addition, each of the previous products' data will be maintained and then migrated into the new Storage Exec database.

▼ **To upgrade from previous versions of Storage Exec or Storage Manager:**

1. At the computer running either Storage Exec or Storage Manager, place the Storage Exec CD in the CD -ROM drive.

   Note If the Storage Exec Browser does not automatically start, start the Windows Explorer and navigate to the CD drive containing the Storage Exec CD media. Double-click **Browser.exe** to start the Storage Exec browser.

2. Select a language and then click **OK**.

3. Click **Install Storage Exec**.

4. Clear the check box for **Remote Agent Install**, if it is selected.

5. Click **Next** to continue with the installation.

6. Select **I accept the terms of the license agreement**, and then click **Next**.

7. On the VERITAS Storage Exec Install Menu screen, click **Local Install**.

   A message appears informing you that a previous version of StorageCentral or Storage Manager has been detected, along with the product's corresponding data. Click the check box preceding this message if it is not selected.

8. Click **Next**.

9. Type the serial numbers for Storage Exec and any options. You can also import an existing scsernum.xml file to enter the serial numbers.

- To manually enter the serial numbers for Storage Exec Server and any additional options, type the serial numbers into the field, and then click **Add**. When finished, click **Next**.
- To import the serial numbers from a file, click **Import**, and then browse the Windows directory. Select an existing scsernum.xml file and then click **Next**.

Note After clicking **Next**, the serial numbers you entered are saved to a file named scsernum.xml, which is located in the Windows directory.

To install an evaluation version, a serial number is not required. Selecting the Storage Exec options you want to evaluate and then clicking **Next** without entering a serial number displays a message informing you that an evaluation copy of Storage Exec Server will be installed.

10. Review the local options to be installed.

    Options that will not be installed have a red "X" displayed in the option icon. To enable any of these options, click the icon to clear the X, and then follow the prompts to install it. If the option icon is gray, the option is not available.

11. To accept the local options for installation, and to accept the default destination folders for both the Storage Exec program files and the Storage Exec databases, click **Next**.

Note To select a different destination folder for either the Storage Exec program files or the Storage Exec databases, click **Change**, and follow the prompts.

If you are reinstalling Storage Exec or upgrading from previous versions of StorageCentral, the Change buttons do not appear, as the original installation folders are used.

12. Provide a user name, password and domain name for the Storage Exec system services to use and then click **Next**. For more information, see "The Storage Exec Service Account" on page 14.

13. Review the Storage Exec Installation Summary screen and then click **Next**.

Note In the Installation Summary page, a link to a Storage Exec warning message appears. The warning message informs you that a previous version of StorageCentral or Storage Manager has been found and will be uninstalled.

The Storage Exec upgrade begins. During the upgrade process, several prompts may appear. Answer each prompt with an appropriate response and continue with the upgrade.

14. When the upgrade finishes, restart the computer.

Related Topics:

- "What's New in Storage Exec" on page 3

Storage Exec Database Configuration

If you have multiple installations of Storage Exec running on your network, you can configure an existing Microsoft SQL Server database to be used as a centralized Storage Exec database.

Centralizing a Storage Exec database means that all computers with Storage Exec installed on them access the same database.

Related Topics:

- "Configuring Microsoft SQL Server as the Centralized Storage Exec Database" on page 30

Configuring Microsoft SQL Server as the Centralized Storage Exec Database

This section presents the steps you must follow to configure Storage Exec to use Microsoft SQL Server as its repository for audit and trending data. You might want to use SQL Server as the repository if you are using Storage Exec in a clustered environment. Storing the audit and trend data in a shared environment ensures they are updated in the event of a failover.

You can store Storage Exec data in one of two formats in SQL Server—ANSI or Unicode. Storage Exec 5.0 can store only ANSI data in SQL Server, but Storage Exec 5.3 can store either ANSI or Unicode data in SQL Server. Storing your data in ANSI format takes up less room and is backward compatible to Storage Exec 5.0, but means you cannot use foreign character sets. If you want to take advantage of Unicode support and store your data in SQL Server, you must use Storage Exec 5.3 and configure it to use the Unicode version of SQL Server. The instructions that follow enable you to choose the ANSI or Unicode version of SQL Server.

▼ To configure SQL Server support:

1. If Storage Exec is installed on the same computer as SQL Server, go to step 2.

If Storage Exec is not installed on the same computer as SQL Server, copy the following files to one directory on the SQL Server computer.

- `SCSQL.bat`
- `SCSRMDB.sql` (if you are going to install the ANSI version of SQL Server) or `SCSRMDBU.sql` (if you are going to install the Unicode version)

These files are located in the *`install-directory`*`\DB` directory of the computer on where Storage Exec is installed.

Note Running the batch file in the next step will drop the existing SQL Server SCSRMDB database.

2. Run the SCSQL.bat batch file by typing the following:

   SCSQL /switch username password

   where

   - *switch* has a value of "a" if you are using the ANSI version of SQL Server; it has a value of "u" if you are using the Unicode version of SQL Server
   - *username* is an account that can create databases, tables, and indexes
   - *password* is the password for this account

   `SCSQL.bat` calls the `ISQL.exe` command, which in turn creates the SCSRMDB database and its tables.

3. Set user permissions to the SCSRMDB database.

4. Provide the SQL Server user name and password by following these instructions:

   a. On the Storage Exec management pane, right-click **My Computer**, **Preferred Computers and Groups**, or **Organizational Unit**, and then click **Properties**. The Properties dialog box appears.

   b. Click the **SQL Server** tab.

   c. Enter the user name and password.

   d. Click **OK**.

5. Remove or rename the previous ODBC DSN for SCAuditDB and SCTrendDB on each computer on which Storage Exec is installed.

6. Configure the ODBC DSN for SCAuditDB and SCTrendDB on each computer using the SCSRMDB database in SQL Server.

7. Provide the SQL Server user name and password by following these instructions:

a. On the Storage Exec management pane, right-click **My Computer**, **Preferred Computers and Groups**, or **Organizational Unit**, and then click **Properties**. The Properties dialog box displays.

b. Click the **SQL Server** tab.

c. Enter the user name and password.

d. Click **OK**.

8. Close the Administration Console user interface and restart these services:

- QuotaAdvisor Server
- FileScreen Server

Note The user name and password you specify in step 4 must be the same as that in the ODBC connection, and this account must have the permission to access the SCSRMDB database in SQL Server.

Note The ODBC DSN should use the access method specified in database properties to access the SCSRMDB database.

Getting Started 3

This chapter includes the following topics to help you start using Storage Exec after you have installed it:

Getting Started with Storage Exec

After you install Storage Exec, you can assess your current storage resource management situation and configure Storage Exec to help you manage it.

What do you want to do?

To	Do this
Find out how your storage is being used	• Identify duplicate files and media files, such as .mp3 files, by running the Duplicate Files report and the Media Files report. • Examine directory usage by running the Space by Folder Resource Summary report. • Determine how much space each user currently owns by running the Space by User Summary report. For instructions on how to run reports, see "Introduction to Reports" on page 121.
Block files	Apply file blocking policies to resources, such as folders or directories, to restrict the types of files that users can save. You can apply one of the default Storage Exec file blocking policies, or create a custom policy. For information about file blocking policies, see "Introduction to File Blocking" on page 83.

To	Do this
Set disk quota limits	Apply space allocation policies to resources, such as folders or directories, to restrict the amount of data users can save on those resources. A policy can specify that a particular folder cannot exceed a specific size or that a specific user can store no more than a certain amount on a resource. You can apply one of the default Storage Exec space allocation policies or create a custom policy. For more information about space allocation policies, see "Introduction to Space Allocation" on page 63.
Customize Storage Exec to meet the needs of your environment	Configure global properties on a computer that contains the resources you want to manage. For more information, see "Configuring Properties for a Computer" on page 34.

Configuring Properties for a Computer

You can configure global properties for an individual computer (or Organizational Unit when using the Storage Exec Enterprise Administration Option).

By configuring global properties, you can customize Storage Exec to meet the needs of your environment.

There are several Properties tabs. Different tabs display depending on which Storage Exec options are installed on the computer.

▼ To set global properties:

1. On the management pane, right-click **My Computer**, an Organizational Unit, domain, or a preferred computer. Then choose **Properties**.

2. Select the tab for the property you want to modify.
   - "Setting Audit Trail Properties" on page 35
   - "Setting Event Log Properties" on page 36
   - "Setting File Blocking Properties" on page 37
   - "Setting Mail Properties" on page 38
   - "Setting Network Appliance Properties" on page 39
   - "Setting Remote Agent Properties" on page 39

- "Setting Report Properties" on page 40
- "Setting Space Allocation Properties" on page 41
- "Setting SQL Server Properties" on page 42
- "Setting Trending Properties" on page 42

3. Click **OK** to modify the properties.

Setting Audit Trail Properties

▼ **To set audit trail properties:**

1. On the management pane, right-click **My Computer**, an Organizational Unit, domain, or a preferred computer. Then choose **Properties**.

2. Select the **Audit Trail** tab.

3. In the **Period** field, enter the number of days you want Storage Exec to keep the audit data. Setting a long retention period causes Storage Exec to use more disk space for storing data.

   To keep audit data indefinitely, select the **Keep infinite data** check box

For additional information about audit data, see "Introduction to Audit Trail" on page 147.

Setting Event Log Properties

On the **Event Log** tab you can specify which events will generate a record in the Microsoft application event log.

For space allocation, Storage Exec defaults to creating a record in the application event log for each space allocation action.

For file blocking, Storage Exec does not create a record in the application event log for any file blocking action by default.

Select the appropriate options as follows:

Event Log Tab

Item	Description
Space Allocation - Send a message to event log when:	
Creating a resource	Select this option if you want Storage Exec to create a record in the application event log when a space allocation managed resource is created.
Modifying a resource's properties	Select this option if you want Storage Exec to create a record in the application event log when a space allocation managed resource is modified.
Deleting a resource	Select this option if you want Storage Exec to create a record in the application event log when a space allocation managed resource is deleted.
File Blocking - Send a message to event log when:	
Creating a resource	Select this option if you want Storage Exec to create a record in the application event log when a file blocking managed resource is created.
Modifying a resource's properties	Select this option if you want Storage Exec to create a record in the application event log when a file blocking managed resource is modified.
Deleting a resource	Select this option if you want Storage Exec to create a record in the application event log when a file blocking managed resource is deleted.

Setting File Blocking Properties

You can set the location where blocked files are placed for quarantine. You can also exclude specific users or groups from file blocking.

File Blocking Tab Fields

Item	Description
Quarantine file location	Enter the location to store blocked files. This option applies only to file content blocking. If the quarantine option is not selected and/or the file location is not provided, the blocked file will be deleted. **Note** Files that are blocked due to content checking will be quarantined only if the policy through which they are blocked is set up to quarantine files.
Excluded users and groups	Enter the users and/or groups you want to allow to save all types of files. These users or groups will be excluded from all file blocking policies. Click **Add** to select users and groups to exclude. To search for users, click **Find User**, type the name or partial name, and then click **Find Now**. When the name of the user you want to exclude displays in the **Search results** field, select the name and then click **Select** The exclusion is implemented on a server-wide basis. For example, if a resource is blocked for graphics files, but you do not want to block them for the “Domain Admins" group, add the "Domain Admins" group to the excluded users and groups list. You can exclude by user and by group on non-Network Appliance computers; you can exclude only by user on Network Appliance computers.

Setting Mail Properties

Storage Exec can use email to notify you when an alarm is activated and to send you reports.

On the **Mail** tab you can specify the parameters that enable Storage Exec to use email: Exchange mail settings, SMTP mail settings, or whether to use Active Directory for email.

You must specify a mail server and mail sender if you want to perform the following actions:

- Email alarm notifications.
- Email reports from alarm actions.
- Email interactive reports after they run.
- Email scheduled reports after they run.

Mail Tab Exchange Mail Settings

Item	Description
Exchange mail settings	
Profile	Enter the Microsoft Exchange profile to be used when the address book is required.
Password	Enter the Exchange password (if required).
SMTP mail settings	
Mail server	Enter the SMTP server from which email alerts and reports are sent.
Mail Sender	Enter the email address that you want to appear in the “From” field in the email. You may need to provide the sender's login ID (for example, DJones) or the sender's email address (for example, DJones@company.com).
Password	Enter the email password
Use Active Directory for email	Select this if you want Storage Exec to retrieve the email address from Active Directory. This helps send notification messages through alarm actions. If you do not want Storage Exec to retrieve the email address using Active Directory, clear the check box.
Test	Select this to test an email address to verify that it is valid and that the intended recipient can receive the email.

Setting Network Appliance Properties

On this tab you can add and delete Network Appliance Filers from the list of known Filers.

To add a Filer, do the following:

1. Click **Add**. The Select Computer dialog box displays.
2. Identify a Network Appliance Filer by doing one of the following:
   - Type its fully qualified path name in the box.
   - Click the browse (**...**) button, find the Filer using the **Browse for Computer** dialog box, and click **OK**.
3. Click **OK** on the **Select Computer** dialog box.

To delete a Filer from the list, highlight a Filer in the list and click **Remove**.

Setting Remote Agent Properties

This tab contains parameters related to the remote agent.

Remote Agent Tab Fields

Item	Description
User name	Enter the user name you use to access the Network Appliance remote agent.
Password and **Confirm Password**	Enter the password associated with the user name.

Setting Report Properties

This tab contains parameters related to generating reports.

Report Tab Fields

Item	Description
Exclude OS files	Select this option to exclude operating system files from reports.
Exclude DLL files	Select this option to exclude all .dll files from reports.
Exclude Administrators	Select this option to exclude all Administrator files from reports.
Include user shares	Select this option to include User shares in reports.
Include default shares	Select this option to include default shares in reports.
Report output folder	Enter the default folder where reports and batch files will be saved. If no value is specified, reports and batch files are stored in the Storage Exec `\Reports` folder.
Enter an address (URL) to download Active HTML report components from	Enter an URL for downloading the Active Reports component that is used in Active HTML reports. For information about customizing the Active Reports component, read the section "Running the Storage Exec Cab File Installation Program on Remote Computers" on page 147.
Charge back	
Cost per GB	This field displays only if the Storage Exec Enterprise Administration Option is installed. Enter the value you want Storage Exec to use in the Chargeback Summary report to compute a chargeback for the disk storage that users use. The default value is $80 per gigabyte. For more information about this report, see "Chargeback Summary Report" on page 172.
Account code	This field displays only if the Storage Exec Enterprise Administration Option is installed. Enter the Active Directory field that the Chargeback Summary report should use when assigning chargeback charges based on the amount of disk storage that users use. For more information about this report, see "Chargeback Summary Report" on page 172.

Setting Space Allocation Properties

This tab contains parameters related to space allocation.

Space Allocation Tab Fields

Item	Description
Device settings	
Auto detect disks	Select this option to enable Storage Exec to automatically detect mounted drives and apply a storage management policy to ensure data protection.
Use policy	Select the managed resource policy to use for auto detection of disks.
Allow active limits on devices	Select this option to allow users to set an active space limit on partitions (non-system disks). This check box is not selected by default. Use this option with caution because an active limit on devices will enforce a device space limit.
Minimum space limit	
Minimum limit (MB)	Type the smallest disk space limit (in megabytes) that can be assigned to a managed resource. This minimum limit applies when new managed resources are created and when a space allocation policy is applied to an existing managed resource. For example, you set this limit to 1MB and then you create a space allocation policy with a disk space limit of 500 KB. If you use the policy to create a managed resource, the resulting managed resource will have a space allocation limit of 1MB, not 500KB. In another example, you set this limit to 1MB. Then you create a space allocation policy with a disk space limit of "100% of current used," and then apply the policy to a managed resource containing 250KB of data. The resulting managed resource will have a space allocation limit of 1MB, not 250KB.

Setting SQL Server Properties

If you want to store Storage Exec audit and trend data in Microsoft SQL Server (rather than in the default Microsoft Access database), you will provide the values below as you follow the instructions in the section "Configuring Microsoft SQL Server as the Centralized Storage Exec Database" on page 30.

SQL Server Tab's Fields

Item	Description
User	Enter the SQL Server user name.
Password	Enter the password associated with the user name.

Setting Trending Properties

Storage Exec supports managed resource trending. Managed resource trending collects historical data about your managed resources and stores it in a database. You can then run trend reports on any managed resources, including disks, directories, and users.

Trend data (along with audit data) can be stored in one of two places: A Microsoft Access database (the default) or Microsoft SQL Server.

- During installation, an ODBC data source called "SCTrendDB" is added. This data source points to the `SCTrend.mdb` Microsoft Access database; the default installation directory for this database is `\VERITAS\Storage Exec\DB`. Data is collected for all managed resources at the interval specified in the server or Active Directory properties.
- To override the default and store the data in Microsoft SQL Server, follow the instructions in the section "Configuring Microsoft SQL Server as the Centralized Storage Exec Database" on page 30.
- To see the records for all computers in the domain that the Administration Console is connected to, use a centralized database.

Regardless of where the trend data is stored, you must configure Storage Exec to collect the data.

After trend data has been collected, it can be reported on using the Space Allocation Trend Summary report. You can also create your own trend reports with plotted graphs and a variety of output by modifying the Space Allocation Trend Summary report query in your reports.

To configure Storage Exec to collect trend data:.

Trending Tab Fields

Item	Description
Enable collection	Select this option to enable space allocation collection. At trend intervals, managed resource information will be saved to a database. You may run trend reports to view the trend information from the database.
Start time	Enter the time when data should start to be collected.
Collection interval	Enter the time interval between space allocation collections.
Period	Enter the amount of time you want Storage Exec to keep the trend data. Setting a long retention period causes Storage Exec to use more disk space for storing data.
Keep infinite data	Select this option if you want Storage Exec to keep trend data indefinitely.

Viewing Version Information

▼ To view product version information or technical support information:

1. On the management pane, right-click **My Computer**, an Organizational Unit, domain, or a preferred computer. Then choose **Properties**.

2. Select the **Version** tab.

Managed Resources 4

This chapter contains the following sections:

Introduction to Managed Resources

Managed resources are files, directories, shares, or partitions on which you want to block files or set disk space quotas. You manage those resources by applying space allocation or file blocking policies to them. When using the Storage Exec Enterprise Administration Option, resources may be managed for an Organizational Unit, Site, or Domain.

When you choose managed resources from the management pane, a list of the managed resources displays in the details pane. You may do the following:

- Create and delete managed resources
- View and modify the properties of a managed resource
- Set the frequency with which Storage Exec automatically refreshes the contents of the details pane
- Control the appearance of the details pane
- Specify the contents of the details pane
- Run a report against a managed resource
- Apply a policy to a managed resource to block files from the resource or to set disk space quotas on that resource
- On Network Appliance Filers: Turn quotas on and off, resize quotas, and restart quotas

Related Topics:

- "Deleting a Managed Resource" on page 53
- "Viewing and Modifying Managed Resource Properties" on page 53
- "Applying a Policy to a Managed Resource" on page 61

Creating a New Managed Resource

This section assists you in using the New Managed Resource Wizard, which enables you to create a managed resource.

1. On the management pane, right-click **Managed Resources**, point to **New**, and then click **Managed Resources**.

   or

   In the managed resource details pane, right-click and click **New**.

2. On the **Welcome** screen, click **Next**.

3. The **Select a Computer** dialog box displays under certain circumstances. For example, you see this dialog box if:

   - You are running the Storage Exec Enterprise Administration Option and you are working at the root level.
   - You are creating a managed resource on a computer that is part of a preferred group.

   If the **Select a Computer** dialog box displays, specify the computer on which you want the managed resource, and then click **Next**.

4. On the **Resources** dialog box, select the files, directories, or partitions you want to manage, and then click **Next**.

   Note If you are working with a Network Appliance Filer and have recently added a share that does not display in the list of folders, you must exit the wizard, refresh the Administration Console, and restart the wizard.

5. On the **Folder Policy Selection** dialog box, complete the fields that display as follows, and then click **Next**:

Folder Policy Selection options

Item	Description
Folder policy	
Apply policy to resource	Select this check box if you want to apply a policy to the resource you are creating. Then select the policy from the **Use policy** field.
Use policy	If you selected the **Apply policy to resource** check box, select the policy you want to apply to this resource.
Subfolder policy	
Auto detect subfolders and apply policies as they are created within a managed resource	Select this check box to apply the Auto detect subfolders space allocation limit on any subfolders of this resource. The space allocation limit will also be applied to any subfolders that are created in the future. Note that the policy will be applied only to subfolders that are one level below the resource.
Use policy	If you selected the **Auto detect subfolders and apply policies as they are created within a managed resource** check box, select the policy you want to apply to this resource.

6. On the **User Policies and Options** dialog box, specify the users to which the restrictions on this managed resource apply. Complete the fields that display as follows, and then click **Next**.

User Policies and Options

Item	Description
Auto detect all users within the resource	Select this check box to apply the Auto detect all users space allocation limit on the resource. Any user who owns a file in the resource will automatically be assigned a space limit. This space limit will also be applied to the owner of any new files.
Exclude administrators	If you selected the **Auto detect all users within the resource** check box, you can select this check box to exempt administrators from the restrictions on this resource.
Check for user or group associations	Select this check box to apply policies associated with each user's primary group. Select a policy from the **Use policy** field.

User Policies and Options

Item	Description
Use policy	Select the policy that you want to apply to this resource.
Apply policy to specific users within the resource	Select this check box to apply a policy to certain users. You select the specific users after you click **Next**.
Use policy	Select the policy that you want to apply to certain users of this resource.

7. If you selected the **Apply policy to specific users within the resource** check box in step 6, the **Users and Groups** dialog box displays. Use one of the following to select the users to which you want to apply the policy, and then click **Next**:

Users and Groups options

Item	Description
Add new	Click this button if you know the user's domain and user name. After you select **Add new**, type the user's name, and then click **OK**.
Select users	Click this button if you want to select a name from a list of users. After you select a user or users, click **OK**.
Find user	Click this button if you want to search for a user. When the **Find User** dialog box displays, type the full or partial name of the user, and then click **Find Now**. Select the user from the list, and then click **Select**.
Remove	To remove a user from the policy, select the user and then click **Remove**.

8. Click **Finish**.

Related Topics:

- "Introduction to Space Allocation" on page 63.
- "Introduction to Using Storage Exec with Network Appliance Filers" on page 173.

Refreshing the Managed Resource Details Pane

The managed resource details pane may be refreshed automatically at an interval you specify, or manually whenever you want. Manually refreshing the display does not re-create the resource, it just recalculates the current space limit.

▼ **To refresh the managed resource details pane:**

1. On the management pane, select **Managed Resources**.
2. To refresh all managed resources, click the refresh button ().
3. To set the frequency with which Storage Exec automatically refreshes the managed resource details pane, on the details pane, right-click and select **Auto Refresh Frequency**.
4. On the **Auto Refresh Frequency** dialog box, use the up and down arrows to adjust the time values in minutes and seconds. The default value is 15 minutes. Click **OK** to save your changes.

Viewing Managed Resource Details

For each managed resource, the following columns display in the details pane. To sort the display, click the column heading

If one or more columns do not display in the details pane, follow the instructions in "Selecting Columns to Display in the Managed Resource Details Pane" on page 50

Managed Resource Details Pane

Item	Description
Server	Name of the server where a managed resource is located.
Managed Resource	Managed resource name (folder name). The column header changes to "Managed Resource (Filtered)" if you apply a filter to the details pane as described in the section "Filtering the Contents of the Managed Resource Details Pane" on page 51. If a Network Appliance Filer is not online, a row displays with a managed resource of "volume-name — status".

Managed Resource Details Pane (continued)

Item	Description
% Used	Percentage of the space limit used: ◆ Red: 90 – 100 ◆ Yellow: 60 – 89 ◆ Green: 0 – 59
Policy	Name of the managed resource policy that is a component of this managed resource. If this column is blank, the managed resource does not have a policy associated with it.
Space Limit	Maximum amount of space that can be used for a managed resource.
Space Used	Space actually used by a managed resource.
User	Owner of the managed resource.
Mode	Indicates whether space allocation or file blocking is enforced. Values are Active and Passive.
Type	Type of managed resource. The types are: ◆ Folder limit ◆ User limit ◆ Blocking ◆ Auto detect users ◆ Auto detect folder
HighWater	The largest amount of disk space the managed resource ever used, even if files were deleted.

Selecting Columns to Display in the Managed Resource Details Pane

▼ **To select columns to display in the managed resource details pane:**

1. On the management pane, click **Managed Resources**.
2. Right-click anywhere in the details pane, and select **Choose Columns**.
3. Select columns to display from the list. Clear the check boxes for the columns you do not want to display.

4. Use the **Move Up** and **Move Down** buttons to reorder the columns. The first column in the list will be the left-most column in the managed resource details pane.

5. Click **OK** to accept the selected columns and order.

Note Use the **Restore** button to revert back to the original details pane layout with the original columns and column order selected.

Filtering the Contents of the Managed Resource Details Pane

▼ **To filter the contents of the details pane so that only those managed resources that meet specific criteria will display:**

1. On the details pane, right-click in the blank area and click **Filter Resources**.

2. Complete the appropriate options as follows:.

Filter Resource options

Item	Description
Resource type	Select the check box for the types of managed resources you want to display on the details pane. Clear the check boxes for the types of managed resources you do not want to display on the details pane.
Allocation fields	Select the type of allocation field to filter on. Your choices are: ◆ High water ◆ Space limit ◆ Space used ◆ Percent used ◆ Select all
Filter values	Select either **Between** or **Greater** from the **Filter values** drop-down list, and then enter the range of values you want to use to filter allocation fields. For example, if you want the details pane to display only those managed resources that are using more than 100 MB, select **Space used** in the **Allocation fields** option, select **Greater than** as the filter value, and then type 100 MB in the value fields.

3. To filter the details pane to include resources with a certain policy name, user name, server name, or mode, click **Advanced**. Then select the policy, user, server, or mode on which you want to filter.

4. Click **OK** to apply the filter.

Note Click **Restore** to revert to the original filter options.

Viewing the Contents of a Managed Resource

▼ **To view the contents of a managed resource:**

1. On the management pane, select **Managed Resources**.

2. On the details pane, right-click a managed resource, and click **Explorer**.

   The Windows Explorer window displays. The selected managed resource is highlighted on the left pane. The contents of the selected folder can be viewed on the right pane.

Running a Report Against a Managed Resource

▼ **To run a report against a managed resource:**

1. On the management pane, select **Managed Resources**.

2. Right-click the managed resource for which you want to run a report, and then select **Run Report**.

3. Select **Run interactively** to run the report now, or select **Schedule report** to set a time to run the report.

4. Click the ellipses (...) next to the **Report** field to select the report you want to run.

5. Click **Submit**.

Related Topics:

- "Running a Report" on page 129

Deleting a Managed Resource

▼ **To delete a managed resource:**

1. On the management pane, select **Managed Resources**.
2. On the details pane, right-click one or more managed resources to delete, and then click **Delete**.
3. A message displays prompting for confirmation. Click **Yes** to delete the managed resources.

Related Topics:

- "Introduction to Managed Resources" on page 45

Viewing and Modifying Managed Resource Properties

This section assists you in viewing and modifying the properties of a managed resource.

Note If a policy is associated with a managed resource, modifying the managed resource properties will break the association. Changes to the policy will no longer be propagated to the managed resource. After you change the properties of a managed resource, you should reapply the policy to the resource. For instructions on how to apply a policy to a managed resource, see "Applying a Policy to a Managed Resource" on page 61.

Note If you are a non-administrative user, you can modify the properties only if you have "Full Control" permission. For more information, read the section "Standard Storage Exec Security" on page 230.

To view or modify a managed resource's properties, go to the managed resource details pane, right-click a managed resource in the details pane, and click **Properties**. Different properties display depending on the type of managed resource you selected.

1. On the management pane, right-click **Managed Resources**.
2. On the details pane, right-click the managed resource, and then click **Properties**.

The table below identifies the types of managed resources that you may select from the details pane.

Managed Resource Icons

This icon in the details pane...	...represents this type of managed resource:
	Folder limit (see section "Changing Properties for a Folder Limit or User Limit Managed Resource Type" on page 54)
	User limit (see section "Changing Properties for a Folder Limit or User Limit Managed Resource Type" on page 54)
	Auto detect folders (see section "Changing Properties for an Auto Detect Folders Managed Resource Type" on page 58)
	Auto detect users (see section "Changing Properties for an Auto Detect Users Managed Resource Type" on page 59)
	File blocking (see section "Changing Properties for File Blocking Managed Resource Types" on page 59)

Related Topics:

- "Introduction to Managed Resources" on page 45
- "Introduction to Space Allocation" on page 63

Changing Properties for a Folder Limit or User Limit Managed Resource Type

▼ **To change properties for a folder limit or user limit managed resource type:**

1. On the management pane, select **Managed Resources**.

   Note Changing properties will disassociate the managed resource from the policy.

2. Right-click the managed resource you want to change, and then click **Properties**.

3. On the **Space Limits and Options** tab, complete the appropriate options as follows:

Space Limits and Options

Item	Description
Limits	
Disk space limit	Type the maximum amount of space the managed resource can use. The disk space limit determines the maximum amount of space the managed resource can use. On a Network Appliance Filer, the disk space limit must be 1 KB or larger. For additional information, read the section "Limitations of Space Allocation on Network Appliance Filers" on page 179.
Overdraft	Type the overdraft limit. The overdraft limit is the amount of space by which the disk space limit can be exceeded before Storage Exec enforces the disk space limit. The overdraft limit does not apply if the managed resource resides on a Network Appliance Filer.
Options	
Passive limit	Select this option if you do not want to enforce the disk space limit. If you select this, I/O operations will never be stopped. However, the alarms will still be activated after the space limit is reached. The **Passive limit** check box defaults to different values under different circumstances. The check box is selected by default if you create a space allocation managed resource on a drive or partition *and* you do not select the **Allow active limit on devices** check box (located on the **Space Allocation** tab of the global Properties dialog box). The check box is selected by default if you create a space allocation managed resource on a system drive or system partition *and* you select the **Allow active limit on devices** check box. VERITAS recommends that any disk space limit set on the system or boot partition be passive. If a disk space limit is set on the system or boot partition and is not passive, there may be trouble booting because system startup performs I/O to the system partition.

Space Limits and Options

Item	Description
Always save open files	Select this option to allow a single I/O that exceeds the space limit to complete, but prevent the next I/O from completing (if the **Passive limit** option is not selected). Example: A user has a 50 MB space limit and is currently at 49 MB. The user opens a file, adds 5 MB of content to that file, and then tries to save the file. Because the space limit for that user is now exceeded, the file will not be saved unless the **Always save open files** option is selected. This option cannot be used with a policy for a Network Appliance Filer.
Reset high-water mark	Select this option to reset the high-water mark. The high-water mark is the largest amount of disk space limit that was ever used on a particular managed resource, even if files were deleted. This option cannot be used with a policy for a Network Appliance Filer.
Send disk full error code	Select this option to send the "disk full" error code instead of the "not enough quota is available" error code. Windows 95 clients do not interpret the "not enough quota is available" error code, but they do interpret the "disk full" error code. This option cannot be used with a policy for a Network Appliance Filer.
Exclude from folder limit	Select this option to exclude a user (or a group) from the space limit calculation. Any files owned by the user will be excluded from the space limit. In addition, the space limit will not be in effect for that user. This option is only available for user space limits. Example: A `\Public` folder may be limited to 500 MB. However, the Administrators Group should not be prevented from saving files in this folder, and the files owned by Administrators should not be counted against the space allocation on `\Public`. In this case, apply a space allocation to a group, because when a member of the Administrators Group saves a file, the file is owned by the Administrators Group security identifier, not by this individual user. This option cannot be used with a policy for a Network Appliance Filer.

4. On the **Alarm Threshold Settings** dialog box, specify the percentage of disk space that can be used before Storage Exec issues an alarm. For each alarm that you want to set, complete the fields that display as follows:

Threshold Tab Fields

Item	Description
Threshold	Enter the percentage of the disk space limit that needs to be exceeded before the alarm actions will occur. Valid values for the alarm threshold can be larger than 100%, because space limit can be passive or active. This percentage is based on the disk space limit alone and does not consider the overdraft limit. Thresholds do not enforce space limits, they are simply a means of warning users and/or taking some actions. Thresholds are exceeded in reverse order so that, of the five thresholds, the fifth threshold is exceeded first. This way the fifth threshold is the least critical and the first threshold is the most critical. Generally, the first threshold would have a value in the 90% – 100% range.
Activate	In the Activate list box, select **Activate Above** if you want to activate the alarm if the current disk space used exceeds the threshold value. Select **Activate Below** if you want to activate the alarm if the current disk space used falls below the threshold value. If you leave the Activate field blank, the alarm is activated when the threshold is met. For example: ◆ Alarm 1 could be configured with a threshold of 90%, the Activate list box is left blank, and a notification message of `Your disk is getting full; please delete or archive unneeded files`. ◆ Alarm 2 could be configured with a threshold of 90%, **Activate below value** is selected in the Activate list box, and a notification message of `Thank you for freeing up disk space.` The second message displays when the percent of disk space used drops below the threshold of 90%.

Threshold Tab Fields (continued)

Item	Description
Actions	Click this to set one or all of the following for each alarm: • Notification messages. Set up a message to send when an alarm is activated, and set up the users who will receive the notification. For more information, see "Setting Up Space Allocation Alarm Notification" on page 74. • Commands to execute. Specify a Windows 2000 (or later) command that Storage Exec will execute if an alarm is activated. For more information, see "Executing Commands for Space Allocation Alarms" on page 76. • Reports to print. Set up a report to run when an alarm is activated. see "Setting Reports to Run for Space Allocation Alarms" on page 77. • Extended disk space quotas. Enter the amount to extend the disk space limit when the alarm is activated. For more information, see "Extending the Disk Space Limit" on page 78

5. Click **OK**.

Changing Properties for an Auto Detect Folders Managed Resource Type

▼ **To change properties for auto detect folders managed resources:**

1. On the management pane, select **Managed Resources**.
2. On the details pane, right-click an auto detect folders managed resource, and then click **Properties**.
3. In the **Use Policy** field, select the policy for Storage Exec to use on all current subfolders of this resource and all subfolders that will be created in the future.

Changing Properties for an Auto Detect Users Managed Resource Type

▼ **To change properties for auto detect users managed resources:**

1. On the management pane, select **Managed Resources**.
2. On the details pane, right-click an auto detect users managed resource, and then click **Properties**.
3. In the **Use policy** field, select the policy for Storage Exec to use for all users who own a file in this resource. This policy will also be applied to users who create any new files on this resource.
4. Select the **Exclude administrators** check box to exempt administrators from the restriction on this managed resource.
5. Select the **Check for group associations** check box to apply policies associated with each user's primary group.

Changing Properties for File Blocking Managed Resource Types

▼ **To change properties for file blocking managed resource types:**

1. On the management pane, select **Managed Resources**.
2. On the details pane, right-click a file blocking managed resource, and then click **Properties**.
3. On the **File Groups** tab, select the file group that contains the file types you want to block. Or clear the check boxes for the file groups you do not want to block with this policy.

4. On the **File Blocking Options** tab, complete the fields that display as follows:

File Blocking Options

Item	Description
Passive	Select this check box to monitor files, but not block them. Clear this check box to block files. If you select this, Storage Exec sends notification to users when they attempt to create or copy blocked file groups.
Check file content	Select this check box to enable Storage Exec to check file content in addition to the type of file. Clear this check box to enable Storage Exec to check only file extensions. When you select the **Check file content** option for file blocking policies or managed resources, you may get the following message: `File group(s) containing the following file extensions have been selected for use with content checking file blocking. This feature relies on registered signatures that do not exist for the following file types: <a list of file types>.` As new file types appear on the market, they may not necessarily be included in Storage Exec's list of known file name extensions. To check file content of such new file types, they need to be added to Storage Exec's list and file signatures need to be created for them. If you have seen new file types in your environment and you want them to be blocked by content, contact VERITAS technical support and our staff will create file signatures for these new file types.
Actions	Click this to set the following: ◆ Notification messages. Set up a message to send when a file blocking alarm is activated, and set up the users who will receive the notification. For more information, see "Setting Up File Blocking Alarm Notification" on page 90. ◆ Commands to execute. Specify a Windows 2000 (or later) command that Storage Exec will execute if a file blocking alarm is activated. For more information, see "Executing Commands for File Blocking Alarms" on page 92. ◆ Reports to print. Set up a report to run when an alarm is activated. see "Setting Reports to Run for File Blocking Alarms" on page 93.

5. On the **Folder Filters** tab, optionally specify folders to include and exclude from the file blocking process.


Add folders to the list.


Remove folders from the list.

 and 
Move folders up and down in the list. The order of the folders does not affect the way Storage Exec processes them; ordering them is for your convenience only.

Applying a Policy to a Managed Resource

Applying a policy to a managed resource associates that policy with the managed resource. Any changes to the policy will be reflected in the managed resource.

▼ **To apply a policy to a managed resource:**

1. On the management pane, select **Managed Resources**.

2. On the details pane, right-click one or more managed resources to associate with a policy, and then choose **Apply Policy**.

3. From the **Apply Policy** dialog box, select a policy from the list, and then click **Apply** to apply that policy to the managed resource.

Space Allocation 5

This chapter contains the following topics:.

Introduction to Space Allocation

Space allocation enables you to control storage by limiting the amount of data stored in resources that Storage Exec manages. Storage Exec can enforce disk quota limits on individual users or on a file, folder, or partition.

You can set active or passive disk quota limits. Active quota limits prevent users from using more space than is allowed by the quota. Passive quota limits send informational messages when users reach their quotas, but do not prevent users from using more space.

You enforce disk quota limits by applying space allocation policies to managed resources. You can set up custom space allocation policies or use the following default policies:

- 250 MB limit with alerts. Stops users from writing to disk after reaching the disk quota limit. Sends an alert when the limit is reached.
- 250 MB limit with reports to user. Stops users from writing to disk after reaching the disk quota limit. Sends a report to the users when the limit is approached. Sends an alert when the limit is reached.
- 250 MB monitor directories. Users can continue to write to disk after reaching the disk quota limit. Sends an alert when the limit is reached.
- 250 MB passive limit with alerts. Users can continue to write to disk after reaching the disk quota limit. Sends an alert when the limit is approached. Sends a different alert when the limit is reached.
- 250 MB passive limit with reports. Users can continue to write to disk after reaching the disk quota limit. Sends an alert when the limit is reached.

- 500 MB limit in 250 MB increments. Extends a user's 500 MB disk quota limit by 250 MB, one time only.
- Baseline directory utilization. Creates a disk quota limit that is 200 percent of the disk space that the user is currently using.
- Partition alert. Users can continue to write to the device after reaching the device capacity. Sends reports to users when the limit is approached. Sends an alert when the capacity is reached.

There are two types of space allocations available: folder space allocation and user space allocation.

- A *folder space allocation* is the space limit set on a file, folder, or partition. This type of space allocation limits the size of the managed resource regardless of who writes to, or who owns files in, the managed resource.

  Example: If a 50 MB folder space allocation is set on the managed resource c:\users\JDoe, that folder and all of its contents will be limited to 50 MB regardless of who owns the files in that folder or who writes files to that folder.

- A *user space allocation* is the space limit set on a specified Security Identifier (SID) that is associated with an individual user. User space allocations can be set on a file, folder, or partition. It limits the amount of space that the user's SID can own in the object.

  Example: If a 50 MB user space allocation is set on user JDoe on the managed resource c:\Public, then JDoe will be limited to 50 MB of space in `c:\Public`. Only files that JDoe owns will be applied to the limit.

Caution Use caution when placing space allocations on the system partition. If the system does not have sufficient space to write files, the system may fail. Also, if the system partition does not have enough space to write temporary files during boot, the system may not restart. You can avoid this by using caution when placing space allocations on the system partition or system folders. If you wish to keep track of growth on the system partition, you should use the **Passive limit** option on any space allocation set on the system partition.

Users may create files and folders on the desktop. These files are stored in `C\Documents and Settings\User name`. To control disk space usage on the system partition, you may want to set modest space allocations for users on their desktop folders.

Deleting a file through Explorer does not always delete the file; instead, it renames it to the Recycle Bin folder. If the user's space allocation is on his or her own folder, this will relieve his or her space limit. However, if a user's space allocation is on the root folder of the partition, the used amount may actually increase on deletion. This is because the Recycle Bin must store additional information to allow the file to be restored. If a user's space allocation is established on the root folder, then all is well. However, if you choose to place the user's space allocation on his or her login folder, make sure you also place a

space allocation for that user on the Recycle Bin to eliminate the possibility of users storing large amounts of data in the Recycle Bin to circumvent their space limits (allocations).

Creating a Space Allocation Policy

Create a space allocation policy to set disk space quotas for users.

▼ **To create a space allocation policy:**

1. On the management pane, right-click **Space Allocation Policies**, point to **New**, and then click **Space Allocation Policy**.
2. On the **Welcome** screen, click **Next**.
3. Type a name for the policy and a description of the policy, and then click **Next**.
4. On the **Space Limits and Options** dialog box, complete the appropriate options as follows, and then click **Next**:

Space Limits and Options dialog box options

Item	Description
Limits	
Disk space limit	Enter the disk space limit and specify a qualifier from the drop-down list. The disk space limit determines the maximum amount of space the managed resource can use. On a Network Appliance Filer, the disk space limit must be one KB or larger. The value you enter for the disk space limit can be overridden by the value in the **Minimum limit** field on the **Space Allocation** global property tab; for more information about this field, read "Setting Space Allocation Properties" on page 41.
Overdraft limit	Enter the overdraft limit and specify a qualifier from the drop-down list. The overdraft limit is the amount of space by which the disk space limit can be exceeded before Storage Exec enforces the disk space limit. The disk space limit will not be enforced until the disk space limit plus the overdraft limit has been reached. The overdraft limit does not apply if the managed resource resides on a Network Appliance Filer.

Space Limits and Options dialog box options

Item	Description
Options	
Passive limit	Select this check box to monitor the disk space limit, but not enforce it. Since the limit will not be enforced, I/O operations will never be stopped. However, the alarms will still be activated after the space limit is reached. The **Passive limit** check box defaults to different values under different circumstances. The check box is selected by default if you create a space allocation managed resource on a drive or partition *and* you do not select the **Allow active limit on devices** check box (located on the **Space Allocation** tab of the global Properties dialog box). The check box is selected by default if you create a space allocation managed resource on a system drive or system partition *and* select the **Allow active limit on devices** check box. VERITAS recommends that any disk space limit set on the system or boot partition be passive. If a disk space limit is set on the system or boot partition and is not passive, there may be trouble booting because system startup performs I/O to the system partition.
Always save open files	Select this option to enable a single I/O that exceeds the space limit to complete. However, the next I/O will fail (if the **Passive limit** option is not selected). Example: A user has a 50 MB space limit and is currently at 49 MB. The user opens a file, adds 5 MB of content to that file, and then tries to save the file. Because the space limit for that user is now exceeded, the file would not be saved unless the **Always save open files** option is selected. This option cannot be used with a policy for a Network Appliance Filer.
Reset high-water mark	Select this option to reset the high-water mark. The high-water mark is the largest amount of disk space limit that was ever used on a particular managed resource, even if files were deleted. This option cannot be used with a policy for a Network Appliance Filer.
Send disk full error code	Select this option to send the "disk full" error code instead of the "not enough quota is available" error code. This option cannot be used with a policy for a Network Appliance Filer.

Space Limits and Options dialog box options

Item	Description
Exclude from folder limit	Select this option to exclude a user (or a group) from the space limit calculation. Any files owned by the user will be excluded from the space limit. In addition, the space limit will not be in effect for that user. This option is only available for user space limits. Example: A `\Public` folder may be limited to 500 MB. However, the Administrators Group should not be limited from writing to this folder and the files owned by Administrators should not be counted against the space allocation on `\Public`. This can be accomplished by setting a disk space limit of 500 MB on `\Public` in conjunction with a space limit on the Administrators Group security identifier (SID) of the device capacity that is instructed to exclude from folder limit. In this case, apply a space allocation to a group, because when a member of the Administrators Group writes a file, the file is owned by the Administrators Group SID, not by this individual user. This option cannot be used with a policy for a Network Appliance Filer.

5. On the **Alarm Threshold Settings** dialog box, specify the percentage of disk space that can be used before Storage Exec issues an alarm. For each alarm that you want to set, complete the fields that display as follows:

Threshold Tab Fields

Item	Description
Threshold	Enter the percentage of the space limit that needs to be exceeded before the actions will occur. Valid values for the alarm threshold can be larger than 100%, because space limit can be passive or active. This percentage is based on the disk space limit alone and does not consider the overdraft limit. Thresholds do not enforce space limits, they are simply a means of warning users and/or taking some actions. Thresholds are exceeded in reverse order so that, of the five thresholds, the fifth threshold is exceeded first. This way the fifth threshold is the least critical and the first threshold is the most critical. Generally, the first threshold would have a value in the 90% – 100% range.

Threshold Tab Fields (continued)

Item	Description
Activate	Select **Activate Above** if you want to activate the alarm if the current disk space used exceeds the threshold value. Select **Activate Below** if you want to activate the alarm if the current disk space used falls below the threshold value. If you leave this field blank, the alarm is activated when the threshold is met.
Actions	Click this to set the following for each alarm: • Notification messages. Set up a message to send when a space allocation alarm is activated, and select the users who will receive the notification. See "Setting Up Space Allocation Alarm Notification" on page 74. • Commands to execute. Specify a Windows 2000 (or later) command that Storage Exec will execute if a space allocation alarm is activated. See "Executing Commands for Space Allocation Alarms" on page 76. • Reports to print. Set up a report to run when an alarm is activated. See "Setting Reports to Run for Space Allocation Alarms" on page 77. • Extended disk space quotas. Enter the amount to extend the disk space limit when the alarm is activated. See "Extending the Disk Space Limit" on page 78.

6. Click **Next**, and then click **Finish**.

Changing Space Allocation Policy Properties

For any default or custom space allocation policy, you can view and change the policy's properties, including the description, space limits, and alarm threshold settings.

Alarm thresholds allow you to specify actions to occur when a threshold value (a percentage of a space allocation) is exceeded. You may configure five alarm settings for non-Network Appliance computers and two alarm settings for Network Appliance Filers.

A threshold is activated only once until the percentage of used space drops below the threshold. For example, if threshold 3 is 70% and threshold 2 is 80% and the space limit is 71%, threshold 3 is activated. Threshold 3 will not be activated again, unless the value first drops below 70%. Threshold 2 will be activated if more files are saved and the value rises above 80%.

▼ To view and modify space allocation policy properties:

1. On the management pane, select **Space Allocation Policies**.
2. On the details pane, right-click the policy you want to view or modify, and then click **Properties**.
3. On the **Description** tab, enter or change the description of the policy. The policy description displays on the details pane next to the policy name.
4. On the **Space Limits and Options** tab, complete the appropriate options as follows, and then click **Next**:

Space Limits and Options dialog box options

Item	Description
Limits	
Disk space limit	Enter the disk space limit and specify a qualifier from the drop-down list. The disk space limit determines the maximum amount of space the managed resource can use. On a Network Appliance Filer, the disk space limit must be one KB or larger.
Overdraft limit	Enter the overdraft limit and specify a qualifier from the drop-down list. The overdraft limit is the amount of space by which the disk space limit can be exceeded before Storage Exec enforces the disk space limit. The disk space limit will not be enforced until the disk space limit plus the overdraft limit has been reached. The overdraft limit does not apply if the managed resource resides on a Network Appliance Filer.
Options	

Space Limits and Options dialog box options

Item	Description
Passive limit	Select this check box to monitor the disk space limit, but not enforce it. Since the limit will not be enforced, I/O operations will never be stopped. However, the alarms will still be activated after the space limit is reached. The **Passive limit** check box defaults to different values under different circumstances. The check box is selected by default if you create a space allocation object on a drive or partition *and* do not select the **Allow active limit on devices** check box (located on the **Space Allocation** tab of the global Properties dialog box). The check box is selected by default if you create a space allocation managed resource on a system drive or system partition *and* select the **Allow active limit on devices** check box. VERITAS recommends that any disk space limit set on the system or boot partition be passive. If a disk space limit is set on the system or boot partition and is not passive, there may be trouble booting as system startup performs I/O to the system partition.
Always save open files	Select this option to enable a single I/O that exceeds the space limit to complete. However, the next I/O will fail (if the **Passive limit** option is not selected). Example: A user has a 50 MB space limit and is currently at 49 MB. The user opens a file, adds 5 MB of content to that file, and then tries to save the file. Because the space limit for that user is now exceeded, the file would not be saved unless the **Always save open files** option is selected. This option cannot be used with a policy for a Network Appliance Filer.
Reset high-water mark	Select this option to reset the high-water mark. The high-water mark is the largest amount of disk space limit that was ever used on a particular managed resource, even if files were deleted. This option cannot be used with a policy for a Network Appliance Filer.
Send disk full error code	Select this option to send the "disk full" error code instead of the "not enough quota is available" error code. This option cannot be used with a policy for a Network Appliance Filer.

Space Limits and Options dialog box options

Item	Description
Exclude from folder limit	Select this option to exclude a user (or a group) from the space limit calculation. Any files owned by the user will be excluded from the space limit. In addition, the space limit will not be in effect for that user. This option is only available for user space limits. Example: A `\Public` folder may be limited to 500 MB. However, the Administrators Group should not be limited from writing to this folder and the files owned by Administrators should not be counted against the space allocation on `\Public`. This can be accomplished by setting a disk space limit of 500 MB on `\Public` in conjunction with a space limit on the Administrators Group security identifier (SID) of the device capacity. In this case, apply a space allocation to a group, because when a member of the Administrators Group writes a file, the file is owned by the Administrators Group SID, not by this individual user.) This option cannot be used with a policy for a Network Appliance Filer.

5. On the **Alarm Threshold Settings** dialog box, specify the percentage of disk space that can be used before Storage Exec issues an alarm. For each alarm that you want to set, complete the fields that display as follows:

Threshold Tab Fields

Item	Description
Threshold	Enter the percentage of the space limit that needs to be exceeded before the actions will occur. Valid values for the alarm threshold can be larger than 100%, because space limit can be passive or active. This percentage is based on the disk space limit alone and does not consider the overdraft limit. Thresholds do not enforce space limits, they are simply a means of warning users and/or taking some actions. Thresholds are exceeded in reverse order so that, of the five thresholds, the fifth threshold is exceeded first. This way the fifth threshold is the least critical and the first threshold is the most critical. Generally, the first threshold would have a value in the 90% – 100% range.

Threshold Tab Fields (continued)

Item	Description
Activate	Select **Activate Above** if you want to activate the alarm if the current disk space used exceeds the threshold value. Select **Activate Below** if you want to activate the alarm if the current disk space used falls below the threshold value. If you leave this field blank, the alarm is activated when the threshold is met.
Actions	Click this to set the following for each alarm: ◆ Notification messages. Set up a message to send when a space allocation alarm is activated, and select the users who will receive the notification. See "Setting Up Space Allocation Alarm Notification" on page 74. ◆ Commands to execute. Specify a Windows 2000 (or later) command that Storage Exec will execute if a space allocation alarm is activated. See "Executing Commands for Space Allocation Alarms" on page 76. ◆ Reports to print. Set up a report to run when an alarm is activated. See "Setting Reports to Run for Space Allocation Alarms" on page 77. ◆ Extended disk space quotas. Enter the amount to extend the disk space limit when the alarm is activated. See "Extending the Disk Space Limit" on page 78.

Setting Space Allocation Alarm Actions

You can set four different types of actions to occur when a space allocation alarm is activated. An alarm is activated when a user reaches the threshold value that you set for the policy. You can set:

- Notification messages. Set up a message to send when a space allocation alarm is activated, and select the users who will receive the notification.
- Commands to execute. Specify a Windows 2000 (or later) command that Storage Exec will execute if a space allocation alarm is activated.
- Reports to print. Set up a report to run when an alarm is activated.
- Extended disk space quotas. Enter the amount to extend the disk space limit when the alarm is activated.

▼ To set space allocation alarm actions:

1. On the management pane, click **Space Allocation Policies**.
2. On the details pane, right-click the policy whose alarm actions you want to set, and then click **Properties**.
3. On the **Alarm Threshold Settings** tab, click **Actions**.
4. Select the tab for the type of alarm action you want to set:
   - Notification messages. See "Setting Up Space Allocation Alarm Notification" on page 74.
   - Commands to execute. See "Executing Commands for Space Allocation Alarms" on page 76.
   - Reports to print. See "Setting Reports to Run for Space Allocation Alarms" on page 77.
   - Extended disk space quotas. See "Extending the Disk Space Limit" on page 78.

Setting Up Space Allocation Alarm Notification

The **Notification** tab enables you to specify the notification message and who should receive notification.

Notification Tab Fields

Item	Description
Message	Enter the notification message to send to the user, administrator, and/or Microsoft event log when the threshold alarm is activated. Message macros can be inserted in the message for customized output; see the section "Space Allocation Message Macros" on page 78 for a list of these macros. Select macros using the **Insert Macro** list. Click the plus sign (**+**) to save a message that can be selected later. Select a saved message (one that came with Storage Exec or one you saved yourself) by clicking the ellipses (**...**) button.
Notification options	
Notify user	Sends the notification message to the user who caused the threshold to be exceeded. This option is enabled by default, except on Windows XP computers. For Windows XP computers, you must manually enable this option. Storage Exec uses Windows messaging to deliver alarm messages. You can test or troubleshoot this capability using this command: `NET SEND username message-text`
Send SNMP trap	Uses SNMP traps to send the notification message to an SNMP client. The computer name, user name, object name, and threshold message will be sent to the SNMP client.
Record alarm	Writes information to the audit database indicating that an alarm has been activated.
Notify	Select this option to send the notification message to a user in the Administrators group when the user attempts to use more space than he or she is allocated. Select the user to notify from the drop-down list next to the **Notify** field. If the user who is logged on to Storage Exec is a domain user, Storage Exec populates the drop-down list with users from the Domain Administrators group. Otherwise, Storage Exec populates the drop-down list with users in the Administrators group on the local computer. If neither the Domain Administrators group nor the local Administrators group can be located, then only the Administrator will display in the drop-down list.
Event log options	

Notification Tab Fields (continued)

Item	Description
Send to event log	Select this option to send a notification message to the Microsoft Windows event log when this alarm is activated
Message level	Select the level of severity for the message: the options are **Severe**, **Warning**, and **Informational**.
Event log server	Specify the name of the server on which to send the notification message.
Mail options	
Mail To and **Mail CC**	Enter the email addresses where the notification message will be sent and copied. Do the following to send email: ◆ If you are using your Active Directory to get the email address of the message's recipient, use [USER NO DOMAIN]. ◆ If you are not using your Active Directory to get the email address of the message's recipient, use [USER NO DOMAIN]@*domain*.com. You can use this format only if the user name that triggered the alarm is also used in the email address. You may also use the macro [OWNER NO DOMAIN] in the **Mail To** and **Mail CC** fields. You must set email options in the global properties page before this option will work; for more information, read "Setting Mail Properties" on page 38. Two separators between email addresses are supported: comma and semicolon.
Subject	Enter the subject line of the email notification message.

Executing Commands for Space Allocation Alarms

The **Execute** tab enables you to specify a command that Storage Exec will execute if a space allocation alarm is activated. Usually the command is a batch file execution or a NET SEND. Separate lines in the text box by pressing ENTER after each line you type.

Parameters to batch files can be hardcoded or you can click **Insert macro** to use these Storage Exec macros:

- Domain name
- Domain name without quotes
- Notification message. This is the message specified in the **Message** field of the **Notification** tab.
- Notification message without quotes
- Managed resource against which a quota threshold was exceeded
- Owner of the file
- Owner without quotes
- User who triggered the action. This will include the domain name.
- User without domain name
- User without domain name or quotes

Do not specify a command that requires interaction with the desktop.

Note When a program or command is executed by the Storage Exec Network Appliance Option, it is executed on the computer on which you entered the Network Appliance Option serial number.

Setting Reports to Run for Space Allocation Alarms

The **Report** tab enables you to specify the report to run when an alarm is activated.

The fields on the **Report** tab are available only if you are running the Storage Exec Enterprise Administration Option.

Report Tab Fields

Item	Description
Report	
Server	Select the server you want to use to run the report.
Report	Select the report you want to run when an alarm is activated.
Output options	
Save To	Enter the folder where the report is to be saved.
Mail To and **Mail CC**	Enter the email addresses where the report output will be sent and copied. You can type the email addresses directly or use macros. To use macros: • If you are using the Active Directory to get the email address of the report's recipient, use [USER NO DOMAIN]. • If you are not using the Active Directory to get the email address of the report's recipient, use [USER NO DOMAIN]@*domain*.com. You can use this format only if the user name that triggered the alarm is also used in the email address. You may also use the macro [OWNER NO DOMAIN] in the **Mail To** and **Mail CC** fields. You must set email options in the global properties page before this option will work; for more information, see "Setting Mail Properties" on page 38. Two separators between email addresses are supported: comma and semicolon.
Subject	Enter the subject line of the email report.
Schedule options	
Schedule interval	Select when the report is to run. Depending on your choice, you may need to provide additional parameters (such as time of the day and day of the week).

Extending the Disk Space Limit

The **Extend** tab enables you to adjust the disk space limit when an alarm is activated.

Extend Tab Fields

Item	Description
Adjust disk space limit	Enter the amount to extend the disk space when the threshold is exceeded. Disk space limit can be in bytes, kilobytes, or megabytes.
Repeat value	Enter the number of times the disk space limit can be increased.
Current	Shows the number of times the disk space limit has been increased.

Clicking the **Reset** button resets the value in the **Current** field to 0.

Space Allocation Message Macros

You can use the macros in the following table when specifying the message that Storage Exec generates to notify users after a space allocation alarm is triggered. You use the space allocation macros in the **Message** field on the **Notification** tab of an alarm's **Actions** dialog box.

Note Not all macros are applicable to messages generated by the Storage Exec Network Appliance Option. These macros are identified by an asterisk (*) in the table below.

Space Allocation Macros

Macro	Description
[ACTIVATE TYPE]	Activate above or below threshold value.
[ALARM NUMBER]	Alarm numbers 1-5.
[ALARM PERCENT]	Percentage of the disk space limit that can be used before Storage Exec issues an alarm.
[CURRENT USAGE]	Current space use in bytes.
[CURRENT USAGE KB]	Current space use in kilobytes.
[CURRENT USAGE MB]	Current space use in megabytes.
[DOMAIN]	Domain name.

Space Allocation Macros (continued)

Macro	Description
[FILE NAME]	Name of the file that caused the action.
[FILE OWNER]	Owner of the file that caused the action.
[FILE SPEC]	File path and name.
[FREE SPACE LIMIT]	Unused space limit in bytes.
[FREE SPACE LIMIT KB]	Unused space limit in kilobytes.
[FREE SPACE LIMIT MB]	Unused space limit in megabytes.
[HIGHWATER] *	High-water mark in bytes.
[HIGHWATER KB] *	High-water mark in kilobytes.
[HIGHWATER MB] *	High-water mark in megabytes.
[OBJECT DIR OWNER] *	Evaluates to the owner of the directory that the space allocation is set on. For example, if the space allocation is set on `D:\Finance` and the NTFS owner of `D:\Finance` is "\\Domain\User1," [OBJECT DIR OWNER] evaluates to "User1".
[OBJECT NAME]	Evaluates to the directory name that the space allocation is set on. For example, if the space allocation is set on `D:\users\jdoe`, [OBJECT NAME] evaluates to "D:\users\jdoe".
[OBJECT NAME SHARE] *	The shared name of the object. This macro returns a normal share (for example, \\abc\C\test) if Storage Exec can find it. Otherwise, the macro returns a default or administrator share (for example, \\abc\C$\test).
[OPENED FILE] *	File that caused the action.
[OVERDRAFT] *	Overdraft in bytes.
[OVERDRAFT KB] *	Overdraft in kilobytes.
[OVERDRAFT MB] *	Overdraft in megabytes.
[OWNER] *	Owner of the file that caused the action.
[OWNER NO DOMAIN] *	Owner of the file that caused the action without domain name.
[PERCENT FREE]	Percent of free space limit.

Space Allocation Macros (continued)

Macro	Description
[PERCENT USED]	Percent of used space limit.
[POLICY NAME]	Name of the policy applied.
[SERVER NAME]	Server name where an alarm is triggered.
[SPACE LIMIT]	Disk space limit in bytes.
[SPACE LIMIT KB]	Disk space limit in kilobytes.
[SPACE LIMIT MB]	Disk space limit in megabytes.
[USER] *	Current user who caused the action.
[USER NO DOMAIN] *	Evaluates to the user name of the user who performed the write operation that triggered the alarm. For example, if the user is "\\Domain\Mark," then the [USER NO DOMAIN] macro evaluates to "Mark".

Best Practices for Space Allocation

These best practices help you use the Storage Exec space allocation feature.

- Implement passive limits initially. By applying passive limits, users will not be hindered by space allocation enforcement; however, you can still monitor disk consumption. With passive limits, you can implement a space allocation value, rather than a percentage of current usage. For example, your corporate SRM policy may specify that each user's home directory should be no larger than 100 MB. By implementing a passive 100 MB limit, you can quickly and easily determine who is violating that policy. Exceptions can be made, and space allocation can be enforced at a later date.

  This practice minimizes disruption to users during the information-gathering phase after Storage Exec is first installed. Frequently, the policies never need to be enforced to gain the benefit of implementing those policies. After the users realize that their space consumption and file-writing activities are being monitored on the corporate servers, they tend to be more conscientious of what and how much they store.

  Additionally, customized notification messages issued when space allocation alarm thresholds are exceeded educate the users and provide a means for them to manage their own disk space.

One example of the customized alarm action is the following notification message sent to the user: "Space limit is approaching for [USER] on [OBJECT NAME]. Current space used is [CURRENT USAGE MB]. Please perform some maintenance on your files. Failure to do so may restrict future access to [SERVER NAME]." For more information about the space allocation notification messages, read the section "Setting Up Space Allocation Alarm Notification" on page 74.

- Use auto detect managed resources. Auto detection automates the application of storage policies when new users or directories are added to the server. Auto detection works for both subfolder resources and user resources. With Auto Detect Subfolders, a specified policy is applied to a subfolder as it is created under the chosen root. Likewise, with Auto Detect Users, a specified policy is applied to each user who owns a file within the selected object. Auto detection should be implemented wherever possible because of its explicit benefit.

  Before you implement Auto Detect Users, you should analyze the space requirements for users and apply separate policies for those users who require an exception to the policy you want to apply via auto detection. For example, 95 out of 100 users require 250 MB or less of disk space. The remaining 5 users require between 500 MB and 1 GB of disk space. For those 5 users, you should apply a space allocation policy that enables them to have the space that they require *before* you set the auto detect users feature.

- Use disk full error message. When enforcing space allocation, send the "Disk full" error message with enforcement. Storage Exec integrates with the operating system to return valid, supported Windows 2000 error messages back to a client when space allocation is enforced. The two supported error messages are: "Not enough quota is available" and "Disk full." Though both are fully supported Windows 2000 error messages, experience has shown that many Microsoft applications and non-Windows 2000 operating systems do not properly handle or translate the "Not enough quota is available" error message. "Disk full" is universally understood and properly handled by applications and operating systems.

  Error messages are only returned if the space allocation policy is enforced. Regardless of enforcement, customized alarm actions still occur. Because the "Disk Full" error message is better understood by applications and client operating systems, the benefit of using this error message is reduced training for end users.

- Use overdrafts. If enforcing space allocation, provide the appropriate overdraft or at least use the **Always save open files** option. The overdraft allows for space allocation to be exceeded by the specified overdraft value. The **Always save open files** option allows quota to be exceeded only by the size of the file the user is modifying.

File Blocking 6

This chapter contains the following sections:

Introduction to File Blocking

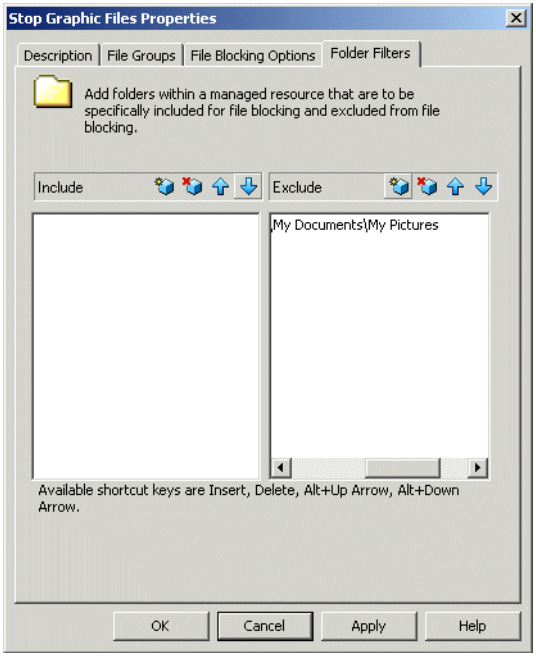
Storage Exec enables you to block users from creating and copying certain types of files, such as graphics files or media files, on a managed resource. To block files on a managed resource, you apply a file blocking policy to the resource. You can create custom file blocking policies to set the types of files you want to block or you can use the default file blocking policies that are included with Storage Exec. The default file blocking policies are:

- Monitor executables and scripts. Allows users to save executable and script files on the resources, but sends an alert.
- Stop executables and scripts. Stops users from saving executable and script files to the resources, and sends an alert.
- Stop graphic files. Stops users from saving graphics files on the resources, and sends an alert.
- Stop media files. Stops users from saving media files on the resources, and sends an alert.
- Stop user email. Stops users from saving email files on the resources, and sends an alert.

In file blocking policies, files are categorized into file groups, such as email files, internet files, or executable files. Storage Exec includes several default file groups, but you can also create custom file groups.

You can customize any file blocking policy to include or exclude specific folders from the policy. For example, if you want to block graphic files from every folder on a managed resource except the My Pictures folder, you can exclude the My Pictures folder from the policy.

Including and Excluding Folders



Related Topics:

- "Introduction to File Groups" on page 97

Creating a File Blocking Policy

Create a file blocking policy to set the types of files that you want to block.

▼ **To create a file blocking policy:**

1. On the management pane, right-click **File Blocking Policies**. Point to **New**, and then click **File Blocking Policy**.
2. On the **Welcome** screen, click **Next**.
3. Type a name for the policy and a description of the policy, and then click **Next**.
4. Select the file groups you want Storage Exec to block. Clear the check boxes for the file groups you do not want to block. Click **Next**.
5. Complete the fields that display as follows:

File Blocking options

Field	Description
Passive	Select this check box to monitor files, but not block them. Clear this check box to block files. If you select this, Storage Exec sends notification to users when they attempt to create or copy blocked file groups.
Check file content	Select this check box to enable Storage Exec to check file content in addition to the type of file. Clear this check box to enable Storage Exec to check only file extensions. When you select the **Check file content** option for file blocking policies or managed resources, you may get the following message: `File group(s) containing the following file extensions have been selected for use with content checking file blocking. This feature relies on registered signatures that do not exist for the following file types: <a list of file types>.` As new file types appear on the market, they may not necessarily be included in Storage Exec's list of known file name extensions. To check file content of such new file types, they need to be added to Storage Exec's list and file signatures need to be created for them. If you have seen new file types in your environment and you want them to be blocked by content, contact VERITAS technical support and our staff will create file signatures for these new file types.

6. Click **Actions** if you want to:

   - Set up a file blocking notification message and determine who should receive the notification. See "Setting Up File Blocking Alarm Notification" on page 90.
   - Specify a command to execute if a file blocking alarm is activated. See "Executing Commands for File Blocking Alarms" on page 92.
   - Specify a report to run if a file blocking alarm is activated. See "Setting Reports to Run for File Blocking Alarms" on page 93.

   If you do not want to perform any of the above actions, click **Next**.

7. On the **Folder Filters** dialog box, optionally specify folders to include in the file blocking policy or to exclude from the file blocking policy. Use these buttons:

	Add folders to the list.
	Remove folders from the list.
 and 	Move folders up and down in the list. The order of the folders does not affect the way Storage Exec processes them; ordering them is for your convenience only.

8. Click **Next**, and then click **Finish**.

Changing File Blocking Policy Properties

For any default or custom file blocking policy, you can view and change the policy's properties, including the description, the types of file groups that are blocked with the policy, the alarm settings, and the folder filters.

▼ **To view and modify file blocking policy properties:**

1. On the management pane, click **File Blocking Policies**.
2. On the details pane, right-click the policy you want to view or modify, and then click **Properties**.
3. On the **Description** tab, enter or change the description of the policy. The policy description displays on the details pane next to the policy name.
4. On the **File Groups** tab, select the check boxes next to the file groups that you want to block with this policy, or clear the check boxes next to the file groups that you want to remove from this policy.
5. On the **File Blocking Options** tab, select or clear the check boxes.

Alarm Tab Fields

Field	Description
Passive	Select this check box to monitor files, but not block them. Clear this check box to block files.
Check file content	Select this check box to enable Storage Exec to check file content. Clear this check box to enable Storage Exec to check only file extensions. When you select the **Check file content** option for file blocking policies or managed objects, you may get the following message: `File group(s) containing the following file extensions have been selected for use with content checking file blocking. This feature relies on registered signatures that do not exist for the following file types: <a list of file types>.` As new file types appear on the market, they may not necessarily be included in Storage Exec's list of known file name extensions. To check file content of such new file types, they need to be added to Storage Exec's list and file signatures need to be created for them. If you have seen new file types in your environment and you want them be blocked by content, contact VERITAS technical support and our staff will create file signatures for these new file types.

6. To change the notification, commands to execute, or the report settings for this policy, click **Actions**. See "Setting File Blocking Alarm Actions" on page 88 for information about changing these settings.

7. On the **Folder Filters** tab, optionally specify folders to include and exclude from the file blocking process. Use these buttons:,

	Add folders to the list.
	Remove folders from the list.
 and 	Move folders up and down in the list. The order of the folders does not affect the way Storage Exec processes them; ordering them is for your convenience only.

8. Click **OK**.

Setting File Blocking Alarm Actions

You can set three different types of actions to occur when a file blocking alarm is activated. An alarm is activated when a user attempts to create or copy a blocked file type on a managed resource to which the policy is applied. You can set:

- Notification messages. Set up a message to send when a file blocking alarm is activated, and determine the users who will receive the notification.
- Commands to execute. Specify a Windows 2000 (and later) command that Storage Exec will execute if a file blocking alarm is activated.
- Reports to print. Set up a report to run when an alarm is activated.

▼ To set file blocking alarm actions:

1. On the management pane, click **File Blocking Policies**.

2. On the details pane, right-click the policy whose alarm actions you want to set, and then click **Properties**.

3. On the **File Blocking Options** tab, click **Actions**.

4. Select the tab for the type of alarm action you want to set:
   - **Notification**. For more information, see "Setting Up File Blocking Alarm Notification" on page 90.
   - **Execute**. For more information, see "Executing Commands for File Blocking Alarms" on page 92.
   - **Report**. For more information, see "Setting Reports to Run for File Blocking Alarms" on page 93.

Setting Up File Blocking Alarm Notification

The **Notification** tab enables you to specify the notification message to send when an alarm is activated, and who should receive the notification.

Notification Tab Fields

Field	Description
Message	Enter the notification message to send to the user, administrator, and/or Microsoft event log when the alarm is activated. You can also select macros for messages using the **Insert Macros** list. When you select a macro, Storage Exec inserts pre-defined text into the message field. The available macros are: Note: The macros marked with an asterisk (*) are not applicable to messages generated by the Storage Exec Network Appliance Option. - **Blocking group** - Name of the blocking group used. - **Domain** *- Domain name. - **File name** * - Name of the file that caused the action. - **File owner** * - Name of the owner of the file that caused the action. - **File spec** * - File path and name. - **Object name** - Name of the object that caused the action. - **Object name share** - Shared name of the object. For example, you can share "h" as h:\drive and the macro will display the share name. - **Owner** - Name of the owner of the file that caused the action. Includes domain information. - **Owner no domain** - Name of the owner of the file that caused the action, without the domain information. - **Policy name** - Name of the policy that is applied to the managed resource. - **Server name** - Name of the server where an alarm has been activated. - **User** - Current user who caused the action. Includes domain information. - **User no domain** - Current user who caused the action, without the domain information. Click the plus sign **(+)** to save a message so it can be selected later. Select a saved message (one that came with Storage Exec or one you saved yourself) by clicking the ellipses **(...)** button.
Notification options	

Notification Tab Fields (continued)

Field	Description
Notify user	Sends the notification message to the user who attempted to save a blocked file type. Storage Exec uses Windows messaging to deliver alarm messages. You can test or troubleshoot this capability using this command: `NET SEND username message-text`
Notify	Select this option to send the notification message to a user in the Administrators group when the user attempts to save a blocked file type. Select the user to notify from the drop-down list next to the **Notify** field. If the user who is logged on to Storage Exec is a domain user, Storage Exec populates the drop-down list with users from the Domain Administrators group. Otherwise, Storage Exec populates the drop-down list with users in the Administrators group on the local computer. If neither the Domain Administrators group nor the local Administrators group can be located, then only the Administrator will display in the drop-down list.
Send SNMP trap	Uses SNMP traps to send the notification message to an SNMP client. The computer name, user name, resource name, and threshold message will be sent to the SNMP client. The following are the Storage Exec SNMP registered Management Information Block (MIB) and related values: - Storage Exec SNMP registered MIB - 1.3.6.1.4.1.3083 - Computer name - 1.3.6.1.4.1.3083.2.1.0 - Resource name - 1.3.6.1.4.1.3083.2.2.0 - User name - 1.3.6.1.4.1.3083.2.3.0 - Message - 1.3.6.1.4.1.3083.2.4.0
Record alarm	Writes information to the audit database that an alarm has been activated.
Event log options	
Send to event log	Select this check box to send notification messages to the Microsoft event log.
Message level	If you selected the **Send to event log** check box, you can choose the message level from the message drop-down list; the options are **Severe**, **Warning**, and **Informational**.
Event log server	Enter the name of the server on which the event log is located.

Notification Tab Fields (continued)

Field	Description
Mail options	
Mail to and **Mail CC**	Enter the email addresses where the notification message will be sent and copied. Do the following to send email: • If you are using the Active Directory to get the email address of the message's recipient, use [USER NO DOMAIN]. • If you are not using the Active Directory to get the email address of the message's recipient, use [USER NO DOMAIN]@*domain*.com. You can use this format only if the user name that triggered the alarm is also used in the email address. You may also use the macro [OWNER NO DOMAIN] in the **Mail to** and **Mail CC** fields. You must set email options in the global properties page before this option will work; for more information, see "Setting Mail Properties" on page 38. Two separators between email addresses are supported: comma and semicolon.
Subject	Enter the subject line for the email notification message.

Related Topics:

- "File Blocking and Network Appliance Filers" on page 177

Executing Commands for File Blocking Alarms

The **Execute** tab enables you to specify a Windows 2000 (and later) command that Storage Exec will execute if a file blocking alarm is activated. Usually the command is a batch file execution or a NET SEND. Separate lines in the text box by pressing ENTER after each line you type.

Parameters to batch files can be hardcoded or you can click **Insert macro** to use these Storage Exec macros:

- Domain name
- Domain name without quotes
- Notification message. This is the message specified in the **Message** field of the **Notification** tab.
- Notification message without quotes

- Managed resource against which a quota threshold was exceeded.
- Owner of the file
- Owner without quotes
- User who triggered the action. This will include the domain name.
- User without domain name
- User without domain name or quotes

Do not specify a command that requires interaction with the desktop.

Note When a program or command is executed by the Storage Exec Network Appliance Option, it is executed on the remote agent and not the Network Appliance Filer.

Setting Reports to Run for File Blocking Alarms

The **Report** tab enables you to specify the report to run when an alarm is activated.

Report Tab Fields

Field	Description
Report	
Server	Select the server you want to use to run the report.
Report	Select the report to run. For more information about the available reports, see "Predefined Reports" on page 133.
Output options	
Save To	Enter the folder where the report is to be saved.

Report Tab Fields (continued)

Field	Description
Mail To and **Mail CC**	Enter the email addresses where the report output will be sent and copied. Do the following to send email: • If you are using the Active Directory to get the email address of the message's recipient, use [USER NO DOMAIN]. • If you are not using the Active Directory to get the email address of the message's recipient, use [USER NO DOMAIN]@*domain*.com. You can use this format only if the user name that triggered the alarm is also used in the email address. You may also use the macro [OWNER NO DOMAIN] in the **Mail To** and **Mail CC** fields. You must set email options in the global properties page before this option will work; for more information, see "Setting Mail Properties" on page 38. Two separators between email addresses are supported: comma and semicolon.
Subject	Enter the subject line of the email report.
Schedule options	
Schedule interval	Select when the report should run. Depending on your choice, you may need to provide additional parameters (such as time of the day and day of the week).

Best Practices for File Blocking

These best practices help you use the Storage Exec file blocking feature.

- Create file blocking policies that suit your site's needs. Storage Exec allows you to create your own file groups and file blocking policies in addition to the standard ones. This gives you the flexibility to customize file groups or policies for your corporate standards.
- Create customized file blocking messages. In Storage Exec, file blocking is integrated with the operating system so that it returns a supported Windows 2000 error message when a blocking rule is enforced. The supported Windows 2000 error messages may not provide enough detail to the user. Therefore, we suggest that you also create a custom message within a file-blocking managed resource policy that provides more detail to the user. The messages are entered in the Message area of the Notification tab on the **Actions** dialog box. For example, you may enter the following message: "The network detected that you may have attempted to save media files on [SERVER NAME]. These files are not permitted. Contact John Smith at extension 1234 with questions." You can modify file blocking messages when you modify an existing file blocking policy or managed resource.

File Groups 7

This chapter contains the following sections:

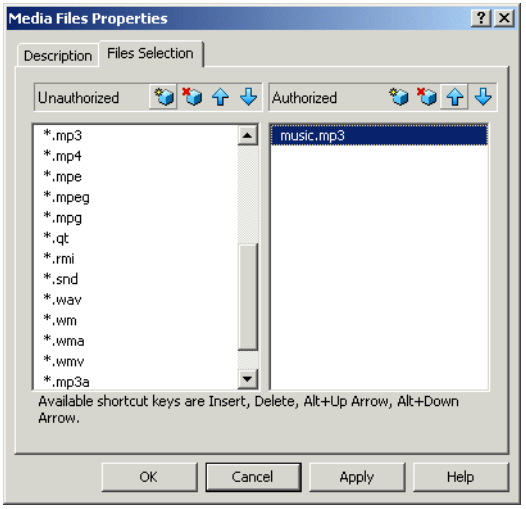
Introduction to File Groups

File groups consist of a set of files that may or may not be related. For example, a graphics file group might contain files with .jpg and .bmp extensions. Within a file group, you can determine which types of files are authorized and which types are unauthorized.

Unauthorized files are those files that Storage Exec will not allow to be saved. Files can be blocked by extension and/or name. For example, if you specify that *.mp3 files are unauthorized, Storage Exec will block all .mp3 files from being saved. If you specify that `test.mp3` is unauthorized, only files with that specific name are blocked.

Authorized files are the files that are allowed to be saved; they are typically exceptions to the unauthorized rules. For example, even though *.mp3 files may be unauthorized, the specific file `music.mp3` can be added to the authorized file list and then allowed to be saved. Full wild carding is supported.

Unauthorized and Authorized Files



File groups are used in file blocking policies. You can set the types of file groups to associate with each policy. For example, you can associate the Graphics Files file group to the Stop Graphic Files file blocking policy.

File groups are also used in reports to filter data for the report.

Warning: Storage Exec does not check the content of an authorized file, even if the **Check file content** option is enabled. The following could potentially happen:

1. You create a file group and unauthorize all files (*.*), but authorize files with specific extensions (*.doc and *.xls).

2. You create a policy that uses this file group with the **Check file content** option enabled.

3. You create a managed resource using this policy.

4. A user renames a .jpg file so that it has a file name extension of .doc.

5. The user copies the file into the folder being monitored by the managed resource. Storage Exec does not block the file because the extension is authorized. The file can be opened using the "open with" option of an application that is capable of viewing image files. Even though the **Check file content** option was enabled, Storage Exec does not check the file content because the file type is authorized.

Related Topics:

- "Introduction to File Blocking" on page 83

Creating a New File Group

Storage Exec is shipped with several default file groups. You can use the default file groups or you can create custom file groups to meet the needs of your organization.

▼ **To create a new file group:**

1. On the management pane, right-click **File Groups**, point to **New**, and then click **File Group**.
2. On the **Welcome** screen, click **Next**.
3. Enter a name for the file group in the **Group name** field, and enter up to 50 characters of descriptive text in the **Description** field.
4. Click **Next**
5. Enter unauthorized and/or authorized files for this file group. You can use wild cards in file names. Use the following buttons:
   -  to enter a file name
   -  to remove files from the list
   -  to move files up and down the list
6. Click **Next**, and then click **Finish** to create the new file group.

Deleting a File Group

▼ **To delete a file group:**

1. On the management pane, select **File Groups**.
2. On the details pane, right-click a file group, and then click **Delete**.
3. A message displays prompting for confirmation. Click **Yes** to delete the file group.

Viewing and Modifying File Group Properties

▼ **To view or modify file group properties:**

1. On the management pane, select **File Groups**.
2. On the details pane, double-click the file group you want to view or modify. The **File Group Properties** dialog box displays.
3. On the **Description** tab, enter up to 50 characters of descriptive text in the **Description** field.
4. On the **Files Selection** tab, add and remove unauthorized and authorized files. You can use wild cards in file names. Use the following buttons:
   -  to enter a file name
   -  to remove files from the list
   -  and  to move files up and down the list
5. Click **OK** to modify the file group properties.

Note You cannot change the file group's name on the **File Group Properties** dialog box. To change a file group name, read the section "Renaming a File Group" on page 101.

Copying a File Group

▼ **To copy a file group:**

1. On the management pane, select **File Groups**.
2. On the details pane, right-click the file group you want to copy. Choose **Copy**.
3. Right-click in the details pane and choose **Paste**. A new file group, named "Copy of *file-group-you-selected*" displays in the list.
4. Rename the new file group by right-clicking it and choosing **Rename**, entering the new name in the text field, and pressing ENTER.
5. Change the properties of the new file group as appropriate as described in the section "Viewing and Modifying File Group Properties" on page 100.

Renaming a File Group

▼ **To rename a file group:**

1. On the management pane, highlight **File Groups**.
2. On the details pane, right-click a file group, and then click **Rename**.
3. Enter the new name in the text field and press ENTER.

Report Queries 8

This chapter contains the following sections:

Introduction to Report Queries

Report queries define the content and appearance of a report. There are two types of report queries: Standard and Enhanced.

- With Standard report queries, you can change some properties, such as the description or the columns that display.

  On the details pane, standard report queries are labelled with this icon: 

- Enhanced report queries are available only with the Storage Exec Advanced Reporting Option. If you have the Advanced Reporting Option, you can customize the default queries to meet the needs of your environment or you can create new queries. On the details pane, enhanced report queries are labelled with this icon: 

  An enhanced report query can report on detail information or summary information. Detail information might be a list of files that meet a specific criteria, while summary information might provide the total amount of storage each user is using.

  When a report query provides detail information, Storage Exec produces the report in one pass through the data. When a report query provides summary information, Storage Exec produces the report in two passes. The first pass produces raw data (for example, a list of the seven files that user 1 is storing, and their sizes), and the second pass summarizes the data (the fact that user 1 is using 100 MB of storage, user is using 240 MB of storage, and so on).

Related Topics:

- "Introduction to Reports" on page 121
- "Creating a Report Query" on page 104
- "Deleting a Report Query" on page 119
- "Viewing and Changing Report Query Properties" on page 107
- "Copying a Report Query" on page 119
- "Renaming a Report Query" on page 120

Creating a Report Query

You must be running the Storage Exec Advanced Reporting Option to create a report query.

To create a standard report query, see "Creating a New Standard Report Query" on page 104.

To create an enhanced report query, see "Creating a New Enhanced Report Query" on page 105.

Creating a New Standard Report Query

▼ **To create a new standard report query:**

1. On the management pane, right-click **Report Queries**.
2. Point to **New**, and then click **Report Query**. On the **Welcome** screen, click **Next**.
3. On the **Name and Description** dialog box, enter the name and description of the report query you are creating, and then click **Next**. The description is included in the report header.

   Do not use these characters in the report query name: + # = ; , " \ / < >
4. Select **Standard**, and then click **Next**.

5. On the **Data Source** dialog box, select the data source for the report, and then click **Next**. Your choices are:
   - **Active file system**. If you select this, data is selected from the File System and Active Directory metadata.
   - **Managed resource database**. If you select this, data is selected from the Storage Exec managed resource database. For example, server, policy, and space limits can be selected.
   - **Trend database**. If you select this, data is selected from the Storage Exec trend database. For example, high water marks, used disk space, and overdrafts can be selected.
6. On the **Display Fields** dialog box, select the columns you want to display on reports that use this query. Select an item from the **Fields** option, then use the right arrow to move the items you select to the **Selected Fields** option. Items in the **Selected Fields** option will display on the report. See the section "Setting Display Field Options for Report Queries" on page 111 for additional information. Click **Next**.
7. On the **Filter Criteria** dialog box, specify the criteria to use to filter the data on the report. For more information, see "Setting Filter Criteria for Report Queries" on page 109. Click **Next**.
8. On the **Graph** dialog box, select graph options for the report. See the section "Setting Graph Options for Report Queries" on page 118 for additional information. Click **Next**.
9. Click **Finish** to create a new report query. If you do not want to create a new report using this query at this time, clear the **Start the Report Wizard to create a report using this wizard** check box.

Creating a New Enhanced Report Query

▼ **To create a new enhanced report query:**

1. On the management pane, right-click **Report Queries**.
2. Click **New**, and then click **Report Query**. On the **Welcome** screen, click **Next**.
3. On the **Name and Description** dialog box, enter the name and description of the report query you are creating, and then click **Next**. The description is included in the report header.

   Do not use these characters in the report query name: + # = ; , " \ / < >

4. Select **Enhanced**, and then click **Next**.

5. On the **Data Source** dialog box, select the data source for the report, and then click **Next**. Your choices are:

   - **Active file system**. If you select this, data is selected from the File System and Active Directory metadata.
   - **Managed resource database**. If you select this, data is selected from the Storage Exec managed resource database. For example, server, policy, and space limits can be selected.
   - **Trend database**. If you select this, data is selected from the Storage Exec trend database. For example, high water marks, used disk space, and overdrafts can be selected.

6. On the **Display Fields** dialog box, select the columns you want to display on reports that use this query. Select an item from the **Fields** option, then use the right arrow to move the items you select to the **Selected Fields** option. Items in the **Selected Fields** option will display on the report. See the section "Setting Display Field Options for Report Queries" on page 111 for additional information. Click **Next**.

7. On the **Filter Criteria** dialog box, specify the criteria to use to filter the data on the report. For more information, see "Setting Filter Criteria for Report Queries" on page 109. Click **Next**

8. On the **Sort** dialog box, define the order of the files in a report. See the section "Setting Report Break and Sort Options for Report Queries" on page 112 for additional information. Click **Next**.

9. On the **Total** dialog box, select the order of the columns' totals, which are determined by the order of the fields in the **Selected Fields** list. See the section "Setting Total Options for Report Queries" on page 114 for additional information. Click **Next**.

10. On the **Summary Filter Criteria** dialog box, specify the criteria to use to filter the summarized data on the report. See the section "Setting Summary Filter Options for Report Queries" on page 115 for additional information. Click **Next**.

11. On the **Summary Sort Options** dialog box, define the order of the files in the report summary. See the section "Setting Summary Sort Options for Report Queries" on page 116 for additional information. Click **Next**.

12. On the **Summary Total** dialog box, select the order of the column totals, which are determined by the order of the fields in the **Selected Fields** list. See the section "Setting Summary Total Options for Report Queries" on page 117 for additional information. Click **Next**.

13. On the **Graph Options** dialog box, select graph options for the report. See the section "Setting Graph Options for Report Queries" on page 118 for additional information. Click **Next**.

14. Click **Finish** to create a new report query. If you do not want to create a new report using this query at this time, clear the **Start the Report Wizard to create a report using this wizard** check box.

Viewing and Changing Report Query Properties

You can view and change the properties of existing report queries. Different types of properties display depending on the type of report query you select.

▼ **To view or change report query properties:**

1. On the management pane, select **Report Queries**.

2. On the details pane, right-click the report query you want to view or change.

3. Click **Properties**.

4. To change the report description that displays on the report header, on the **Description** tab, type the new description.

5. Select the tab for the type of property you want to change. For details about the options on each tab, see the appropriate topic from the following list:
   - "Setting the Range for Report Queries" on page 108
   - "Setting Filter Criteria for Report Queries" on page 109
   - "Setting Display Field Options for Report Queries" on page 111
   - "Setting Report Break and Sort Options for Report Queries" on page 112
   - "Setting Total Options for Report Queries" on page 114
   - "Setting Summary Filter Options for Report Queries" on page 115
   - "Setting Summary Sort Options for Report Queries" on page 116
   - "Setting Summary Total Options for Report Queries" on page 117
   - "Setting Graph Options for Report Queries" on page 118

Setting the Range for Report Queries

When you view properties for certain types of report queries, Storage Exec displays a **Settings** tab. This tab enables you to set the range for data in the report query. Additional fields may display on the **Settings** tab, depending on the type of report query you are viewing.

To change the range settings for a report query, select a new range from the drop-down lists.

For the Space by Folder Resource report query, you can also set the following options:

Space by Folder Resource Ranges

Item	Description
All levels	Select this option to include all directory levels in the report query. If you do not want to include all levels, enter a specific number of levels in the **Number of levels** field.
Number of levels	Select this option to include a specific number of directory levels in the report query. After you select the option, type the number of levels to include in the query.

For the Duplicate File Summary and the Files with Duplicates report queries, you can also set the following options:

Duplicate File Summary and FIles with Duplicates Ranges

Item	Description
Exact name match	Select this option to include only those files that have the exact same name on the report.
Close name match	Select this option to include all files that have similar names on the report. You can determine how close the file name and the file extension should match by typing a percentage amount in the **File Name** and **Extension** fields.
Compare contents	Select this option to enable Storage Exec to compare the contents of files that are included in the report.

Setting Filter Criteria for Report Queries

The Filter Criteria property defines the files that are selected for the report.

There are two types of filters: simple and complex.

- Simple: <Field Name> <Operator> <Value>

  The following example selects all files with an allocated size greater than 1024 KB:

  SizeAllocatedKB > 1024

- Complex:

  (Simple Filter) <Operator> (Simple Filter)

  or

  NOT(Simple Filter)

  The following example selects all files with the allocated size greater than 1024 KB and a creation date less than 30 days old:

  (SizeAllocatedKB > 1024) AND (CreatedDays < 30)

Date values are represented inside curly brackets in the form {MM/DD/YYYY HH:MM:SS}. The time portion of the date is optional.

Parentheses are not necessary, but they ensure that the proper evaluation is done. As in arithmetic, operations within parentheses are evaluated first. The order of precedence without parentheses is NOT AND OR.

These expressions are different:

- (SizeAllocatedKB > 1024) AND (CreatedDays < 30)
- SizeAllocatedKB > 1024 AND CreatedDays < 30

These expressions are the same:

- NOT(SizeAllocatedKB > 1024) AND (CreatedDays < 30)
- NOT(SizeAllocatedKB > 1024 AND CreatedDays < 30)

To specify filter criteria, complete the following fields:

Filter Criteria

Item	Description
Field name	Select the name of the column to use as the filter criteria. Click **Show available fields** to display all of the possible filter names.

Filter Criteria

Item	Description
Operator	Select the operator to use in this filter. The available operators are ◆ = (Equal). ◆ <> (Not Equal) ◆ > (Greater Than) ◆ < (Less Than) ◆ >= (Greater or equal to) ◆ <= (Less or Equal to) ◆ $ (Contains) ◆ NOT$ (Not Contains)
Value	Type the value that you want to filter on. For example, if you want to filter on all files that are larger than 1024 KB, select SizeAllocatedKB in the **Field** Name field, select = (Equal) in the **Operator** field, and type 1024 in the **Value** field.
Add	After you selected filter choices, click this button to add them to the **Filter Syntax** field.
Show advanced fields	Select this check box to display all of the possible filter names.
AND	Select this button to combine two sets of filter criteria. Both sets must be true for the result to be true.
OR	Select this button to combine two sets of filter criteria. Either set must be true for the result to be true.
Filter Syntax	Displays the result of the filter choices you made. Or you can type filter choices directly into this field.

Setting Display Field Options for Report Queries

The **Display Field** option defines the columns that will appear in a report. The order of the columns is determined by the order of the fields in the **Selected Fields** list, with the top field appearing on the left column.

Here is how to perform some common tasks:

- To add a field to the **Selected Fields** column, select the field name in the **Fields** column and click the  button.
- To delete a field from the **Selected Fields** column, select the field name to delete from the list and click the  button.
- To change the order in the **Selected Fields** column, select the field name to move and use the up and down arrow buttons.

Some of the numeric fields in the **Fields** and **Selected Fields** columns are dynamic and some are static. If a field is *dynamic* (for example, SizeAllocated) the output in the report will be affected by the value specified in the **Show sizes in** field on a report's **Format** property tab. If a field is *static* (for example, SizeAllocatedGB, SizeAllocatedKB, or SizeAllocatedMB), the output in the report is not affected by the value specified in the **Show sizes in** field.

To illustrate:

- You select the dynamic field **HighWater** to be included in a report query. On the report's **Format** tab you select "Gigabytes" in the **Show sizes in** field. When the report runs, the highwater mark is shown in gigabytes because that is what you selected in **Show sizes in**.
- You select the static field TotalSizeDeviceMB to be included in a report query. On the report's **Format** tab you select "Gigabytes" in the **Show sizes in** field. When the report runs, the total size of the device is shown in megabytes because TotalSizeDeviceMB is a static field, and the value selected in **Show sizes in** does not affect the output.

If the data source for the report query is active file system, the dynamic fields are:

- Allocation Size
- CompressedSize
- DupsWastedSpace
- EndofFileByte
- HighWater
- LargestExtent
- OverDraft
- SizeAllocated

- SizeUsed
- SizeWasted
- SmallestExtent
- SpaceAllocationFree
- SpaceAllocationUsed
- SpaceLimit
- TotalSizeDevice
- TotalUsedDevice
- ValidDataLength

If the data source for the report query is a space allocation resource, the dynamic fields are: HighWater, OverDraft, SizeUsed, SpaceAllocationFree, and SpaceLimit.

If the data source for the report query is space allocation history, the dynamic fields are: HighWater, OverDraft, SpaceLimit, and SpaceUsed.

Related Topics:

- "Viewing and Changing Report Query Properties" on page 107

Setting Report Break and Sort Options for Report Queries

The Report Break property allows you to define a summary break in the report. A summary break is associated with a sort column. A break occurs whenever the value changes from one row to the next in the associated sort column or any other major sort column. You can define totalling actions for a summary break.

The Report Break property controls subtotaling in the report. Subtotaling is associated with the sort. A report break associated with a sort column will cause subtotals to occur whenever the value changes in that column or any other major sort column. After the report break is associated with a sort column, defining the report totals is similar to defining final totals. The difference is that the totals are calculated for the group of rows in the report break, not for all the rows.

For example: If a report is sorted on file owner and directory, you might want to show total usage for each directory within each file owner. You would associate the report break with the directory sort and define your totals there. This would give you the totals for every directory by the file owner. You may create a summary report of just report breaks by not defining the detail line. As a result, only the report breaks are printed.

Here is how to perform some common tasks:

- To add a field to the **Selected Fields** column, select the field name in the **Fields** column and click the  button.
- To delete a field from the **Selected Fields** column, select the field name to delete from the list and click the  button.
- To change the order in the **Selected Fields** column, select the field name to move and use the up and down arrow buttons.
- To change the sort order for a column or to select a column for the report break, select that column from the **Selected fields** option, and then click **Field options**. Select **Ascending** or **Descending** to determine the order of the items in the column. Select **Choose for Report Break** to select this column for the report break.

The Sort property defines the order of the rows in a report. Sort is defined by the order of the data elements specified as sort keys. For example:

- If a report is sorted on File Name, then the rows of the report will be in alphabetical order by the File Name.
- If a report is sorted in Date Created descending order, then the rows will show in the newest to the oldest order.

If you sort on more than one column, then the first sort column will control the overall order of the report and the subsequent sort columns will be defined in the order within the overall or major order. For example:

- If a report is sorted on Date Created and then File Name, the overall report will be displayed in Date Created order.
- If two or more rows have the same creation date, then within that date they will be displayed in File Name order.

Related Topics:

- "Viewing and Changing Report Query Properties" on page 107
- "Setting Report Break and Sort Options for Report Queries" on page 112
- "Setting Summary Sort Options for Report Queries" on page 116

Setting Total Options for Report Queries

The Total property controls the totals displayed at the end of the report. These totals are for all the values in the column you are totalling. The order of the Total columns is determined by the order of the fields in the **Selected Fields** list with the top field appearing in the left column.

Here is how to perform some common tasks:

- To add a field to the **Selected Fields** column, select the field name in the **Fields** column and click the  button.
- To delete a field from the **Selected Fields** column, select the field name to delete from the list and click the  button.
- To change the order in the **Selected Fields** column, select the field name to move and use the up and down arrow buttons.
- To set the way a field's values are totalled, select the field in the **Selected fields** option, and then click the **Field options** button. The table below summarizes the totalling properties.

Action Properties

Action	Description
Sum	Displays the sum of all the values in the column.
Max	Displays the largest value in the column.
Min	Displays the smallest value in the column.
Average	Displays the average value in the column.
Store	Displays the last row's value in the column.

Related Topics:

- "Viewing and Changing Report Query Properties" on page 107
- "Setting Summary Total Options for Report Queries" on page 117

Setting Summary Filter Options for Report Queries

The Summary Filter option enables you to specify the file criteria to use during summarization of a report. You may type the filter criteria directly into the **Filter Syntax** field or select the filter components. Use the following field selectors to define the filter criteria:

Summary Filter Options

Item	Description
Field name	Select the name of the column to use as the filter criteria. Click **Show available fields** to display all of the possible filter names.
Operator	Select the operator to use in this filter. The available operators are ◆ = (Equal) ◆ <> (Not Equal) ◆ > (Greater Than) ◆ < (Less Than) ◆ >= (Greater or equal to) ◆ <= (Less or Equal to) ◆ $ (Contains) ◆ NOT$ (Not Contains)
Value	Type the value that you want to filter on. For example, if you want to filter on all files that are larger than 1024 KB, select SizeAllocatedKB in the **Field** Name field, select = (Equal) in the **Operator** field, and type 1024 in the **Value** field.
Add	After you selected filter choices, click this button to add them to the **Filter Syntax** field.
Show advanced fields	Select this check box to display all of the possible filter names.
AND	Select this button to combine two sets of filter criteria. Both sets must be true for the result to be true.
OR	Select this button to combine two sets of filter criteria. Either set must be true for the result to be true.
Filter Syntax	Displays the result of the filter choices you made. Or you can type filter choices directly into this field.

Related Topics:

- "Viewing and Changing Report Query Properties" on page 107
- "Setting Filter Criteria for Report Queries" on page 109

Setting Summary Sort Options for Report Queries

The Summary Sort property defines the order of the columns to sort on for summarization in a custom report. Like Sort, Summary Sort is defined by the order of the data elements specified as sort keys. For example:

- If a report is sorted on File Name, then the rows of the report will be in alphabetical order by the File Name.
- If a report is sorted in Date Created descending order, then the rows will show in the newest to the oldest order.

If you sort on more than one column, then the first sort column will control the overall order of the report and the subsequent sort columns will be defined in the order within the overall or major order. For example:

- If a report is sorted on Date Created and then File Name, the overall report will be displayed in Date Created order.
- If two or more rows have the same creation date, then within that date they will be displayed in File Name order.

Here is how to perform some common tasks:

- To add a field to the **Selected Fields** column, select the field name in the **Fields** column and click the  button.
- To delete a field from the **Selected Fields** column, select the field name to delete from the list and click the  button.
- To change the order in the **Selected Fields** column, select the field name to move and use the up and down arrow buttons.

A summary sort may be in ascending or descending order. To change a sort's direction, select the field in the **Selected fields** option, and then click the **Field options** button.

Related Topics:

- "Viewing and Changing Report Query Properties" on page 107
- "Setting Report Break and Sort Options for Report Queries" on page 112

Setting Summary Total Options for Report Queries

A summary may be created instead of a detailed report. Use the Summary Total property to select the columns to summarize on at the end of the custom report. These summary totals are for all the values in the column you are totalling. The order of the Summary Total columns is determined by the order of the fields in the **Selected Fields** list with the top field appearing in the left column.

Here is how to perform some common tasks:

- To add a field to the **Selected Fields** column, select the field name in the **Fields** column and click the  button.
- To delete a field from the **Selected Fields** column, select the field name to delete from the list and click the  button.
- To change the order in the **Selected Fields** column, select the field name to move and use the up and down arrow buttons.
- To set the way a field's values are totalled, select the field in the **Selected fields** option, and then click the **Field options** button. The table below summarizes the totalling properties.

Field Summary Total Properties

Action	Description
Sum	Displays the sum of all the values in the column.
Max	Displays the largest value in the column.
Min	Displays the smallest value in the column.
Average	Displays the average value in the column.
Store	Displays the last row's value in the column.

Related Topics:

- "Viewing and Changing Report Query Properties" on page 107
- "Setting Total Options for Report Queries" on page 114

Setting Graph Options for Report Queries

The Graph property enables you to define a graph to include in the report. You may select the type of graph to display: pie, bar, or plot. (The plot graph option is available only for trending reports.) Graph settings determine the data to be used for the X- and Y axis, as well as the line break. The graph settings are described below.

Item	Description
Graph Disabled	To include a graph in the report, select the type of graph from the drop-down list.
Graph Settings	
X axis	Select the files you want to use as the X axis in the graph.
X axis label	Select the label to display for the x axis.
Y axis	Select the field that you want to use as the Y axis in the graph.
Line Break	Select the field that you want to use for the line break in the graph. The line break determines which Y axis option is used to constitute a new line. If FileName is used, then Storage Exec draws one line for each file name. Only the first line has regression analysis performed on it. For example: Y axis = Space Used, and line break = File name. This shows the space used for each file at each TimeStamp.
Regression Line	Select this option to display a regression line in the graph depicting the trend as an ascending or descending line. This line is used to forecast future usage based on historical analysis.

Deleting a Report Query

▼ **To delete a report query:**

1. On the management pane, click **Report Queries**.
2. On the details pane, right-click the report query to delete and choose **Delete**.
3. A message displays prompting for confirmation. Click **Yes** to delete the report query.

Related Topics:

- "Introduction to Report Queries" on page 103

Copying a Report Query

You must be running the Storage Exec Advanced Reporting Option to copy and paste a report query.

▼ **To copy a report query:**

1. On the management pane, click **Report Queries**.
2. On the details pane, right-click the report query you want to copy, and choose **Copy**.
3. Right-click in the details pane and choose **Paste**. A new report query, named "Copy of *report-query-you-selected*," displays in the list.
4. Rename the new report query by right-clicking it and choosing **Rename**, entering the new name in the text field, and pressing ENTER.
5. Change the properties of the new report query as appropriate as described in the section "Viewing and Changing Report Query Properties" on page 107.

Related Topics:

- "Introduction to Report Queries" on page 103

Renaming a Report Query

▼ **To rename a report query:**

1. On the management pane, click **Report Queries**.
2. On the details pane, right-click the report query you want to rename, and click **Rename**.
3. Enter the new name in the text field and press ENTER.

Related Topics:

- "Introduction to Report Queries" on page 103

Reports 9

This chapter contains the following sections:

Introduction to Reports

Reports provide an overview of disk consumption as well as information required to manage space effectively. Reports can provide a wealth of information to help identify inappropriate file types being stored on corporate resources, identify file types and applications being stored on non-designated servers or partitions, and identify files not being included in the backup policies.

You can create reports in five different formats:

- HTML. Provides the report details in a traditional browser format.
- Active HTML. Provides the report details in a spreadsheet style in Microsoft Internet Explorer.

  Note On Windows NT computers, you cannot drill down on Active HTML reports.

- Text. Provides the report details in a text file.
- Excel. Provides the report details in a Microsoft Excel spreadsheet.
- TSV. Provides the report details in a Microsoft Excel spreadsheet in a tab separated values file format. Each line represents one entry. In every line, each field is separated by a tab character.

The content and appearance of reports are determined by report queries. When you create a new report, you select the report queries that you want to associate with the report. For existing reports, you can change the report queries with which the reports are associated. Storage Exec is shipped with default report queries. If you have purchased and installed the Storage Exec Advanced Reporting Option, you can create custom report queries.

Introduction to the Storage Exec Advanced Reporting Option

The Storage Exec Advanced Reporting Option is an add-on option. You must be running the Storage Exec Advanced Reporting Option if you want to:

- Have access to the expanded list of predefined reports (see "Predefined Reports" on page 133).
- Create a report query (see "Creating a Report Query" on page 104).

Creating a New Report

Before you create a new report, you should be familiar with the types of report queries that are available. Report queries define the content and appearance of reports.

▼ **To create a new report:**

1. On the management pane, right-click **Reports**. Point to **New**, and then click **Report**.

   or

   On the details pane, right-click, click **New**, and then click **Report**.

2. When the Welcome screen displays, click **Next**.

3. On the **Report Name and Description** dialog box, enter the name and description of the report you are creating. Click **Next**.

Note Do not use these characters in the report name: + # = ; , " \ / < >

4. On the **Filter** dialog box, define the selection criteria for the report. Select as many of the available options as desired. See the section "Setting Filter Properties for a Report" on page 124 for additional information. Click **Next**.

5. On the **Format** dialog box, select output formatting for the report. This includes the report format and how to display the sizes. See the section "Setting Format Properties for a Report" on page 126 for additional information. Click **Next**.

6. On the **Save and Email Settings** dialog box, specify where the report should be saved and optionally where to email the report. See the section "Setting Save and Email Properties for a Report" on page 128 for additional information. Click **Next**.

7. On the **Content** dialog box, select the report queries to include in the report. Multiple report queries can be selected.

8. The **Completing the Report Wizard** dialog box displays. If you want to run the report now, select **Run report now**, and then click **Finish**. If you want to create the report now, but do not want to run it now, click **Finish**.

Related Topics:

- "Introduction to Report Queries" on page 103
- "Introduction to Reports" on page 121
- "Running a Report" on page 129

Viewing and Modifying Report Properties

To view or modify report properties:

1. On the management pane, highlight **Reports**.

2. On the details pane, right-click a report, and choose **Properties**.

3. To change the description of the report, on the **Description** tab, type a new description.

4. To change the filter criteria, select the **Filter** tab, and then see "Setting Filter Properties for a Report" on page 124.

5. To change the format in which the report will display, select the **Format** tab, and then see "Setting Format Properties for a Report" on page 126.

6. To change the location where the report is saved or the person who receives the report via email, select the **Save and Email Settings** tab, and then see "Setting Save and Email Properties for a Report" on page 128.

7. To change the report queries that are associated with this report, select the **Content** tab, and then select the check boxes for any report queries you want to add to this report, or clear the check boxes for report queries you want to remove from this report.

8. Click **OK**.

Related Topics:

- "Introduction to Reports" on page 121
- "Running a Report" on page 129
- "Creating a New File Group" on page 98

Setting Filter Properties for a Report

You can control the type of information that displays on reports by setting filters. You can filter based on the name or path of a file, by file group, or by user. You can limit the number of records to display on reports. In addition, you can select up to six types of file attributes, such as read only or hidden, on which to filter.

Filter Properties

Item	Description
File Filters	
By name	Choose this option to specify which files are included in the report. You can filter by path name or by file name. Use semicolons to enter multiple file selections. Examples: ◆ Enter **`*.exe; *.dll`** to select all the files with an .exe or .dll extension. ◆ Enter **`c:\Marketing\*`** to select all the files in the Marketing directory. ◆ Enter **`c:\Marketing\*.exe`** to select all the files in the Marketing directory with an .exe extension.
By file group	Choose this option to filter by predefined file groups.
By user	Choose this to filter files by the name of the file owner. For example, **`Admin*`** includes all files whose owner's name begins with *Admin*.
Report length	

Filter Properties (continued)

Item	Description
Number of records to display	Type the number of records to include in the report. By default all the records will be included in the report. You must clear the **Display all records** check box before you can type a number. For example, a **Number of records to display** of 50 would include the first 50 records.
Display all records	This check box is selected by default to display all records that match the filter criteria. If you want to display only a certain number of records, clear this check box, and then type the number of records to display in the **Numer of records to display** field.
File attributes	Files may be selected based on six standard file attributes.: ◆ Read Only: The file is read-only. ◆ Hidden: The file is hidden. ◆ System: The file is a system file. ◆ Compressed: The file is compressed. ◆ Archive: The file has been changed and not backed up. ◆ Directory: The file is a directory. Dark check—Select if the attribute is present Blank—Select if the attribute is absent

Setting Format Properties for a Report

Reports can be created in several different formats.

Format Properties

Item	Description
HTML	Presents the report in a traditional browser, which does not require any special controls. Files have a file name extension of .htm. File management capabilities are not available with this format.
Active HTML	Report output is in a spreadsheet-style and is displayed in Microsoft Internet Explorer. Files have a file name extension of .htm. This style provides for sorting and limited file management, such as copy, move, and delete. In addition, a file launch feature, which will launch a file based on file associations, is available. This functionality requires that the ActiveX controls are loaded on the client computer that is viewing the report. If the Active X control is not installed, you will be prompted to install it.
Text	Report output is in the text format (txt).
Excel	Report output is in Microsoft Excel format (that is, with a file name extension of .xls).
TSV	Report output is in a tab-separated values format, which can be imported into most spreadsheets or database applications.
Show sizes in	You can specify the size units in the report as bytes, kilobytes, megabytes, or gigabytes.

Format Properties (continued)

Item	Description
Batch command	Enter a command from which a batch file will be created. The batch command may be entered either when creating a new report or when modifying the existing report properties. After the report runs, the batch file is created. To execute the commands, you must run the batch file. For example, if users want to delete all of their .jpg files, they should enter the `del "#"` command. The report will produce a set of commands similar to these: Del /y graphic1.jpg Del /y graphic2.jpg Del /y graphic3.jpg The batch file has the same file name as the generated report except that it has an extension of BAT. The batch file is stored in one of several locations. • By default, it is stored in the Storage Exec `\Reports` folder. • If you specify a value in the **Report Output Folder** field of the global properties **Reports** tab (described in the section "Setting Report Properties" on page 40), the value takes precedence over the default. • If you specify a value in the **Save the report to the following folder** field in the **Save and Email Settings** tab, the value takes precedence over the default and the global destination property value.

Setting Save and Email Properties for a Report

You can set a location where Storage Exec will save report output. In addition, you can enter an email address for a person who should receive the report output.

Save and Email Properties

Item	Description
Save the report to the following directory	Enter the name of the file where the report output will be written. You may specify the value in one of several formats: ◆ Directory and file name (for example, C:\Reports\Duplicates.htm) ◆ File name only (for example, Duplicates.htm): Because no folder was specified, Storage Exec places the report in the folder specified in the **Report output folder** field on the **Reports** tab of the global Properties dialog box. ◆ Directory path only (for example, C:\Reports): Because no file name was specified, Storage Exec places the report in the directory you specified and names the report output *report-name_computer_timestamp*, where *computer* is the name of the computer where the report was run and *timestamp* is in the format hours, minutes, seconds, and milliseconds in GMT time. If you specify a directory, the directory must already exist; Storage Exec will not create it dynamically. If you specify a file name extension that Storage Exec does not support, the report will be produced in the format you specified on the **Format** tab. Batch files created by entering a value in the **Batch Command** field (on the Format dialog box) are also saved to the folder specified in **Save the report to the following directory**. If you specify a value in the **Save the report to the following directory** field, the value takes precedence over the value in the **Report output folder** field of the global properties **Reports** tab (described in the section "Setting Report Properties" on page 40).
Mail the report to the following email address	Enter the default email address where the report will be sent. This value will be superseded by the following: ◆ The email address provided in the **Mail To** field on alarm **Report** tabs. ◆ The email address provided in the **Mail To** field when the user schedules a batch report from the administration console. For more information, read "Running a Report on a Schedule" on page 131.

Choosing the Contents of a Report

Use the **Content** tab to modify the content of the report. Select the report queries to include in the report.

Related Topics:

- "Introduction to Report Queries" on page 103

Running a Report

You can run reports in one of two ways:

- Interactively. When a report is run interactively, the report generates after you submit it. For instructions on running a report interactively, see "Running a Report Interactively" on page 129.
- On a schedule (in batch). When a report is run in batch, it is scheduled to run on a specific date and at a specific time. You can set batch reports to run one time or to run on a recurring basis. For instructions on scheduling a report, see "Running a Report on a Schedule" on page 131.

Running a Report Interactively

Follow these instructions to run a report interactively:

1. On the management pane, click **Reports**.

   Storage Exec lists the existing report on the details pane.

2. On the details pane, double-click the report you want to run.

   The Run Report dialog box displays.

3. Verify that the **Run interactively** option is selected.

4. If you want to use a different computer to run the report, change the value in the **Server** field.

   You might want to use a different computer if you expect the report to return a large number of files. This might happen if you are running a single report against multiple managed resources. In a case like this, the collection process may take a lot of memory and you may want to distribute the load.

5. Click the **...** button to the right of the **Resource(s)** box; the **Select Folder** dialog box displays. Select the computer, drive, folder, or sub-folder against which you want to run the report. You may select more than one. Click **OK** when you finish.

6. Click **Submit**.

   The report begins running.

   When the report finishes, the output displays on your screen in the format specified on the **Format** tab (described in section "Setting Format Properties for a Report" on page 126) of the report's properties.

   Output is also sent to one of several locations.

   - By default, it goes to the Storage Exec `\Reports` folder.
   - If you specify a value in the **Report Output Folder** field of the **Reports** tab (described in the section "Setting Report Properties" on page 40) of the global properties, the value takes precedence over the default.
   - If you specify a value in the **Save the report to the following folder** field of the **Output** tab of the report's properties dialog box, the value takes precedence over the default and the global destination property value.

After examining the report on your screen, you may do one or more of the following:

- Print it. If the report is in Active HTML format, you must print using the report's **Print this report** link, which is located below the report title. If you use the browser's **Print** button or the **Print** menu option, you may receive unexpected results.
- Back up the data from the report, if you have Backup Exec for Windows Servers installed. For more information, see "Integration with Backup Exec" on page 139.
- Save it to a hard drive for future examination. Storage Exec automatically saves the report for you in a file; this name displays in the **Report Status** field of the **Run Report** dialog box and in the web browser's **Address** field.
- Send it to another user. From the **File**, menu, click **Send**, and then click **Page by E-mail** from the web browser's menu.
- Take action directly from the report if it permits. For example, some reports enable you to run another report to get additional details; this is called *drilling down*. Other reports enable you to open, delete, and move individual files.

Note You are unable to drill down if you are running Storage Exec under Windows NT.

Running a Report on a Schedule

Use batch reports when you want to run a report at a specific time, either once or on a recurring basis.

If a scheduled report does not run, do one of the following:

- If the report is scheduled to run on a remote server, verify that the Windows Task Scheduler account on that server has access to your computer. Give access if there is none.
- Check the `\Program Files\Veritas\Storage Exec\bin\StorageReports.log` file for errors.
- View the Windows Task Scheduler log. The log will indicate if the job was submitted and ran successfully.

1. On the management pane, click **Reports**.

   Storage Exec lists the existing reports on the details pane.

2. On the details pane, double-click the report you want to run.

   The Run Report dialog box displays.

3. Select **Schedule report**.

4. On the **Schedule Reports Date and Time** dialog box, complete the fields that display as follows, and then click **Next**:.

Item	Description
Schedule interval	Select when you want to run the report. Your choices are: Today, Tomorrow, Every, and Next.
Time of day	Select the time of day to run the report.
Days of week	To run the report on a specific day of the week, select the day.
Days of month	To run the report on a specific day of the month, select the day.
Mail	Click this button to mail the report information to someone when the report completes. On the **Mail Configuration** dialog box, enter the email address of the person who should receive the email and enter a subject line for the email, and then click **OK**.

5. If you want to use a different computer to run the report, change the value in the **Server** field.

   You might want to use a different computer if you expect the report to return a large number of files. This might happen if you are running a single report against multiple managed resources. In a case like this, the collection process may take a lot of memory and you may want to distribute the load.

6. Click the **...** button to the right of the **Resource(s)** box; the **Select Folder** dialog box displays. Select the computer, drive, folder, or sub-folder against which you want to run the report. You may select more than one. Click **OK** when you finish.

7. Click **Submit**.

   Storage Exec schedules the report and adds the report information to the Scheduled Reports details pane.

   When the report finishes, the output displays on your screen in the format specified on the **Format** tab (described in section "Setting Format Properties for a Report" on page 126) of the report's properties.

   Output is also sent to one of several locations.

   - By default, it goes to the Storage Exec `\Reports` folder.
   - If you specify a value in the **Report Output Folder** field of the **Reports** tab (described in the section "Setting Report Properties" on page 40) of the global properties, the value takes precedence over the default.
   - If you specify a value in the **Save the report to the following folder** field of the **Output** tab of the report's properties dialog box, the value takes precedence over the default and the global destination property value.

Viewing and Modifying Scheduled (Batch) Reports

After you schedule a report to run, you can view or modify the schedule and the settings for it.

Note You cannot modify a scheduled report if you are using Microsoft Windows 2003 or Windows XP.

▼ **To view and modify scheduled reports:**

1. On the management pane, select **Scheduled Reports**. On the details pane, right-click the scheduled report you want to view or modify.

Predefined Reports

This section lists and describes the reports that come pre-packaged with Storage Exec. Some of the reports come with the Storage Exec Server, while others require the Storage Exec Advanced Reporting Option (ARO).

Predefined Reports

Report	Description	Comes with Storage Exec Server	Comes with ARO
Best Practices	Provides a representation of storage management best practices that is a good starting point for disk space analysis. The Best Practices Report gives an overall indication of your system's disk health. This report identifies files by type, duplicate files, large scale files, files not being backed up, most commonly used files, and nightly backup requirements. This report contains drill-down capabilities so you may access file detail.		X
Chargeback Summary	Allows you to view the files by any property contained within the user profile in the Active Directory and assigns a dollar value to the storage used by those files.		X

Predefined Reports (continued)

Report	Description	Comes with Storage Exec Server	Comes with ARO
Daily Storage	Provides daily storage usage details for the managed resource.		X
Disk Drive Summary	Lists all partitions and their capacity, free space, and type. You may drill into the partition for more detailed information.	X	X
Duplicate Files	Identifies duplicate files that may use an excessive amount of space. This information is useful for cleaning up disk space quickly.	X	X
File Type Summary	Provides usage details for the disk profile. Drill down into category details by double-clicking a category in the pie chart or from the report table. In addition, files are sorted by file groups, and the size of each file group is calculated.	X	X
Files Created This Month	Identifies files based on when the file was created. This is useful for determining environment changes that may have caused system or disk capacity problems.		X
Files Not Accessed in Over One Year Summary	Identifies files that have not been accessed in over one year.	X	X
Files Not Being Backed Up	Identifies files that have been modified but have not been backed up according to the NTFS archive bit. This bit is used by backup applications to indicate a file's backup status.		X
Files To Remove	Identifies various temporary file types that can be removed from the system.		X
Graphic Files	Displays all the graphics files contained in the resource. This is useful for locating graphic files by name or type.	X	X

Predefined Reports (continued)

Report	Description	Comes with Storage Exec Server	Comes with ARO
Insecure Files	Displays "at risk" files. Files that any user account can access are considered to be "at risk" files.		X
Internet Files	Displays all the files contained in the managed resource with extensions *.htm, *.html, *.url, and *@*.		X
Large Duplicate Files	Selects large files that contain duplicate copies within the passed directory path. Files that have a close name match and the same size can be considered duplicates. A close match is done by comparing the number of letters in the file name that are the same, starting with the left-most letter and proceeding right. Optionally, the files may be compared before being counted as a duplicate.		X
Large Files	Identifies large files based on the file's size. This is useful for locating and recovering disk space quickly.	X	X
Large Folder Resource Summary	Identifies folder resources larger than 2 MB. This information is useful to quickly locate large folder resources.		X
Large Users Summary	Identifies space by user. This information is useful to track space usage by a user identifier.		X
Media Files	Displays all the media files contained in the resource. This is useful for locating media files by name or type.		X
Microsoft Office Files	Displays all Microsoft Office files contained in the resource. This is useful for locating Microsoft Office files by name or type.		X

Predefined Reports (continued)

Report	Description	Comes with Storage Exec Server	Comes with ARO
Most Commonly Used Files	Presents the amount of raw capacity accessed each day. This is useful for balancing applications, data, and users across available resources and to prevent under-used or over-burdened file servers.		X
New Files	Identifies files created today. This is useful for determining environment changes that may have caused system or disk capacity problems.	X	X
Pinpoint Security Problems	This report is for advanced users who understand file security. This report identifies files that contain undefined Access Control Entries (ACEs) within an Access Control List (ACL) and also identifies files that have an undefined owner. Undefined ACEs impact file system performance as well as system security integrity, whereas files that have an undefined owner are useful to pinpoint potential security breaches, orphaned files, and to ensure files are owned by the proper user.		X
Space Allocation Summary	Identifies all of the space limits defined on the server.	X	X
Space Allocation Trend Summary	Reads the trending database (`SCTrend.mdb`) and reports about the space allocation resources, space used by them, their space limit, the owner, and other information.		X
Space By Folder Resource Summary	Identifies all the folder resources in the managed resource to the depth specified in the report content property. This information is useful to quickly identify large folder resources and folder resource trees.	X	X

Predefined Reports (continued)

Report	Description	Comes with Storage Exec Server	Comes with ARO
Space By Group Summary	Identifies space by file group. This information is useful to track space usage by group identifier.		X
Space By User Summary	Displays the utilization by each user in the domain for the selected path.	X	X
Weekly Storage	Provides weekly storage usage details for the managed resource.		X

Related Topics:

- "Introduction to Reports" on page 121

Best Practices for Reports

These best practices help you get the most out of the Storage Exec reporting feature.

- Use predefined reports. Using predefined reports enables you to begin examining your storage immediately and answer questions like "Do I have duplicate files?" and "How much space is each user using?"
- Create your own report queries and reports. Because each organization has unique needs, it is important to determine what these are and configure custom reports that provide custom answers. Additionally, the reports may need to be distributed or presented in a different fashion to different administrators, managers, and users. Determine what reports your organization requires, who needs to view those reports, and in what format the reports should be presented. Then create your own report queries and reports using a custom report writer or adjust the parameters of the default ones.

Integration with Backup Exec 10

This chapter contains the following sections:

How Storage Exec and Backup Exec for Windows Servers Work Together

VERITAS Backup Exec™ SmartLink technology integrates Backup Exec with other VERITAS solutions. With Backup Exec SmartLink, you can manage and view jobs created by VERITAS Storage Exec™.

When you view a Storage Exec HTML or an Active HTML report on a computer where both Storage Exec and Backup Exec for Windows Servers are installed, Storage Exec seemlessly integrates with the Backup Exec media server, enabling you to quickly and easily back up or archive the data referenced in a Storage Exec report.

To guide you through the backup or archive process, Storage Exec provides an easy-to-use wizard called *Back Up With Backup Exec Wizard*. This wizard guides you through the process of submitting a full backup or archive job to the Backup Exec media server.

Using the full backup selection, all selected report data is backed up to a media server using Backup Exec. After the job finishes, the data remains on the server.

Using the archive selection, all selected report data is backed up and verified. After the verification process finishes, the data is then deleted from the server.

All backup jobs submitted to Backup Exec through a Storage Exec report are processed completely by Backup Exec. As such, Backup Exec is used to restore any Storage Exec data using the media server where the original backup or archive jobs occurred.

Related Topics:

- "Requirements for Running the Back Up With Backup Exec Wizard" on page 140
- "Understanding the Back Up With Backup Exec Wizard" on page 141

Requirements for Running the Back Up With Backup Exec Wizard

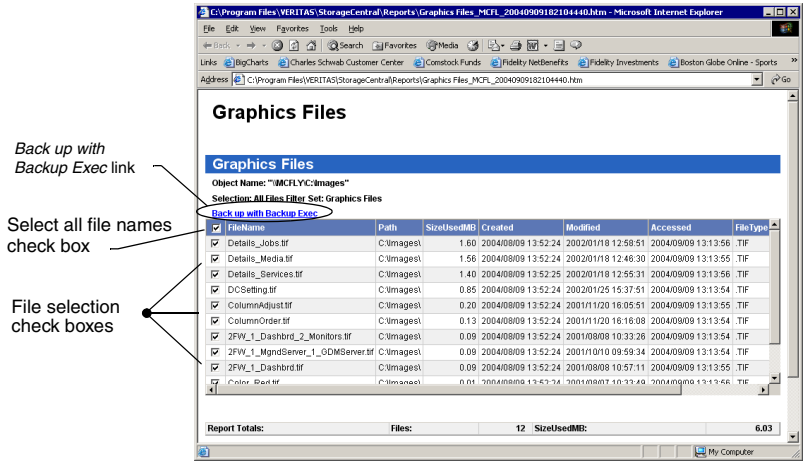
The following requirements must be in place before you can back up or archive report objects with Backup Exec for Windows Servers:

- A Backup Exec for Windows Servers 9.1 or higher media server must be installed and configured on your network.
- To back up or archive data referenced in a Storage Exec Active HTML report on a Windows computer where Storage Exec is not installed, the computer must be connected to the internet.
- The report data must contain both File and Path columns.
- The report must be generated using Storage Exec 5.3.
- The login credentials used to view the report must have access to the local Backup Exec media server.

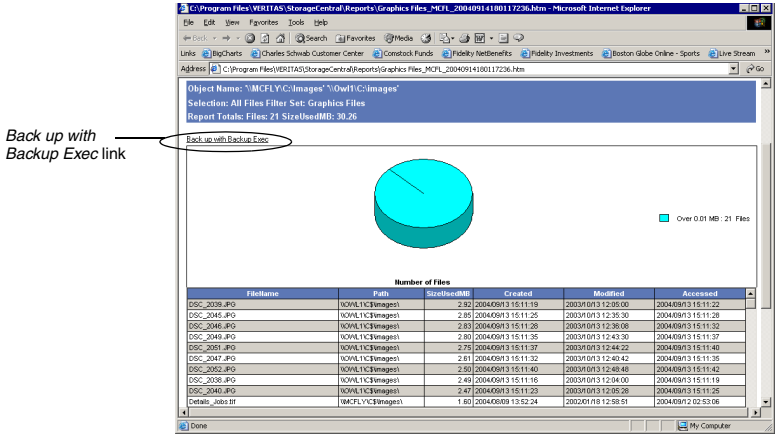
Understanding the Back Up With Backup Exec Wizard

After running a Storage Exec report, you can back up or archive report resources that appear using the **Back up with Backup Exec** link provided. This link, which appears on the left side of each report, launches the *Back Up With Backup Exec Wizard*. The wizard guides you through the process of creating a Backup Exec selection list based on the data referenced in the report. After building a selection list, you are prompted to configure general backup job settings such as naming the job, choosing a local or remote Backup Exec media server to run the job, and selecting the backup job type (Full backup, or Archive). After reviewing the job configuration details, you submit the job for processing with Backup Exec by exiting the wizard. After exiting the wizard, a wizard dialog box appears stating that the job was successfully submitted to Backup Exec. To monitor the job while processing occurs, you can view the job in the Backup Exec Job Monitor.

Back up with Backup Exec link in a StorageCentral HTML report



Back up with Backup Exec link in a StorageCentral Active HTML report



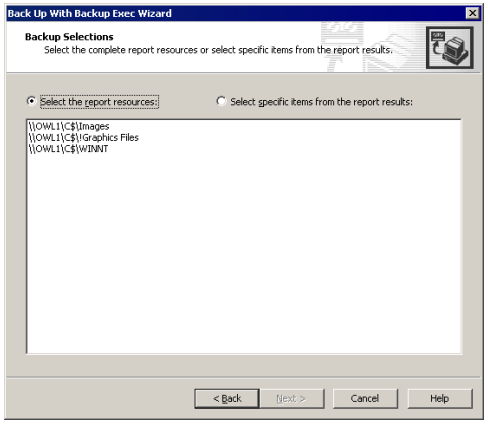
Selecting Data by Report Resources or Report Results

The Back Up With Backup Exec Wizard enables you to make data selections by *report resources* or by *report results*.

Selecting by Report Resources

When selecting data by report resources, the wizard displays the resources by the server name, volume letter and folder name where the resources reside.

Selecting data by report resources



When multiple report resources appear in the Backup Selections screen, you can individually select resources by pressing CTRL and clicking the resources that you want to include in a backup job. To select all report resources, right-click anywhere on the Backup Selections screen and click **Select All**.

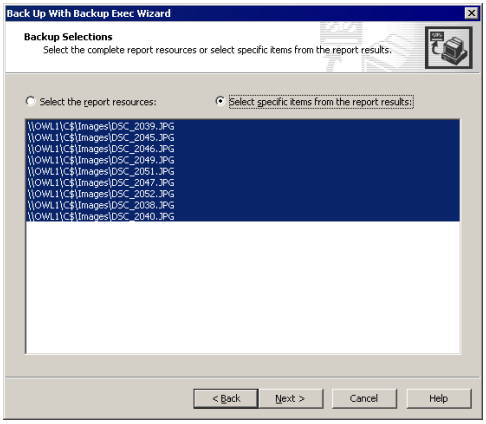
Selecting a report resource automatically includes all files contained within the resource. You can exclude individual file selections from a report object. Press CTRL and click the files you want to exclude when prompted. You can also exclude a file or a set of files by manually entering file names in the field provided at the bottom of the Backup Selections screen.

Note When entering a file names manually, the wildcard characters (?) and (*) can be used in the place of single or multiple characters.

Selecting by Report Results

When selecting data by *report results*, the wizard displays the resources using a format that includes not only the server name, volume letter and folder name where the resource resides, but it also displays the actual file names of the resources themselves.

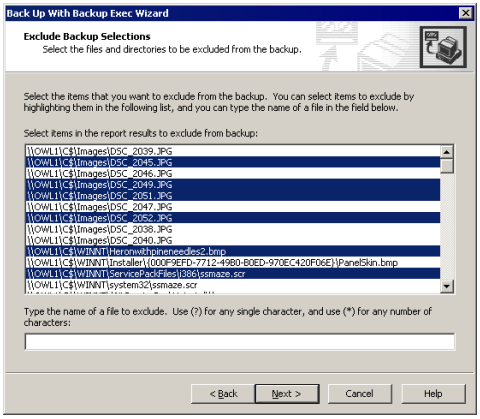
Selecting data from report results



When selecting data using this option, all file names contained in the report result are selected for backup, by default.

You can exclude individual file selections from a report result set when you are prompted by the wizard to select the files you want to back up or archive. Press CTRL and click the files you want to exclude.

Excluding file selections from the Backup Selections screen



Related Topics:

- "Requirements for Running the Back Up With Backup Exec Wizard" on page 140
- "Viewing Reports and Running the Back Up With Backup Exec Wizard" on page 142

Viewing Reports and Running the Back Up With Backup Exec Wizard

Before you can run the Back Up With Backup Exec Wizard, you must first run and view a Storage Exec report. Typically, a Storage Exec report is run and viewed at a Storage Exec Server. However, in the case of Storage Exec Active HTML reports, these reports also can be viewed on remote Windows computers. For example, you can email an Active HTML report to a user working on a computer where Storage Exec is not installed.

You can also launch the Back Up With Backup Exec Wizard from reports viewed locally or at remote Windows computers.

When viewing a Storage Exec HTML or Active HTML report on a Backup Exec media server where Storage Exec is installed, the backup job created using the wizard can be submitted to a local or a remote Backup Exec media server. In either case, after the job is submitted, you can monitor its progress using Backup Exec's Job Monitor at the media server where the job is being processed.

When you open an Active HTML report on a Windows computer that does not have Storage Exec installed, the report launches a VERITAS security warning that asks if you want to run an installer that automatically downloads and installs a Storage Exec cab file from a VERITAS FTP site. The cab file contains the components required to view the report and run the Back Up With Backup Exec Wizard. Responding **Yes** to the security warning enables the report to download the required cab file. After the download completes, an install wizard launches, which guides you through the component installation process. After the components are installed, the report can be viewed, and the Back Up With Backup Exec Wizard can be run, just as if you were viewing the report at a local Storage Exec Server.

Note To launch the Back Up With Backup Exec Wizard from a Storage Exec HTML report, the report must be viewed on a Windows computer running Storage Exec. If Backup Exec is installed on the computer, the Back Up With Backup Exec Wizard will direct you to submit the job to the local Backup Exec media server, or to a remote media server for processing.

If Backup Exec is not installed, the wizard will prompt you for the name of a remote Backup Exec media server where the job will be submitted for processing.

▼ To run the Back Up With Backup Exec Wizard from a Storage Exec HTML report:

1. Open a Storage Exec HTML report on a computer where Storage Exec is installed.

2. On the report, click the check boxes preceding the file names you want to back up or archive. To select all files in the report, click the check box preceding the column name **FileName**.

3. Click **Back up with Backup Exec**.

4. On the Welcome screen, click **Next**.

5. On the Backup Selections screen, select the items you want to back up, either by choosing specific items by the report results, or by report resources. By default, the wizard selects the option, **Choose specific items from the report results** and highlights all listed files.

   You can exclude files on the Backup Selections screen by pressing CTRL and then clicking individual file names to be excluded.

   Note If you select **Choose the report resources**, select one or more resources to back up or archive. Click **Next** and then select the files you want to exclude. Continue with step 6.

6. Click **Next**.

7. Select a local or remote Backup Exec media server where you want the job to run. If you select **Remote media server**, enter the media server's name along with valid user logon credentials to the computer.

8. Click **Next**.

9. Review the settings selected for job and then click **Next**.

   Note The default configuration settings that appear in the Review Backup Job Settings screen for Device and Media, and Advanced are set on the Backup Exec media server. To make changes to these options before submitting the job, click Back and then click the option, On hold on the Backup Job Options screen. After placing the job on hold, click Next. On the Review Backup Job Settings screen, click Next. Click Finish to submit the job. In the Backup Exec Job Monitor, right-click the Storage Exec job. Make the desired changes to the Device and Media or Advanced options on these property pages. Click Submit. The Storage Exec job accepts the updated settings and automatically changes the job state to a Run Now job.

10. Click **Finish** to submit the job to Backup Exec for processing.

▼ **To run the Back Up With Backup Exec Wizard from a Storage Exec Active HTML report:**

1. Open a Storage Exec Active HTML report.

   Note If you are viewing an Active HTML report on a remote computer that has an active internet connection, a VERITAS security warning appears asking if you want to run an installer that automatically downloads and installs required Storage Exec components from a VERITAS FTP site. Click **Yes** and then follow the install wizard instructions. For more information, see "Running the Storage Exec Cab File Installation Program on Remote Computers" on page 145.

2. Click **Back up with Backup Exec**.

3. On the Welcome screen, click **Next**.

4. On the Backup Selections screen, select the items you want to back up, either by choosing specific items by the report results, or by report resources. By default, the wizard selects the option, **Choose specific items from the report results** and highlights all listed files.

5. You can exclude files on the Backup Selections screen by pressing CTRL and then clicking individual file names to be excluded.

   Note If you select **Choose the report resources**, select one or more resources to back up or archive. Click **Next** and then select the files you want to exclude. Continue with step 6.

6. Click **Next**.

7. Select a local or remote Backup Exec media server where you want the job to run. If you select **Remote media server**, enter the media server's name along with valid user logon credentials to the computer.

8. Click **Next**.

9. Review the settings selected for job and then click **Next**.

   Note The default configuration settings that appear in the Review Backup Job Settings screen for **Device and Media**, and **Advanced** are set on the Backup Exec media server. To make changes to these options before submitting the job, click **Back** and then click the option, **On hold** on the Backup Job Options screen. After placing the job on hold, click **Next**. On the Review Backup Job Settings screen, click **Next**. Click **Finish** to submit the job. In the Backup Exec Job

Monitor, right-click the Storage Exec job. Make the desired changes to the **Device and Media** or **Advanced** options on these property pages. Click **Submit**. The Storage Exec job accepts the updated settings and automatically changes the job state to a Run Now job.

10. Click **Finish** to submit the job to Backup Exec for processing.

Note To monitor the job, start Backup Exec on the media server where the Storage Exec job is running, and then click **Job Monitor**.

Related Topics:

- "How Storage Exec and Backup Exec for Windows Servers Work Together" on page 139
- "Understanding the Back Up With Backup Exec Wizard" on page 141

Running the Storage Exec Cab File Installation Program on Remote Computers

When you open an Active HTML report on an internet-connected Windows computer that does not have Storage Exec installed, the report launches a VERITAS security warning that asks if you want to download a Storage Exec cab file from a VERITAS FTP site. This cab file contains the components necessary to run the Back up for Backup Exec Wizard.

The following steps guide you through the process of downloading and installing the components from the Storage Exec cab file.

▼ To access the Storage Exec cab file:

1. View a Storage Exec Active HTML report on a Windows network computer that has an active internet connection.

   After a few moments, a VERITAS security warning appears.

2. Click **Yes** to enable the download of the Storage Exec cab file to your computer.

3. Click **Next** on the VERITAS Storage Exec OCX Welcome screen.

4. Click **I accept the terms in the license agreement and then click Next**.

5. Click **Install** to begin the installation.

After the installation finishes, the report contents can be viewed and the Back Up With Backup Exec Wizard can be launched.

Audit Trail 11

This chapter contains these sections:

Introduction to Audit Trail

You can view space allocation and file blocking actions in the Audit Trail details pane. To save and later view space allocation and blocking actions, when creating a managed resource or defining a managed resource policy, select the **Record alarm** option on the **Notification** tab.

To view space allocation and blocking actions, from the management pane, select **Audit Trail**. The table below describes what displays in the details pane.

Audit Trail Data

Field name	Description
Status	Identifies whether the action that caused the alarm to be triggered was Allowed or Denied. Allowed means that the space allocation or file blocking resource was defined as being passive. Denied indicates that the resource was active, or non-passive.
Time	The date and time that the alarm was triggered.
User	The user who performed the file operation that triggered the alarm. The user and domain name are provided.
Object	The drive, partition, folder, or file name that was being monitored by the managed resource.
Server	The Windows server name where the managed resource resides.

Audit Trail Data (continued)

Field name	Description
Message	The message that was triggered by the alarm for the managed resource.
Policy Name	The policy name, assuming the managed resource is associated with a policy. You can create managed resources that have no policy association.
Type	Identifies the type of managed resource. **ALLOC** displays for space allocation resources. **BLOCK** displays for file blocking resources.
File Name	The fully-qualified file name that triggered the alarm action. For example, this is the file that was being updated when the quota was exceeded or a prohibited file type for file blocking.
ID	A sequential number that is assigned to each audit record.

To see the audit records for all computers in the domain, use a centralized Microsoft Access database. For information about the centralized database, read "Storage Exec Database Configuration" on page 30.

You may choose to have Storage Exec store its audit data in Microsoft SQL Server. However, you must first configure Storage Exec to use SQL Server to store this data. For instructions, read the section "Storage Exec Database Configuration" on page 30.

Note The Audit Database is accessed through the ODBC data source. By default, the Administration Console looks only at the local Microsoft Access database even if the UI focus is on another server or another domain.

Related Topics:

- "Deleting an Audit Record" on page 150
- "Refreshing Audit Data" on page 151

Customizing Audit Trail Properties

You can customize the audit trail details pane by:

- Selecting the columns to display.
- Selecting a date range for the audit records to display.
- Selecting records that contain certain user names, policy names, resource names, or file names.

▼ **To customize audit trail properties:"**

1. On the management pane, select **Audit Trail**.
2. On the details pane, right-click on any of the column headings, and then select **Audit Properties**.
3. On the **Columns** tab, select the columns that you want to display or clear the check boxes for the columns you do not want to display.
4. On the **Date** tab, select one of the following to display audit records for certain dates:

Date tab options

Item	Description
All Records	Select this to display all audit records, regardless of the date.
Between x and x	Select this to display all records created between a specific range of dates. Then type the date range in the fields provided.
Before	Select this to display all records created before a specific date, then select the date.
Since	Select this to display all records created after a specific date, then select the date.

5. On the **Custom** tab, enter the names of users, policies, resources, or files that you want to display on the audit details pane:

Custom tab options

Item	Description
User name	To display audit records for a specific user, enter the user's name.
Policy name	To display audit records for a specific policy, enter the policy name.
Object name	To display audit records for a specific managed resource, enter the name of the resource.
File name	To display audit records for a specific file, enter the file name.
Access	To display only audit records for passive resources, select **Denied**. To display only audit records for active resources, select **Allowed**.
Type	To display only space allocation audit records, select **Allocation**. To display only file blocking audit records, select **Blocking**.

Deleting an Audit Record

You can set up Storage Exec to automatically delete audit records after they have been in the audit database for a specific number of days. Or you can manually delete audit records at any time.

▼ **To set up Storage Exec to automatically delete audit records:**

1. On the management pane, right-click **My Computer**, and then select **Properties**.
2. On the **Audit Trail** tab, complete the following fields:
   - In the **Period** field, enter the number of days you want Storage Exec to keep the audit data. Setting a long retention period causes Storage Exec to use more disk space for storing data.
   - To keep audit data indefinitely, select the **Keep infinite data** check box.

▼ **To manually delete an audit record:**

1. On the management pane, select **Audit Trail**.
2. On the details pane, right-click the audit record you want to delete, and then click **Delete**.
3. A message displays prompting for confirmation. Click **Yes** to delete the record.

Refreshing Audit Data

▼ **To refresh audit data:**

1. On the management pane, select **Audit Trail**.
2. Right-click anywhere in the details pane, and click **Refresh** *or* click the refresh icon on the toolbar.

Preferred Computers and Groups 12

This chapter contains the following sections:

Introduction to Preferred Computers and Groups

A *preferred group* is a named logical entity that contains one or more computers. The purpose of creating a preferred group is to group commonly used computers in one place.

Preferred computers can be included in a preferred group or added to the root of the Preferred Computers and Groups node for quick access.

For a preferred group, you can:

- Run a report on all objects in the preferred group
- Delete a preferred group
- Rename a preferred group
- View and modify preferred group properties

For a single preferred computer, you can:

- Start and stop services
- Run a report
- Delete a preferred computer
- View and modify preferred computer properties

Automatically Detecting Storage Exec Servers and Agents

You can set Storage Exec to automatically detect new Storage Exec servers and agents in the same domain. After Storage Exec detects the new servers and agents, it lists them under the **Preferred Computers and Groups** node.

▼ **To automatically detect new Storage Exec servers and agents:**

1. On the management pane, right-click **Preferred Computers and Groups**.
2. Select **Auto Detect Servers and Agents**.
3. Verify that the **Auto detect Servers and Agents when the administrative console starts** check box is selected.
4. Click **Run**.

Creating a New Preferred Group or Computer

You can create a new group in which to add computers, or you can add computers to the root of the **Preferred Computers and Groups** node.

▼ **To create a new preferred group or computer:**

1. On the management pane, right-click **Preferred Computers and Groups**. Point to **New**, and then click **Preferred Computer and Group**.
2. On the **Welcome** screen, click **Next**.
3. On the **Wizard Options** dialog box, select the option for the type of item you want to add, and then click **Next**. If you select **Create a preferred group**, proceed to step 4. If you select **Add preferred computers**, proceed to step 5.

4. On the **Preferred Group Name** dialog box, enter the name and description of the group, and then click **Next**.

5. On the **Computer Selection** dialog box, do one of the following:
   - Expand the **Computers** list and select computers to add.
   - Right-click the **Selected Computers** area and click **Add**. The **Add Computer** dialog box displays. Type the domain and name of the computer you want to add and then click **OK**.

6. Click **Next**, and then click **Finish**.

Related Topics:

- "Introduction to Preferred Computers and Groups" on page 153

Deleting a Preferred Group

▼ **To delete a preferred group:**

1. On the management pane, expand the **Preferred Computers and Groups** node.

2. Right-click the preferred group you want to delete, and then click **Delete**.

3. A message displays prompting for confirmation. Click **Yes** to delete the preferred group.

Related Topics:

- "Introduction to Preferred Computers and Groups" on page 153

Renaming a Preferred Group

▼ **To rename a preferred group:**

1. On the management pane, expand the **Preferred Computers and Groups** node.
2. Right-click the preferred group to rename and click **Rename**.
3. Enter the new name in the text field and press ENTER.

Related Topics:

- "Introduction to Preferred Computers and Groups" on page 153

Adding or Removing Computers from a Preferred Group

▼ **To add or remove computers from a preferred group:**

1. On the management pane, expand the **Preferred Computers and Groups** node.
2. Right-click the preferred group and select **Properties**.
3. On the **Select Computers** tab, do one of the following:
   - Add a computer to the list by expanding the **Computers** list and selecting computers to include in the group.
   - Add a computer to the list by right-clicking the **Selected Computers** area and clicking **Add**. The Add Computer dialog box displays. Type the domain and name of the computer you want to add and then click **OK**.
   - Remove a computer from the list by highlighting it in the **Selected Computers** area and clicking **Remove**.
4. Click **Apply** and then click **OK** to save your modifications.

Related Topics:

- "Introduction to Preferred Computers and Groups" on page 153

Starting Services on a Preferred Computer

A computer that does not have services running is marked with the icon  and nothing displays in the details pane.

▼ **To start services on a preferred computer:**

1. From the management pane, expand the **Preferred Computers and Groups** node.
2. Expand a preferred group, right-click a target computer, and then click **Start Services**.

When the service starts, Storage Exec deletes audit and trend data that have exceeded their retention period.

Stopping Services on a Preferred Computer

A computer that has services running is marked with the icon  and its file groups, policies, reports, and managed resources display in the details pane.

▼ **To stop services on a preferred computer:**

1. From the management pane, expand the **Preferred Computers and Groups** node.
2. Expand a preferred group, right-click a target computer, and then click **Stop Services**.

Deleting a Preferred Computer From a Preferred Group

▼ **To delete a preferred computer:**

1. On the management pane, expand the **Preferred Computers and Groups** node.
2. Expand a preferred group, right-click the computer to delete, and click **Delete**.
3. A message displays prompting for confirmation. Click **Yes** to delete the computer.

Related Topics:

- "Introduction to Preferred Computers and Groups" on page 153

Viewing and Modifying Preferred Computer Properties

▼ **To view and modify preferred computer properties:**

1. On the management pane, expand the **Preferred Computers and Groups** node.
2. Expand the preferred group, right-click the target computer, and click **Properties**. The properties are organized on a series of tabs. Different tabs display depending on which Storage Exec options are installed on the computer.
3. View or modify the properties on the tabs.

   Refer to the section "Configuring Properties for a Computer" on page 34 for a detailed description of the options available on the tabs you see.
4. Click **OK** to modify the properties.

Related Topics:

- "Introduction to Preferred Computers and Groups" on page 153

Storage Exec Enterprise Administration Option A

This chapter applies only to users of the Storage Exec Enterprise Administration Option.

This chapter contains these sections:

Introduction to the Enterprise Administration Option

The Storage Exec Enterprise Administration Option provides centralized storage and automated dissemination of its data across the enterprise. With this option, Storage Exec stores its global properties, policies, file groups, and reports queries and reports in a central repository.

The management pane of the Administration Console changes when you install the Storage Exec Enterprise Administration Option. First, the name of the domain replaces the **My Computer** option. Second, these options are now available:

- **Computer Policies** enables you to create and modify computer policies. See the section "Computer Policies" on page 166 for more information about this topic.
- **Computers** lists the computers that have been configured to use the Enterprise Administration Option that you can manage.
- **Organizational Units** lists the domain controllers that you can manage.

Concepts

This section defines and illustrates two concepts that make the Storage Exec Enterprise Administration Option a powerful enterprise management tool:

- "Propagation" on page 162
- "Scoping" on page 160

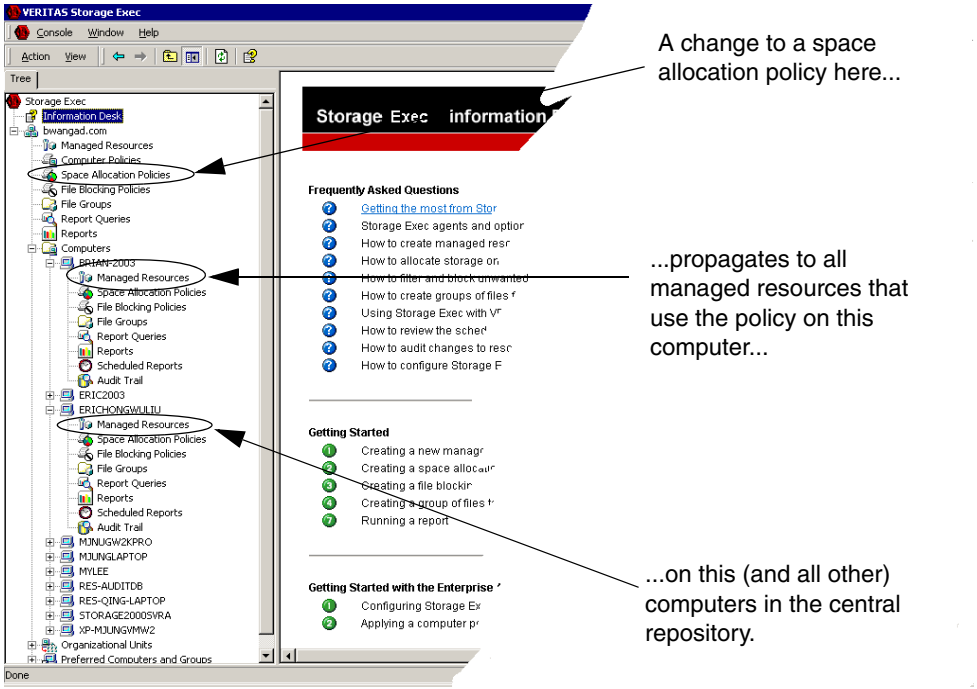
Propagation

Propagation, as it applies to the Storage Exec Enterprise Administration Option, means if you change a managed resource policy in the central repository, Storage Exec automatically makes that change in each managed resource that uses the policy, regardless of what computer the managed resource resides on.

The benefit of propagation is that a system administrator can modify a managed resource policy just once and have the change show up in all the enterprise's computers having a managed resource that uses that policy.

The figure below shows the management pane in an enterprise that has the Storage Exec Enterprise Administration Option installed.

Propagation



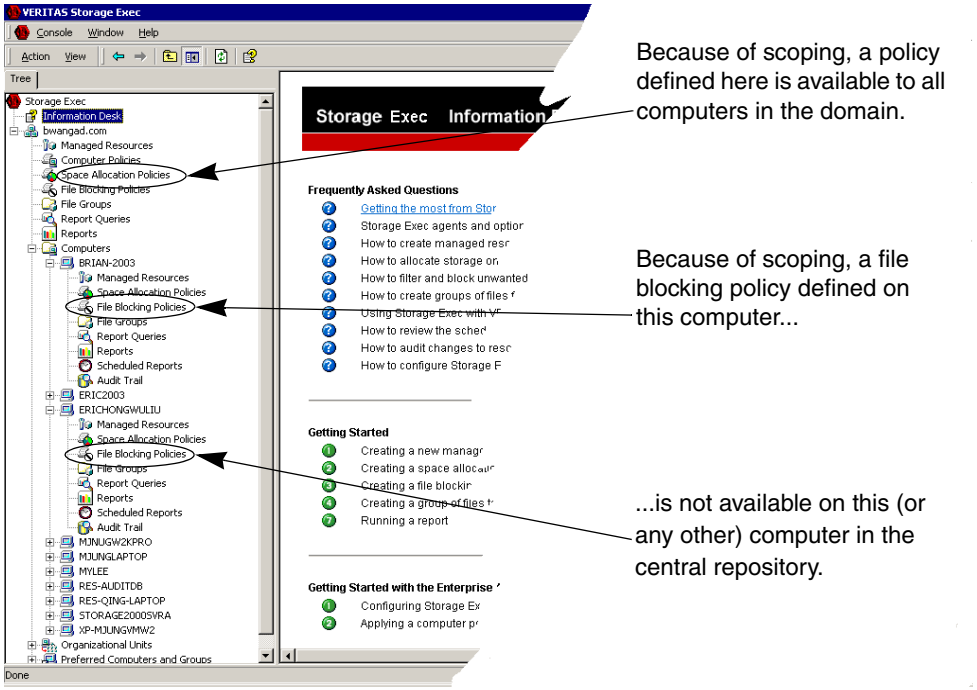
Scoping

Scoping, as it applies to the Storage Exec Enterprise Administration Option, means that managed resource policies stored in the central repository will be available to every computer that uses the repository. Also, a managed resource policy created on a computer in the central repository will be available to only that computer's managed resources. Other computers in the central repository's domain will not be able to see or use that managed resource policy.

The benefit of scoping is that space allocation and file blocking managed resource policies created for a specific computer will not be available for use on other computers, thus reducing the possibility for inadvertent misuse on the other computers.

The figure below shows the management pane in an enterprise that has the Storage Exec Enterprise Administration Option installed.

Scoping



If multiple policies having the same name exist, the more local policy takes precedence over the less local policy.

For example, you have a computer that is part of an Organizational Unit (OU), and this computer has a file blocking policy named Block Text Files. There is another policy at the OU level with the same name. When a user creates a managed resource on this computer and chooses the Block Text Files policy, Storage Exec will apply the policy stored on that computer—not the policy stored at the OU level.

Installation and Configuration

This section provides the following instructions for installing the Storage Exec Enterprise Administration Option and configuring your system to use it.

Requirements for the Enterprise Administration Option

These are the requirements associated with the Storage Exec Enterprise Administration Option:

- The computer where the Storage Exec Enterprise Administration Option is installed must be in an Active Directory domain.
- You must have Domain Admin or Enterprise Admin privileges to start the configuration wizard.
- You must have Schema Admin privileges to extend the schema.

Also, if the schema must be extended across domains, the current user account must have write access to the schema master registry.

Installing the Enterprise Administration Option

You can install the Storage Exec Enterprise Administration Option when you initially install the Storage Exec Server or any time after that. Regardless of when you install the option, you must enter the Storage Exec Enterprise Administration Option license key on the Serial Numbers dialog box of the installation program. For instructions to install the option, read the section "Installing Storage Exec from the Installation CD" on page 16.

After you install the option you must configure your system to take advantage of it. Follow the instructions in the section "Configuring the Enterprise Administration Option," below.

Configuring the Enterprise Administration Option

The Storage Exec Enterprise Administration Option uses Microsoft's Windows 2000 (or later) Active Directory to centrally store its data. However, before you can use Active Directory with Storage Exec you must run a wizard that performs these configuration tasks:

- Extend the Active Directory schema. The wizard adds two new attributes ("wquinn-DataType" and "wquinn-String") and two new classes ("wquinn-Container" and "wquinn-Value").
- Copy Storage Exec data from the local registry to the Active Directory domain. Placing the data in the Active Directory domain makes them available to all computers in the Active Directory domain on which the Storage Exec Enterprise Administration Option is installed.
- Add the Storage Exec Server computer, and those remote agents the user specifies through the wizard, to the Active Directory. Having the computer listed in the Active Directory enables Storage Exec to apply centralized policies to this computer.

To launch the Storage Exec Enterprise Administration Wizard, click the **Configuring Storage Exec to leverage your Active Directory** link on the Information Desk.

Extending the schema is done only once. After the schema is extended, all the domains can see it.

In a large, multi-tree domain, the schema extension can take several hours. The wizard gives the schema administrator the ability to restart the wizard later and run the part that copies data to the Active Directory.

Removing the Enterprise Administration Option

▼ To remove the Storage Exec Enterprise Administration Option

1. Remove the computer on which the option is installed from the Storage Exec portion of the Active Directory. Do so by following these instructions:

   a. Launch the Storage Exec Enterprise Administration Wizard by clicking the **Configuring Storage Exec to leverage your Active Directory** link on the Information Desk. Proceed through the wizard's dialog boxes until you reach the Select Computers to Remove From Enterprise Administration dialog box.

   b. Select the computer from which you want to remove the option on the wizard's Select Computers to Remove From Enterprise Administration dialog box. Proceed through the wizard's remaining dialog boxes.

2. Uninstall the option, along with Storage Exec Server, by following the instructions in the section "Uninstalling Storage Exec using Windows Add/Remove Programs" on page 25.

3. Reboot the computer to complete the removal.

Permissions for the Enterprise Administration Option

This section documents the following topics regarding permissions required to run the Storage Exec Enterprise Administration Option.

For information about permissions that apply to the entire product, read the chapter "Permissions" on page 229.

Permissions for Help Desk Users

Help desk users of the Storage Exec Enterprise Administration Option require FULL CONTROL permission to the Active Directory \WQuinn container.

To edit this, run the ADSI (Active Directory Services Interface) Administration Console utility that can be installed from the `\Support Tools` directory of the Windows 2000 (and Windows 2003) CD-ROM.

To add this utility, choose **Start | Run**, type **`MMC`**, and press Enter. In the MMC menu, choose **File | Add/Remove Snap-in**. Click the **Add** button. Select **ADSI** in the list. Click **OK**.

Granting Permissions to the Active Directory \WQuinn Container

The domain group SCWrite does not grant users permissions to the \WQuinn Active Directory container beneath servers in the Active Directory. Because a help desk user is not a Domain Administrator, permissions must be set for those users. This is only needed if a help desk user will change global properties of these servers.

▼ **To grant permissions to the Active Directory \WQuinn container**

1. Log in as Administrator.
2. In the ADSI Editor, right-click the root **ADSI** and choose **Connect to**. Click **OK**.
3. Expand the directory tree and select the \WQuinn container. Right-click and choose **Properties** from the menu. Click the **Security** tab. Then click the **Advanced** button.
4. Click the **ADD** button and select your help desk user or group. While they are selected, click the **Edit** button.
5. In the **Apply Onto** box, select **This object and all child objects**. Then select the **Allow** check box for the FULL CONTROL permission.
6. Click **OK** three times to close three open security properties dialogs.

Permissions for Active Directory

The READ permission to the \WQuinn container within the Active Directory is required for a user or group to read the properties of a policy in order to apply those properties to a managed resource. Likewise for report execution, the properties of the report must be read from the Active Directory. This is true only if you are running the Storage Exec Enterprise Administration Option.

Adding the SCRead and SCWrite Groups to the WQuinn Container in the Active Directory and Assigning Permissions

A WQuinn container is a container in the Active Directory hierarchy where the product attributes, such as the key, policy, and report information, are stored. During the installation of Storage Exec the WQuinn container is created by default at the domain root in the Active Directory. In case you need to override a policy or another setting, you may create a WQuinn container at any other node in the Active Directory hierarchy (for example, at a single computer or a group).

The Permissions Utility program used during installation allows you to assign permissions to the WQuinn container only at the domain root. In this section you will learn how to use ADSI Edit to assign permissions to the WQuinn container in the Active Directory that is not located at the domain root.

▼ To assign permissions to the WQuinn container in the Active Directory

1. Choose **Start** | **Run** and type **mmc**. Click **OK**.
2. When the Administration Console appears, click **File** and choose **Add/Remove Snap-in** in the menu.
3. The Add/Remove Snap-in dialog box displays. Select the **Standalone** tab and click **Add**.
4. The Add Standalone Snap-in dialog box displays. Select **ADSI Edit** in the list and click **Add**. Click **Close**.
5. On the Add/Remove Snap-in dialog box, click **OK** to close the dialog.
6. In the Administration Console, select the ADSI Edit node in the left pane, right-click and choose **Connect to** in the menu.

   The Connection Settings dialog box displays. The boxes **Name** and **Select a well known Naming Context** will contain values in them.
7. Click **OK** on the Connection Settings dialog box. The console window is now connected to the Active Directory for the domain.
8. Expand the **Domain NC** node in the left pane and find the CN=WQUINN node that is not located at the domain root. The permission at the domain root CN=WQUINN has been changed during the installation.
9. Right-click the **CN=WQUINN** node and choose **Properties** from the menu.

10. The CN=WQUINN Properties dialog box displays. Select the **Security** tab and click **Add**.

11. The Select Users, Computers or Groups dialog box displays. Click **Advanced**, click **Find Now**, select the SCRead and SCWrite groups in the list, and click **OK**.

    Now you have returned to the CN=WQuinn Properties dialog box.

12. Select the **SCRead** group on the **Security** tab. Make sure that the **Allow** check box is selected only for the Read permission.

13. Select the **SCWrite** group on the **Security** tab. Make sure that the **Allow** check box is selected for the Full Control, Read, Write, Create All Child Objects, and Delete All Child Objects permissions. Selecting the Full Control permission automatically selects all permissions.

14. Click **Apply** on the CN=WQUINN Properties dialog box. Then click **OK**. This will change standard ACL for the CN=WQUINN container in the Active Directory.

Computer Policies

This section contains the following sections:

Introduction to Computer Policies

A *computer policy* is a policy for applying managed resource policies to servers. When a computer policy is applied to a server, the included managed resource policies are applied to devices and folders on that server. Computer policies are a valuable feature because they allow organizations to implement policies across the enterprise quickly.

Computer policies are stored in the Storage Exec central repository. Only computers running the Storage Exec Enterprise Administration Option can see, create, or use computer policies.

The Enterprise Administration Option comes with one predefined computer policy. You can also define your own computer policies that apply managed resource policies to an entire computer device (for example, C:), to specific folders, or both. To define your own computer policy, follow the instructions in the section "Creating a New Computer Policy" on page 167.

To use a computer policy in your enterprise, follow the instructions in the section "Applying a Computer Policy" on page 170.

Note File blocking policies are placed on the folder itself, not on the children. With file blocking policies, "auto detect folders" and "apply to folder" are treated identically, meaning the file blocking policy is placed on the parent folder only.

Note Computer policies currently do not have mount point support.

Related Topics:

- "Creating a New Computer Policy" on page 167
- "Deleting a Computer Policy" on page 169
- "Viewing and Modifying Computer Policy Properties" on page 169
- "Applying a Computer Policy" on page 170
- "Introduction to Space Allocation" on page 63
- "Introduction to File Blocking" on page 83

Creating a New Computer Policy

▼ To create a computer policy

1. On the management pane, right-click **Computer Policies**. Click **New**, and then click **Computer Policy**.

2. Click **Next** on the Computer Policy Wizard's Welcome dialog box.

3. On the Policy Name dialog box, do the following:

   a. Enter a name for the computer policy you are creating. Do not use the following characters in the computer policy name: + # = ; , " \ / < >

   b. Enter a description of the computer policy.

   c. Click **Next**.

4. On the Device Selection dialog box, select the devices (drives) to apply the computer policy to. If you select **All Devices**, the dialog box enables you to select specific devices to not apply the computer policies to. Click **Next**.

   For example: If you choose the C: and J: devices, the managed resource policies you specify on the Device Policies dialog box (below) will be applied to the entire C: and J: drives of all computers you apply this computer policy to.

5. On the Device Policies dialog box, select a space allocation managed resource policy and/or a file blocking managed resource policy to apply to the entire device(s) you selected on the Device Selection dialog box. Click **Next**.

6. On the Folder Selection dialog box, specify the folders to include in the computer policy.

   To add folder names, click the  icon; press ENTER after you type each folder name.

   Optionally select the **Create folder if it does not exist** check box to instruct Storage Exec to automatically create the folder if it does not exist on the device(s) selected on the Device Selection dialog box. Click **Next**.

7. On the Folder Policies dialog box, select policies to apply to the folders specified on the Folder Selection dialog box. You may also specify a space allocation policy to apply to subfolders in a managed resource. Click **Next**.

8. Optionally select one or more reports to run using data from the computer you apply the computer policy to. To schedule the reports, do the following on the Report Schedule dialog box:

   a. Select one or more reports and the name of the server that is to process the reports.

   b. Click **Schedule** to specify when the report is to run. Click **OK**.

   c. Click **Next**.

9. A completion dialog box displays. Click **Finish** to create the computer policy.

Related Topics:

- "Introduction to Computer Policies" on page 166

Deleting a Computer Policy

▼ To delete a computer policy

1. On the management pane, expand **Computer Policies**. A list of computer policies displays in the details pane.
2. On the details pane, right-click the computer policy to delete, and then click **Delete**.
3. A message displays prompting for confirmation. Click **Yes** to delete the computer policy.

Related Topics:

- "Introduction to Computer Policies" on page 166

Viewing and Modifying Computer Policy Properties

▼ To view or modify computer policy properties

1. On the management pane, click **Computer Policies**. A list of computer policies displays in the details pane.
2. On the details pane, right-click a computer policy, and then click **Properties**.
3. On the Properties dialog box, you may view and modify properties. The tabs on the Properties dialog box correspond to the dialog boxes that are documented in the section "Creating a New Computer Policy" on page 167.
4. Click **Apply** to modify the properties.

Related Topics:

- "Introduction to Computer Policies" on page 166

Applying a Computer Policy

▼ **To apply a computer policy to a server**

1. On the management pane, right-click a server to apply a policy to, and then click **Apply Computer Policy**.
2. On the Select Computer Policy dialog box, select one or more computer policies to apply.
3. Click **OK** to apply the computer policy.
4. Go to the managed resource details pane and click the refresh button (). The managed resources created through the computer policy now display in the details pane.

Related Topics:

- "Introduction to Computer Policies" on page 166

Additional Reporting Capabilities

The Storage Exec Enterprise Administration Option provides several additional reporting capabilities.

- "Chargeback Summary Report" on page 170
- "Active Directory Fields in Custom Reports" on page 171

Chargeback Summary Report

You must have the Storage Exec Advanced Reporting Option installed to run the Chargeback Summary report. This is because this report is one of the extra reports that comes with the Storage Exec Advanced Reporting Option.

The Chargeback Summary report uses values your organization provides to compute a chargeback to a user's associated cost center in the Active Directory based on the amount of disk storage that user uses.

Before running this report, the Storage Exec administrator must set the cost per gigabyte and the account code (that is, the Active Directory field the report will use to assign its charges). The administrator sets these values on the global properties **Reports** tab.

Active Directory Fields in Custom Reports

You must have the Storage Exec Advanced Reporting Option installed to take advantage of Active Directory fields. This is because to use these fields you must create a report query, and you can create a report query only if the Storage Exec Advanced Reporting Option is installed.

Active Directory fields are the fields that contain information about the managed resource owners. Active Directory fields are supported only in the Storage Exec Enterprise Administration Option.

The Active Directory fields are useful when you want to view the owner information about a managed resource (folder) against which you are running a report. If several users own one folder, the report created using Active Directory fields will display information about all owners of that folder.

You may select Active Directory fields when creating a report query. To see the Active Directory fields, select the **Show advanced fields** check box from the Report Query Wizard's Display Fields and Filter Criteria dialog boxes. Selecting this check box causes Storage Exec to present additional fields.

Some of the Active Directory fields are: Account Expires, Company, Country Code, Employee ID, Given Name, Home Phone, Machine, Mail, Name, Owner, Street Address, and Title.

Related Topics:

- "Introduction to Reports" on page 121
- "Creating a Report Query" on page 104

Working with Network Appliance Filers B

This chapter applies only to the Storage Exec Network Appliance Option.

This chapter contains these sections:

Introduction to Using Storage Exec with Network Appliance Filers

The Storage Exec Network Appliance Option enables space allocation, file blocking, and reporting for Network Appliance Filers.

The Storage Exec Network Appliance Option provides support for the Filer in a manner quite different from that for directly attached storage devices. The reason for this difference is that no third-party software runs on the Filer. Network Appliance has provided a set of APIs that can be used to set and manage space allocation and file blocking. Space allocation is enforced directly by the Filer, while file blocking is enforced by third-party software, such as the Storage Exec Network Appliance Option, running on a computer other than the Filer.

Note Auto detection and computer policies are not supported with Network Appliance Filers.

There are several requirements that must be met before you can use Storage Exec with your Network Appliance Filer. For example, the proper version of ONTAP must be installed on the Filer, and the Filer must have CIFS enabled. Read the section "Requirements for the Storage Exec Network Appliance Option" on page 175 for a complete explanation of what you need to run Storage Exec.

For information about configuring the Network Appliance Filer, read these sections:

- "Converting to Qtrees on Network Appliance Filers" on page 175
- "Configuring SNMP for Space Allocation on Network Appliance Filers" on page 176
- "Configuring File Blocking on Network Appliance Filers" on page 178

For information about specific Storage Exec features and Network Appliance Filers, read these sections:

- "File Blocking and Network Appliance Filers" on page 177
- "Space Allocation and Network Appliance Filers" on page 178

For information about macros you can use to generate notification messages from Network Appliance Filers, read the sections "Space Allocation Message Macros" on page 78 and "Changing File Blocking Policy Properties" on page 87.

Network Appliance Filers and the Details Pane

The details pane does not present space allocation or file blocking managed resources for a Network Appliance Filer volume that is not online. Instead, you see a row with a managed resource of *volume-name — status*.

For example: You have defined a folder named Accounting on volume Prime on your Network Appliance Filer to have file blocking properties. If Prime is online, you see a row labelled Prime\Accounting. However, if this volume is offline, you see a row labelled Prime — Offline.

Additionally, the details pane indicates that a volume is initializing by displaying a row with the message *volume-name* — `quota initializing`. After the managed resource has initialized, the row is replaced with rows for the managed resources on that volume.

Related Topics:

- "Controlling the Filer from Storage Exec" on page 177

Requirements for the Storage Exec Network Appliance Option

To run the Storage Exec Network Appliance Option, your system must meet the minimum requirements listed in the section "System Requirements" on page 12. The sections below list additional requirements for running the Storage Exec Network Appliance Option.

To run Storage Exec on a Network Appliance Filer, the following items are required:

- ONTAP version 6.4 (or later) from Network Appliance must be installed on the Filer to provide support for third-party products (such as Storage Exec).
- The CIFS protocol must be enabled on the Filer you want to manage.
- SNMP must be configured on both the Filer and remote agent to generate traps for your remote agent.
- The Storage Exec Remote Agent and Administration Console must be installed and executed within the same domain as the Network Appliance Filers that they are intended to manage.
- Create a VERITAS qtree on the Network Appliance Filer.

Configuring the Filer to Work with Storage Exec

This section provides the following instructions to set up the Filer to work with Storage Exec.

- "Converting to Qtrees on Network Appliance Filers" on page 175
- "Configuring SNMP for Space Allocation on Network Appliance Filers" on page 176

Converting to Qtrees on Network Appliance Filers

Applying quotas to resources on the Filer can only be done when the resource is defined through the Filer as a qtree. If a root level folder needs to have quota management applied to it and it is not a qtree, then it must be converted.

To convert a root-level folder, follow the steps below. Take care during this process to prevent access to the folders during the conversion and make backups before conversion.

▼ **To convert to qtrees on Network Appliance Filers:**

1. Rename the existing folder.
2. Create a qtree with the name of the original folder.
3. Move the data from the saved folder to the qtree.
4. Remove the renamed folder.

Configuring SNMP for Space Allocation on Network Appliance Filers

When space allocation on a Filer is exceeded, the Filer can generate SNMP traps that can be used to create notifications (including email) for the administrators. SNMP must be configured correctly in the Filer and on the computer on which the Remote Agent is running.

Using the FilerView application provided by Network Appliance, follow the steps below to configure a Filer that Storage Exec is managing.

▼ **To configure SNMP for space allocation on Network Appliance Filers:**

1. Click **SNMP**.
2. Click **Configure**.
3. Set **SNMP Enabled** to **Yes**.
4. Set **Traps Enabled** to **Yes**.
5. Set **Auth Traps** to **Yes**.
6. Under **Communities**, set the first unused row to: Read-Only, Public
7. Set the **Traphosts**, which correspond to the community, to the name of the computer on which the Remote Agent is running. A fully qualified host name is recommended.
8. Click **Apply**.

Repeat these steps for each of the other Filers that Storage Exec is managing.

Controlling the Filer from Storage Exec

You can turn a Network Appliance Filer's quotas on or off from the managed resource details pane. You can also resize and restart quotas.

- To turn all quotas on, right-click a volume that has its quotas turned off, and choose **Quotas on**.
- To turn all quotas off, right-click one of the Filer's quotas, choose **Quota Management** and then select **Quotas off**.
- To resize all quotas, right-click one of the Filer's quotas, choose **Quota Management** and then click **Resize quotas**.
- To restart all quotas, right-click one of the Filer's quotas, choose **Quota Management** and then click **Restart quotas**.

Permissions for the Network Appliance Option

Help desk users of the Storage Exec Network Appliance Option require full administrator rights to the Filer.

For information about permissions that apply to the entire product, read the chapter "Permissions" on page 229.

File Blocking and Network Appliance Filers

Full support for file blocking is provided. However, all blocking requests are sent over the network from the Filer to the Storage Exec Network Appliance Option agent (remote agent) for servicing.

For file blocking to be enabled, file screening on the Network Appliance Filer must be enabled. For instructions, read the section "Configuring File Blocking on Network Appliance Filers" on page 178.

Note *File blocking* is the term used by Storage Exec, while *file screening* is the term used by Network Appliance.

Storage Exec does not block files residing on Network Appliance Filers under these conditions:

- The files were added or modified through a UNIX client; only files added or modified through a Windows computer can be blocked on Filers.
- The file blocking request originated from the computer on which the Remote Agent is running.

Configuring File Blocking on Network Appliance Filers

File blocking must be enabled on the Filers for the Storage Exec agent to successfully register.

Using a Microsoft Windows command window, issue a telnet command against the Filers and connect to the Filers. After a connection has been established, do one of the following:

- If you are running Data ONTAP version 6.4, enter this command:

  ```
  fpolicy enable default
  ```

- If you are running Data ONTAP version 6.5.1, enter these commands:

  ```
  fpolicy create default screen
  fpolicy enable default
  ```

For information about the `fpolicy` command, refer to the Data ONTAP documentation from Network Appliance.

Space Allocation and Network Appliance Filers

The Filer has a paradigm for space allocation that does not match Storage Exec. The Filer:

- Has hard and soft limits, and a threshold—all specified by numbers. Each of these numbers can cause an alarm to be triggered.
- Supports space allocation on a qtree, not on a folder.
- Rounds all quotas up to the next multiple of 4. For example, a quota established at 1 K becomes 4 K, while a 6 K quota becomes 8 K.

When working with Microsoft Windows-controlled resources, Storage Exec:

- Has a flag to determine if the space allocation is passive, and a single value for the space allocation. Up to 5 alarms can be set, all based on the space allocation amount as a percentage.
- Supports space allocation on any folder or file on a disk.

With these differences in mind, Storage Exec has implemented space allocation support in a fashion that mimics, as closely as possible, the support found in its Windows environment while using the values available through the Filer. For examples of this, read the section "Space Allocation and Network Appliance Filers—Examples" on page 180.

Storage Exec provides the two types of quotas that Network Appliance Filers provide: qtree and user. A qtree quota affects all users on one specific qtree. A user quota affects one specific user on one specific qtree.

A volume root share is required to manage quotas on a Network Appliance Filer. If the Administrator neglects to set a share on the volume root, but has created shares on qtrees, no folders appear in the New Managed Resource Wizard even though qtrees and shares exist on the Filer, and you are unable to create managed resources.

Limitations of Space Allocation on Network Appliance Filers

If a managed resource that resides on a Network Appliance Filer is renamed, Storage Exec will not know about the newly renamed resource. The resource will no longer display in the list of managed resources.

Network Appliance requires that a Filer's quotas be 1 KB or larger. This size limit applies to quotas you set explicitly and implicitly.

- If you manually create a quota with a space limit of 1-1023 bytes, a quota rule with all null values is created on the Filer.
- If you try to create a quota on a qtree using the "% of Size Used" units with a percent value that results in a quota of less than 1 KB, a quota rule with all null values is created on the Filer.

Space allocation features on the Filer that Storage Exec does not support:

- File limits, hard and soft
- Default space allocation
- Multiple users on one quota

Storage Exec space allocation features not available for Filer support:

- Overdraft limit
- Always save open files
- Reset high-water mark
- Send disk full error code
- Exclude from folder limit
- Activate below value (an option associated with alarms)
- Notify user (an action option) is not supported for qtree limits, but it is supported for user limits
- Extend (an action option)
- Alarms 3, 4, and 5
- File space allocation
- Folders below root level

Space Allocation and Network Appliance Filers—Examples

This section provides numerical examples of the information presented in the section "Space Allocation and Network Appliance Filers" on page 178.

Background

You used the FilerView application to establish a quota on the Network Appliance Filer with these values:

Disk space limit		Threshold
Soft	**Hard**	
40 MB	50 MB	30 MB

If you then viewed this configuration using Storage Exec, this is what you would see on the Properties dialog box when examining the managed resource (that is, the Filer's qtree):

Passive limit check box	Disk space limit	Alarm 1	Alarm 2
Not selected	50 MB	100%	80%

An explanation of these values:

- The **Passive Limit** check box is not selected because you specified a hard disk space limit through FilerView. Put another way, the space allocation limit for this managed resource is active.
- Storage Exec sets the disk space limit to 50 MB because that is the value of the hard disk space limit on the Filer.
- Storage Exec automatically sets Alarm 1's percentage to 100%.
- Storage Exec computes Alarm 2's percentage using the Filer's soft and hard disk space limits—the 40 MB soft disk space limit is 80% of the 50 MB hard disk space limit.

Example 1: Turn Passive Limit On

Starting with the example presented in the section "Background" on page 180, use Storage Exec to change the properties of the managed resource. Specifically, select the **Passive Limit** check box to change the space allocation limit for this managed resource from active to passive.

Passive limit check box	Disk space limit	Alarm 1	Alarm 2
Selected	50 MB	100%	80%

If you then used FilerView to view the properties of this quota on the Filer, you would see this:

Disk space limit		Threshold
Soft	Hard	
50 MB	--	40 MB

An explanation of these values:

- The soft disk space limit is 50 MB because the Storage Exec disk space limit becomes the Filer's soft disk space limit.
- There is no hard disk space limit because the space allocation limit is passive rather than active.
- The threshold is 40 MB because it is 80% of the 50 MB Storage Exec disk space limit. (The 80% comes from the Storage Exec Alarm 2.)

Example 2: Change the Disk Space Limit

Starting with the example presented in the section "Background" on page 180, use Storage Exec to change the properties of the managed resource. Specifically, change the disk space limit from 50 MB to 100 MB.

Passive limit check box	Disk space limit	Alarm 1	Alarm 2
Not selected	100 MB	100%	80%

If you then used FilerView to view the properties of this quota on the Filer, you would see this:

Disk space limit		Threshold
Soft	Hard	
80 MB	100 MB	--

An explanation of these values:

- The soft disk space limit is computed as a percentage of the hard disk space limit. The percentage used in this calculation (80%) comes from Alarm 2 of Storage Exec.
- The hard disk space limit has a value because there is an active (not passive) space allocation limit. This value (100 MB) comes from the Storage Exec disk space limit.
- There is no threshold because Storage Exec supports only two alarms on Filers, and the second alarm sets the soft disk space limit.

Example 3: Change Alarm 2

Starting with the example presented in the section "Background" on page 180, use Storage Exec to change the properties of the managed resource. Specifically, change the value of Alarm 2 from 80% to 40%.

Passive limit check box	Disk space limit	Alarm 1	Alarm 2
Not selected	50 MB	100%	40%

If you then used FilerView to view the properties of this quota on the Filer, you would see this:

Disk space limit		Threshold
Soft	Hard	
20 MB	50 MB	--

An explanation of these values:

- The soft disk space limit is computed as a percentage of the hard disk space limit. The percentage used in this calculation (40%) comes from Alarm 2 of Storage Exec.

- The hard disk space limit has a value because there is an active (not passive) space allocation limit. This value (50 MB) comes from the Storage Exec disk space limit.
- There is no threshold because Storage Exec supports only two alarms on Filers, and the second alarm sets the soft disk space limit.

Remote Server Agent C

This appendix applies only to users of the Storage Exec Remote Server Agent.

This appendix contains these sections:

Introduction to the Storage Exec Remote Server Agent

The Storage Exec Remote Server Agent, a component of the Storage Exec family of products, gives you these benefits:

- Much of the power of Storage Exec—such as the ability to set disk space quotas and perform file blocking—at less cost.
- The ability for a system administrator, logged on to a computer running Storage Exec Server, to monitor and administer an enterprise's servers from a single location.
- Reduced overhead for servers running as a Remote Server Agent. This is because the remote server will not process Storage Exec reports itself—rather, reports are run from the Storage Exec Server.

If you want the Storage Exec features that Storage Exec Remote Server Agent does not support (that is, being able to work in a clustered environment or to function as a report server), you can upgrade the remote server to be a Storage Exec Server.

Installing the Remote Server Agent on Remote Servers

This section provides the steps necessary for installing the Storage Exec Remote Server Agent on remote Windows servers in your network. Topics in this section include:

Requirements for Installing a Remote Server Agent

You must have a valid serial number for Storage Exec when installing Storage Exec agents on remote servers.

You must install Storage Exec Remote Server Agent on a network that has at least one computer running as a Storage Exec Server.

You must install a Storage Exec Remote Server Agent on any server running one of these Microsoft operating systems:

- Windows 2003 Server family
- Windows XP Professional Workstation with Service Pack 1 or higher
- Windows 2000 Server family with Service Pack 3 or higher
- Windows NT 4.0 Server and Workstation with Service Pack 6A or higher
- Windows Storage Server 2003

Installing a Remote Server Agent and the Storage Exec Server

Use these instructions to install one or more Remote Server Agents and Storage Exec Server at the same time.

Note You may also use the installation program, documented below, to install one or more Remote Server Agents after the Storage Exec Server is installed.

These instructions assume you are logged on at the server on which you will install the Storage Exec Server.

▼ To install a Remote Server Agent and the Storage Exec Server at the same time

1. From the Storage Exec Installation CD, double-click **Browser.exe.**
2. Select a language and then click **OK**.
3. Click **Install Storage Exec**.

   The Welcome window of the installation program appears.
4. Click **Next** to continue with the installation.
5. If the License Agreement screen appears, select **I accept the terms of the license agreement**, and then click **Next**.
6. On the Install Menu screen, select both **Local Install** and **Remote Agent Install**. Then click **Next**.
7. On the Serial Numbers screen, provide a serial number for Storage Exec Server and a serial number for the Remote Server Agent. Click **Add** after entering each serial number. You may also supply serial numbers for options you have purchased (for example, Storage Exec Advanced Reporting Option) if you want to install them on this Storage Exec Server. Click **Next** when you finish entering serial numbers.
8. On the Product Components screen, click **Next**.
9. On the Services screen, supply the requested values. Click **Next**.
10. On the Server Remote Features screen, right-click **Windows Agent/Option Computers** to display a shortcut menu for selecting the remote server(s) that you want to install to.

    On the shortcut menu, do one of the following:

    - Click **Add Remote Computer**, and then browse the list to select all of the remote servers that you want to install to, and then click **Next**.
    - Click **Add Remote Computer Manually**, and then type the domain and computer name, and then click **OK**. If using a Server Principal Name, type a fully qualified domain name for the computer.

    Add as many remote servers as you want to install Storage Exec to.

    When prompted, supply the user name, password, and domain credentials of an account that has administrative rights on the remote server, and then click **OK**. Select the **Remember user name and password** check box to have the installation program

use the values you supply for the first remote server on the second and subsequent remote servers, thus saving you the effort of re-entering values that remain constant across remote servers.

The remote servers you selected are displayed in the Remote Computers pane on the Server Remote Features screen, under **Windows Agent/Option Computers**.

11. Still on the Server Remote Features screen, for each remote server click the remote server name and then enable the **Remote Server Agent** feature. You may also enable the Remote Administration Console.

    If you do not see the **Remote Server Agent** option displayed, it means the installation program did not detect a server with an operating system that would support this remote agent.

    Click **Next**.

12. Review the information presented on the Installation Summary screen and then click **Next**.

    A status screen appears as Storage Exec Server is installed and as Storage Exec Remote Server Agent is installed on the remote server(s).

13. Follow the instructions on the screen to restart the remote server(s).

14. Click **Next** and then **Finish**. The server on which you installed Storage Exec Server restarts.

Installing the Remote Server Agent Using the Command Line Interface

These instructions assume you will execute the `Setup` command from the server on which you will install the remote agent.

▼ To install a Remote Server Agent using the command line interface

1. Log on as a local administrator.
2. Use the `Setup` command with the /AGENT: switch to install the Remote Server Agent. This command is located in multiple places:
   - On the installation CD, `Setup.exe` is in the `\WINNT\Agent` directory
   - On a computer that has the Storage Exec Server installed, the file is in the `Program Files\VERITAS\Storage Exec\Utilities\Agent` directory

   The table below lists the additional switches that `Setup` supports:

Setup Command Switches

Additional switches	Description
/RAC:	Installs the Remote Administration Console
/SNO:*RSA-serial-number*	Specifies the Remote Server Agent serial number
/NOREBOOT:	Specifies that the server will not be restarted after the installation finishes. The default is to restart the server.
<none>	Installs an evaluation copy of the Remote Server Agent

Here are some examples of the `Setup` command:

- **Setup /AGENT:**
  Installs an evaluation copy of the Remote Server Agent on a server.
- **Setup /AGENT: /SNO:*RSA-serial-number***
  Installs the Remote Server Agent on a server.
- **Setup /AGENT: /SNO:*RSA-serial-number* /RAC:**
  Installs the Remote Server Agent and the Remote Administration Console on a server.
- **Setup /AGENT: /SNO:*RSA-serial-number* /RAC: /NOREBOOT:**
  Installs the Remote Server Agent and the Remote Administration Console on a server with no restart.

Uninstalling the Remote Server Agent

Use the following steps to uninstall the Storage Exec Remote Server Agent from remote Windows servers in your network.

These instructions assume you are logged on at the server from which you will uninstall the Remote Server Agent.

▼ **To uninstall Remote Server Agent**

1. Choose **Start** | **Settings** | **Control Panel**, and then double-click **Add/Remove Programs**.
2. At the Add/Remove Programs dialog box, select **VERITAS Storage Exec Remote Agent**, and then click **Remove.**
3. When prompted to confirm the deletion of Storage Exec Remote Server Agent from your server, click **Yes.**

   When the uninstall is completed, you are prompted to restart the server.
4. Click **Yes.**

Using the Remote Server Agent

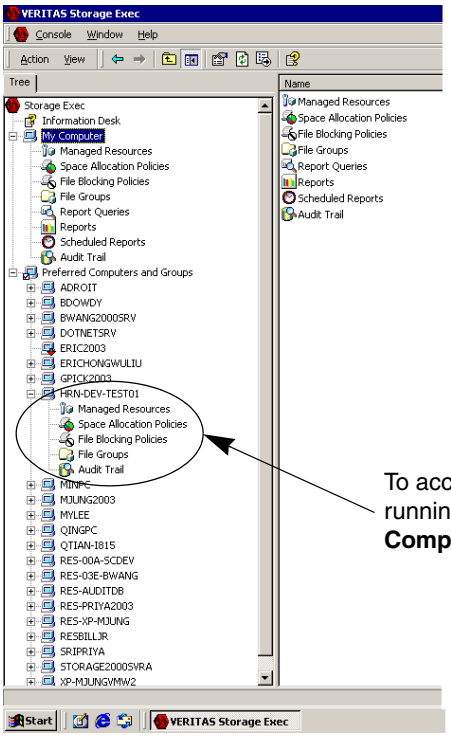
This section explains how to take advantage of the capabilities that come with the Storage Exec Remote Server Agent. Topics in this section include:

Accessing the Remote Server

There are multiple ways to access a remote server through Storage Exec.

- You can access a remote server from the Storage Exec Server. On the Storage Exec Server you must first add the remote server as a preferred computer (or a preferred computer as part of a preferred group). Then access the remote server as you would access any preferred computer. You can read more about this topic in "Preferred Computers and Groups" on page 153. The screen shot below illustrates remote access.

Accessing a Remote Server Agent Remotely



To access a remote server, log on to the server running Storage Exec Server and expand **Preferred Computers and Groups** in the management pane.

- You can access a remote server directly, by logging on to that server, starting the Storage Exec Administration Console, and accessing the Storage Exec capabilities by expanding the **My Computer** option on the management pane.
- You can log onto a computer that has the Storage Exec Remote Administration Console installed, but no Storage Exec services installed. You can then access and monitor any computer running Storage Exec.

Configuring Options on the Remote Server

You can remotely examine and modify a remote server's global properties from the server running Storage Exec Server by doing the following:

1. Log on to the Storage Exec Server and start Storage Exec.
2. Expand **Preferred Computers and Groups**.
3. Highlight the preferred computer that represents the remote server, right-click, and select **Properties**. The properties dialog box for that computer displays.

You may view and modify the remote server's properties by clicking the dialog box's tabs. (There is no reports tab because you cannot run reports from a remote server.) To read more about global properties, see the section "Configuring Properties for a Computer" on page 34.

You can also access a remote server's properties directly, by logging on to that server, starting Storage Exec, right-clicking the **My Computer** option on the management pane, and selecting **Properties**.

Working with Managed Resources

Managed resources are resources (for example, files, directories, and partitions) with space allocation or file blocking policies associated with them. You can create, delete, and modify managed resources on a remote server.

You can access a managed resource on a remote server two ways—remotely or directly.

- Remotely—To work with the managed resources on the remote server while logged in on the Storage Exec Server, expand **Preferred Computers and Groups** on the Storage Exec Server. Then locate and expand the preferred computer that represents the remote server.
- Directly—To work with the managed resources from the remote server while logged in on that server, go to the Administration Console on the remote server and expand **My Computer** and then expand the **Managed Resources**.

The figures in the section "Accessing the Remote Server" on page 191 illustrate these access methods.

You can read more about managed resources in "Managed Resources" on page 45.

Performing Space Allocation and File Blocking

From the Administration Console of a Storage Exec Server, you can perform storage resource management on remote servers. That is, you can enforce *space allocation* (limiting the amount of data stored in resources that Storage Exec manages) and *file blocking* (preventing users from storing data based on file type).

You can enforce space allocation and file blocking on a remote server two ways—remotely or directly.

- To perform storage resource management on a remote server while logged in on the Storage Exec Server, expand **Preferred Computers and Groups** on the Storage Exec Server. Then locate and expand the preferred computer that represents the remote server. Use the **File Groups**, **Space Allocation Policies**, and **File Blocking Policies** options of the remote server as you would if you were logged on to that server.
- To perform storage resource management on a remote server directly, log on to that server, start Storage Exec, right-click the **My Computer** option on the management pane, and use the **File Groups**, **Space Allocation Policies**, and **File Blocking Policies** options.

For more information about the options you can use remotely or directly, read these sections:

- "Introduction to File Groups" on page 97
- "Creating a Space Allocation Policy" on page 65
- "Creating a File Blocking Policy" on page 85

You can run reports as part of an alarm action. The only restriction is that you cannot select a remote server to be the server upon which Storage Exec runs the report.

If the Storage Exec Enterprise Administration Option is installed on a computer running the Storage Exec Server, the Active Directory's scoping rules will be in effect. For example, when you run the Managed Resource Wizard to create a new managed resource, the wizard presents you a list of policies to select from. Policies can reside on the local computer, the OU, or the domain. For more information about how the Storage Exec Enterprise Administration Option works, read the section "Concepts" on page 160.

Running Reports

You cannot run reports from the remote server. That is, there are no **Report Queries** and **Reports** options on the Storage Exec Remote Server Agent management pane.

However, you can run reports from a Storage Exec Server that gather data from one or more remote servers. To do so, follow these steps from the Storage Exec Server management pane:

1. Click **Reports** in the management pane. The list of available reports displays in the details pane.

2. Right-click the report you want to run and select **Run Report**.

3. In the **Resource(s)** field, specify one or more remote managed resources against which you want to run the report. Enter values in the other fields as you normally would; read section "Running a Report" on page 129 for more information.

4. Click **Submit**.

Account for Running the Remote Server Agent

If you are running a Remote Server Agent in an environment that does not include the Storage Exec Enterprise Administration Option, use the local system account for the services.

If you are running a Remote Server Agent in an environment that includes the Storage Exec Enterprise Administration Option, the Enterprise Administration Wizard assigns a logon user name and password to the Storage Exec services (QuotaAdvisor Server and FileScreen Server) when the wizard runs.

Troubleshooting the Remote Server Agent

This section identifies some problems you may encounter with the Remote Server Agent and offers some suggestions for resolving them.

Remote Agent Fails to Install

Problem: The remote agent does not install properly on the remote server.

Explanation: The installing user may have insufficient privilege to perform the installation or to communicate properly with the remote server.

Possible solutions: (1) Verify that the installing user is a member of the local administrators account on the remote server. (2) Examine the installation job log named `seinst.log`, which the install procedure creates on the computer where Storage Exec components are installed. This file lists any errors that may have occurred during installation. (3) Reboot and retry the installation procedure.

Remote Server Fails to Restart

Problem: A remote server fails to restart after the remote agent is installed on it.

Explanation: The installing user may have insufficient privilege to perform the restart or to communicate properly with remote server.

Possible solutions: (1) Verify that the installing user is a member of the local administrators account on the remote machine. (2) Examine the installation job log named `seinst.log`, which the install procedure creates on the computer where Storage Exec components are installed. This file lists any errors that may have occurred during installation. (3) You may need to restart the remote server manually.

Services Fail to Start on the Remote Computer

Problem: Services fail to start on the remote server.

Explanation: The installing user may have insufficient privilege to perform the installation. There may also be an installation error. Or the services may have been locked during the upgrade to an earlier version.

Possible solutions: (1) Validate that the installing user is a member of the local administrators account. (2) Examine the installation job log named `\WINDOWS\seinst.log`, which the install procedure creates on the computer where Storage Exec components are installed. This file lists any errors that may have occurred during installation. A message at the end of the log indicates if the installation was successful and if restarting the server is required. (3) Remove and reinstall Storage Exec on the remote server.

Remote Workstation Agent D

This appendix applies only to users of the Storage Exec Remote Workstation Agent.

This appendix contains these sections:

Introduction to the Storage Exec Remote Workstation Agent

The Storage Exec Remote Workstation Agent, a component of the Storage Exec family of products, gives you these benefits:

- Much of the power of Storage Exec—such as the ability to perform file blocking—at less cost.
- The ability for a system administrator, logged on to a computer running Storage Exec Server, to monitor and administer an enterprise's workstations from a single location.
- Reduced overhead for workstations running as a Remote Workstation Agent. This is because the remote workstation will not process Storage Exec reports itself—rather, reports are run from the Storage Exec Server.

Installing the Remote Workstation Agent on Remote Workstations

This section provides the steps necessary for installing the Storage Exec Remote Workstation Agent on remote Windows workstations in your network. The topics in this section include:

Requirements for Installing a Remote Workstation Agent

You must have a valid serial number for Storage Exec when installing Storage Exec agents on remote workstations.

You must install Storage Exec Remote Workstation Agent on a network that has at least one computer running as a Storage Exec Server.

You must install Storage Exec Remote Workstation Agent on any workstation running one of these Microsoft operating systems:

- Windows 2000 Professional with Service Pack 4 or higher
- Windows XP Professional Workstation with Service Pack 1 or higher
- Windows NT 4.0 Workstation with Service Pack 6A or higher

Installing a Remote Workstation Agent and the Storage Exec Server

Use these instructions to install one or more Remote Workstation Agents and Storage Exec Server at the same time.

Note You may also use the installation program, documented below, to install one or more Remote Workstation Agents after the Storage Exec Server is installed.

These instructions assume you are logged on at the workstation on which you will install the Storage Exec Server.

▼ To install a Remote Workstation Agent and the Storage Exec Server at the same time

1. From the Storage Exec Installation CD, double-click **Browser.exe.**
2. Select a language and then click **OK**.
3. Click **Install Storage Exec**.

   The Welcome window of the installation program appears.
4. Click **Next** to continue with the installation.
5. If the License Agreement screen appears, select **I accept the terms of the license agreement**, and then click **Next**.
6. On the Install Menu screen, select both **Local Install** and **Remote Agent Install**. Then click **Next**.
7. On the Serial Numbers screen, provide a serial number for Storage Exec Server and a serial number for the Remote Workstation Agent. Click **Add** after entering each serial number. You may also supply serial numbers for options you have purchased (for example, Storage Exec Advanced Reporting Option) if you want to install them on this Storage Exec Server. Click **Next** when you finish entering serial numbers.
8. On the Product Components screen, click **Next**.
9. On the Services screen, supply the requested values. Click **Next**.
10. On the Server Remote Features screen, right-click **Windows Agent/Option Computers** to display a shortcut menu for selecting the remote workstation(s) that you want to install to.

On the shortcut menu, do one of the following:

- Click **Add Remote Computer**, and then browse the list to select all of the remote workstations that you want to install to, and then click **Next**.
- Click **Add Remote Computer Manually**, and then type the domain and computer name, and then click **OK**. If using a Server Principal Name, type a fully qualified domain name for the computer.

Add as many remote workstations as you want to install Storage Exec to.

When prompted, supply the user name, password, and domain credentials of an account that has administrative rights on the remote workstation, and then click **OK**. Select the **Remember user name and password** check box to have the installation program use the values you supply for the first remote workstation on the second and subsequent remote workstations, thus saving you the effort of re-entering values that remain constant across remote workstations.

The remote workstations you selected are displayed in the Remote Computers pane on the Server Remote Features screen, under **Windows Agent/Option Computers**.

11. Still on the Server Remote Features screen, for each remote workstation click the remote workstation name and then enable the **Remote Workstation Agent** feature. You may also enable the Remote Administration Console.

If you do not see the **Remote Workstation Agent** option displayed, it means the installation program did not detect a workstation with an operating system that would support this remote agent.

Click **Next**.

12. Review the information presented on the Installation Summary screen and then click **Next**.

A status screen appears as Storage Exec Server is installed and as Storage Exec Remote Workstation Agent is installed on the remote workstation(s).

13. Follow the instructions on the screen to restart the remote workstation(s).

14. Click **Next** and then **Finish**. The server on which you installed Storage Exec Server restarts.

Installing the Remote Workstation Agent Using the Command Line Interface

These instructions assume you will execute the `Setup` command from the workstation on which you will install the remote agent.

▼ To install a Remote Workstation Agent using the command line interface

1. Log on as a local administrator.

2. Use the `Setup` command with the /AGENT: switch to install the Remote Workstation Agent. This command is located in multiple places:

   - On the installation CD, `Setup.exe` is in the `\WINNT\Agent` directory
   - On a computer that has the Storage Exec Server installed, the file is in the `Program Files\VERITAS\Storage Exec\Utilities\Agent` directory

   The table below lists the additional switches that `Setup` supports.

Setup Command Switches

Additional switches	Description
/RAC:	Installs the Remote Administration Console
/SNO:*RSA-serial-number*	Specifies the Remote Workstation Agent serial number
/NOREBOOT:	Specifies that the workstation will not be restarted after the installation finishes. The default is to restart the workstation.
<none>	Installs an evaluation copy of the Remote Workstation Agent

Here are some examples of the `Setup` command:

- **Setup /AGENT:**
  Installs an evaluation copy of the Remote Workstation Agent on a workstation.
- **Setup /AGENT: /SNO:*RSA-serial-number***
  Installs the Remote Workstation Agent on a workstation.
- **Setup /AGENT: /SNO:*RSA-serial-number* /RAC:**
  Installs the Remote Workstation Agent and the Remote Administration Console on a workstation.
- **Setup /AGENT: /SNO:*RSA-serial-number* /RAC: /NOREBOOT:**
  Installs the Remote Workstation Agent and the Remote Administration Console on a workstation with no restart.

Uninstalling the Remote Workstation Agent

Use the following steps to uninstall the Storage Exec Remote Workstation Agent from remote Windows workstations in your network.

These instructions assume you are logged on at the workstation from which you will uninstall the Remote Workstation Agent.

▼ **To uninstall Remote Workstation Agent**

1. Choose **Start** | **Settings** | **Control Panel**, and then double-click **Add/Remove Programs**.

2. At the Add/Remove Programs dialog box, select **VERITAS Storage Exec Remote Agent**, and then click **Remove.**

3. When prompted to confirm the deletion of Storage Exec Remote Workstation Agent from your workstation, click **Yes.**

   When the uninstall is completed, you are prompted to restart the workstation.

4. Click **Yes.**

Using the Remote Workstation Agent

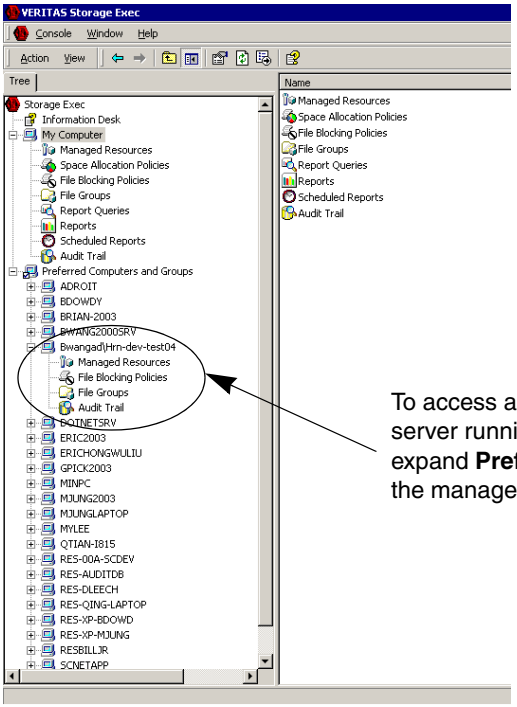
This section explains how to take advantage of the capabilities that come with the Storage Exec Remote Workstation Agent. Topics in this section include:

Accessing the Remote Workstation

There are multiple ways to access a remote workstation through Storage Exec.

- You can access a remote workstation from the Storage Exec Server. On the Storage Exec Server you must first add the remote workstation as a preferred computer (or a preferred computer as part of a preferred group). Then access the remote workstation as you would access any preferred computer. You can read more about this topic in "Preferred Computers and Groups" on page 153. The screen shot below illustrates remote access.

Accessing a Remote Workstation Agent Remotely



- You can access a remote workstation directly, by logging on to that workstation, starting the Storage Exec Administration Console, and accessing the Storage Exec capabilities by expanding the **My Computer** option on the management pane.
- You can log onto a computer that has the Storage Exec Remote Administration console installed, but no Storage Exec services installed. You can then access and monitor any computer running Storage Exec.

Configuring Options on the Remote Workstation

You can remotely examine and modify a remote workstation's global properties from the server running Storage Exec Server by doing the following:

1. Log on to the Storage Exec Server and start Storage Exec.
2. Expand **Preferred Computers and Groups**.
3. Highlight the preferred computer that represents the remote workstation, right-click, and select **Properties**. The properties dialog box for that computer displays.

You may view and modify the remote workstation's properties by clicking the dialog box's tabs. (There is no reports tab because you cannot run reports from a remote workstation.) To read more about global properties, see the section "Configuring Properties for a Computer" on page 34.

You can also access a remote workstation's properties directly, by logging on to that workstation, starting Storage Exec, right-clicking the **My Computer** option on the management pane, and selecting **Properties**.

Working with Managed Resources

Managed resources are resources (for example, files, directories, and partitions) with file blocking policies associated with them. You can create, delete, and modify managed resources on a remote workstation.

You can access a managed resource on a remote workstation two ways—remotely or directly.

- Remotely—To work with the managed resources on the remote workstation while logged in on the Storage Exec Server, expand **Preferred Computers and Groups** on the Storage Exec Server. Then locate and expand the preferred computer that represents the remote workstation.
- Directly—To work with the managed resources from the remote workstation while logged in on that workstation, go to the Administration Console on the remote workstation and expand **My Computer** and then expand the **Managed Resources**.

The figures in the section "Accessing the Remote Workstation" on page 203 illustrate these access methods.

You can read more about managed resources in "Managed Resources" on page 45.

Performing File Blocking

From the Administration Console of a Storage Exec Server, you can perform storage resource management on remote workstations. That is, you can enforce *file blocking* (preventing users from storing data based on file type).

You can enforce file blocking on a remote workstation two ways—remotely or directly.

- To perform storage resource management on a remote workstation while logged in on the Storage Exec Server, expand **Preferred Computers and Groups** on the Storage Exec Server. Then locate and expand the preferred computer that represents the remote workstation. Use the **File Groups** and **File Blocking Policies** options of the remote workstation as you would if you were logged on to that workstation.
- To perform storage resource management on a remote workstation directly, log on to that workstation, start Storage Exec, right-click the **My Computer** option on the management pane, and use the **File Groups** and **File Blocking Policies** options.

For more information about the options you can use remotely or directly, read these sections:

- "Introduction to File Groups" on page 97
- "Creating a File Blocking Policy" on page 85

You can run reports as part of an alarm action. The only restriction is that you cannot select a remote workstation to be the server upon which Storage Exec runs the report.

If the Storage Exec Enterprise Administration Option is installed on a computer running the Storage Exec Server, the Active Directory's scoping rules will be in effect. For example, when you run the Managed Resource Wizard to create a new managed resource, the wizard presents you a list of policies to select from. Policies can reside on the local computer, the OU, or the domain. For more information about how the Storage Exec Enterprise Administration Option works, read the section "Concepts" on page 160.

Running Reports

You cannot run reports from the remote workstation. That is, there are no **Report Queries** and **Reports** options on the Storage Exec Remote Workstation Agent management pane.

However, you can run reports from a Storage Exec Server that gather data from one or more remote workstations. To do so, follow these steps from the Storage Exec Server management pane:

1. Click **Reports** in the management pane. The list of available reports displays in the details pane.

2. Right-click the report you want to run and select **Run Report**.

3. In the **Resource(s)** field, specify one or more remote managed resources against which you want to run the report. Enter values in the other fields as you normally would; read section "Running a Report" on page 129 for more information.

4. Click **Submit**.

Account for Running the Remote Workstation Agent

If you are running a Remote Workstation Agent in an environment that does not include the Storage Exec Enterprise Administration Option, use the local system account for the services.

If you are running a Remote Workstation Agent in an environment that includes the Storage Exec Enterprise Administration Option, the Enterprise Administration Wizard assigns a logon user name and password to the Storage Exec services (QuotaAdvisor Server and FileScreen Server) when the wizard runs.

Troubleshooting the Remote Workstation Agent

This section identifies some problems you may encounter with the Remote Workstation Agent and offers some suggestions for resolving them.

Remote Agent Fails to Install

Problem: The remote agent does not install properly on the remote workstation.

Explanation: The installing user may have insufficient privilege to perform the installation or to communicate properly with the remote workstation.

Possible solutions: (1) Verify that the installing user is a member of the local administrators account on the remote workstation. (2) Examine the installation job log named `seinst.log`, which the install procedure creates on the computer where Storage Exec components are installed. This file lists any errors that may have occurred during installation. (3) Reboot and retry the installation procedure.

Remote Workstation Fails to Restart

Problem: A remote workstation fails to restart after the remote agent is installed on it.

Explanation: The installing user may have insufficient privilege to perform the restart or to communicate properly with remote workstation.

Possible solutions: (1) Verify that the installing user is a member of the local administrators account on the remote machine. (2) Examine the installation job log named `seinst.log`, which the install procedure creates on the computer where Storage Exec components are installed. This file lists any errors that may have occurred during installation. (3) You may need to restart the remote workstation manually.

Services Fail to Start on the Remote Computer

Problem: Services fail to start on the remote workstation.

Explanation: The installing user may have insufficient privilege to perform the installation. There may also be an installation error. Or the services may have been locked during the upgrade to an earlier version.

Possible solutions: (1) Validate that the installing user is a member of the local administrators account. (2) Examine the installation job log named `\WINDOWS\seinst.log`, which the install procedure creates on the computer where Storage Exec components are installed. This file lists any errors that may have occurred during installation. A message at the end of the log indicates if the installation was successful and if restarting the workstation is required. (3) Remove and reinstall Storage Exec on the remote workstation.

Command Line Interface E

The Storage Exec Command Line Applet is a convenient way to access some of the most useful features of Storage Exec from a command prompt. This chapter contains the following topics to help you use the Storage Exec command line interface.

- "Command SEAlloc" on page 209 explains the command that enables you to perform functions on space allocation managed resource policies.
- "Command SEBlock" on page 213 explains the command that enables you to perform functions on file blocking managed resource policies.
- "Command SEDisplayLimit" on page 214 explains the command that conveys information to users regarding their current space allocation usage.
- "Command SEReport" on page 215 explains the command that enables you to produce reports.
- "Command SESRM" on page 217 explains the command that enables you to perform functions on all managed resource policies.
- "Command SEClusterConfig" on page 219 explains the command that enables you to configure Storage Exec for a cluster.

Command SEAlloc

Use this command to perform functions related to space allocation managed resource policies.

Use the following switches with the SEAlloc command:

SEAlloc switches

Switch	Description
/LIST	List all space allocation policies
/SHOW	Show all space allocation managed objects

SEAlloc switches

/A	Add -- Default space limit is 10 MB -- Default overdraft value is 0 MB
/D[A][Y]	Delete[All][No confirmation]
/M	Modify
/S	Scan the named managed resource
/Y	/Y = Scan each individual managed resource on each volume /Y /O "*object*" = Scan each individual managed resource on the named volume
/X	Delay the scan until an SEAlloc command is issued with a /S or /Y switch
/O	managed resource name
/I	Enable auto detect subfolders
/L	Enable auto detect users
/T	Policy name
/P	Space limit in bytes (default)
/P:KB	Space limit in kilobytes
/P:MB	Space limit in megabytes
/P:GB	Space limit in gigabytes
/R	Overdraft in bytes (default)
/R:KB	Overdraft in kilobytes
/R:MB	Overdraft in megabytes
/R:GB	Overdraft in gigabytes
/[-]E	Active limit (default), -E Passive limit
/[-]W	Save open files (default), -W Do not save open files

SEAlloc switches	
/[-]Z	Enable volume, -Z Disable volume
/U	User or group, [Domain\User]
/?	Help

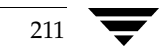
Use the following syntax with the SEAlloc command:

```
SEAlloc [\\server] /LIST

SEAlloc [\\server] /SHOW  [/O "object"]

SEAlloc [\\server] /A  /O "object"  /T "policy"
[[/I | /L] | [/U "domain\user"]]  [/X]

SEAlloc [\\server] /A  /O "object"
[[/I | /L] | [/U "domain\user"]]  [/P[:KB | :MB | :GB] "number"]
[/R[:KB | :MB | :GB] "number"]  [/[-]W]  [/[-]E]  [/X]

SEAlloc [\\server] /M  /O "object"  /T "policy"
[[/I | /L] | [/U "domain\user"]]  [/X]

SEAlloc [\\server] /M  /O "object"
[[/I | /L] | [/U "domain\user"]] [/P[:KB | :MB | :GB] "number"]
[/R[:KB | :MB | :GB] "number"]  [/[-]W]  [/[-]E  [/X]

SEAlloc [\\server] /DA[Y]  /O "object"

SEAlloc [\\server] /D[Y]  /O "object"
[[/I | /L] | [/U "domain\user"]]

SEAlloc [\\server] /S  /O "object"

SEAlloc [\\server] /Y  [/O "object"]

SEAlloc [\\server] /[-]Z  /O "object"
```

SEAlloc Command Examples

SEAlloc /a /o C:\Test /t "100 MB Limit":
Adds a space allocation object on `C:\Test` using the "100 MB Limit" managed object policy.

SEAlloc /a /x /o C:\Test /t "100 MB Limit":
Adds a space allocation object on `C:\Test` using the "100 MB Limit" managed object policy and does not perform a scan.



SEAlloc /a /o C:\ /p:mb 10 /r:kb 2 /e /u Domain\Joe:
Adds a user allocation object on `C:\` with user Domain\Joe.

SEAlloc /a /l /o C:\Test /t "100 MB Limit":
Adds an auto detect user object on `C:\Test` using the "100 MB Limit" managed object policy.

SEAlloc /a /i /o C:\Test /t "100 MB Limit":
Adds an auto detect folder object on `C:\Test` using the "100 MB Limit" managed object policy.

SEAlloc /d /o C:\Test:
Deletes the space allocation object on `C:\Test`.

SEAlloc /d /o C:\ /u Domain\Joe:
Deletes the user allocation object on `C:\` with user Domain\Joe.

SEAlloc /d /l /o C:\Test:
Deletes the auto detect user object on `C:\Test`.

SEAlloc /d /i /o C:\Test:
Deletes the auto detect folder object on `C:\Test`.

SEAlloc /m /o C:\Test /p:mb 5 /-e:
Modifies the space allocation object `C:\Test`.

SEAlloc /s /o C:\Test:
Scans the managed resource `C:\Test`.

SEAlloc /y:
Scans all the quota managed objects.

SEAlloc /y /o C:\:
Scans all the quota managed objects on volume `C:\`.

When using the SEAlloc command against a Network Appliance Filer, specify the Filer name before the first option and specify the path to the qtree (in the format volume\qtree) using the /O option. For example:

SEAlloc \\scnetapp /a /o vol0\Test /t “250MB limit with alerts”

This command creates a tree quota on qtree vol0\Test on a Network Appliance Filer named “scnetapp” and creates a space allocation managed resource in Storage Exec. Both the qtree quota and the space allocation managed resource use the “250MB limit with alerts” managed resource policy.

Command SEBlock

Use this command to perform functions related to file blocking managed resource policies.

Use the following switches with the SEBlock command

SEBlock switches

Switch	Description
/SHOW	Show all managed objects
/LIST	List all file blocking policies
/A	Add
/D[A][Y]	Delete[All][No confirmation]
/P	Policy name
/O	managed resource name
/S	Notify driver to scan managed objects
/?	Help

Use the following syntax for the SEBlock command:

```
SEBlock [\\server] /LIST
SEBlock [\\server] /SHOW
SEBlock [\\server] /A  /O "object"  /P "policy"
SEBlock [\\server] /DA[Y]
SEBlock [\\server] /D[Y]  /O "object"
SEBlock [\\server] /S
```


SEBlock Command Examples

SEBlock /a /o C:\Users /p "Monitor Office Files":
Adds the managed resource `C:\Users` with the "Monitor Office Files" managed object policy.

SEBlock \\NTDEV /d /o C:\Test:
Deletes the managed resource `C:\Test` on computer `\\NTDEV`.

When using the SEBlock command against a Network Appliance Filer, specify the Filer name before the first option and specify the path to the folder (in the format volume\folder) using the /O option. For example:

SEBlock \\scnetapp /a /o vol0\Test\Test0 /p “Stop graphic files”

This command creates a file blocking managed resource on folder vol0\Test\Test0 on a Network Appliance Filer named “scnetapp” in Storage Exec using the “Stop graphic files” managed resource policy.

Command SEDisplayLimit

The `SEDisplayLimit.exe` command displays a message showing users their current space allocation usage information. The command displays the information during logon.

Before this command can be used, the domain administrator must follow these steps to configure the user's logon script to run `SEDisplayLimit.exe` during logon:

1. Copy `SEDisplayLimit.exe` and `qasvr.tlb` from the directory `Program Files\VERITAS\Storage Exec\Utilities` to the NETLOGON shared directory on the domain controller.

   The NETLOGON shared directory is located in a directory similar to this:
   `your-system-drive``:\winnt\SYSVOL\sysvol\`*`your-domain-name`*`\Scripts`

2. Create a logon script in the NETLOGON shared directory to run `SEDisplayLimit.exe`.

   For example, the following script file might be named `DisplayLimit.cmd`:

   ```
   echo displaylimit script
   \\NTDEV\C$\winnt\SYSVOL\sysvol\wquinn.com\Scripts\
     SEDisplayLimit /hd
   pause
   ```

3. Configure a user's logon script to run the script created in step 2 by entering the script name (`DisplayLimit.cmd` in the above example) in the **Logon Script** box of the **Profile** tab on the user's Properties dialog box.

Command SEReport

Use this command to perform functions related to producing reports.

In addition to running report sets through the command line interface, you can run them through the Storage Exec graphical user interface. For more information, read the section "Running a Report" on page 129.

Use the following switches for the SEReport command:

Switch	Description
/LIST	List all report set names.
/R	Specify report set name. For a list and explanation of the report sets that come with Storage Exec, read the section "Predefined Reports" on page 133.
/O	Specify one or more managed objects separated by a pipe line.
/M	Specify the "Mail To" addresses separated by a semicolon. The values you specify for the /M switch override the values (if any) specified in the **Mail the report to the following email address** field on the **Output** tab of the report set's properties dialog box. If you do not use the /M switch, SEReport will email the report output to the value specified in the **Mail the report to the following email address** field.
/D	Specify the output directory or file name.
/F	Specify the command (parameter file) file name.
/UF	Specify user filter (Only available in the command file).
/?	Help.

Note The /R, /O, /M, /D, and /UF switches can be used in the command file.

Use he following syntax with the SEReport command:

```
SEReport [\\server] /LIST

SEReport [\\server] /F "parameterfile"

SEReport [\\server] /R "reportset" /O "object" [/M "email"]
[/D "output-directory-or-file-name"]
```


If the report object of the /O switch contains the root of two or more partitions (for example, C:\ and D:\) separated by a pipe character and enclosed in quotes, SEReport incorrectly interprets what you type as the escape sequence and the report is only run against the first partition. For example, typing this causes the problem:

```
SEReport /R "File Type Summary" /O "C:\|D:\"
```

To work around this problem, type one of the following:

- `SEReport /R "File Type Summary" /O "C:\\|D:\\"`
- `SEReport /R "File Type Summary" /O "C:|D:"`

SEReport Command Examples

SEReport \\NTDEV /r "Best Practices" /o "C:\Test|D:\Test":
Run the report set named Best Practices against the C:\Test and D:\Test managed objects.

SEReport /r "File Type Summary" /o C:\ /m xyz@veritas.com:
Run the report set named File Type Summary against the C:\ volume and send the output to the xyz@veritas.com email address.

SEReport /r "Best Practices" /o C:\ /d C:\report.html:
Run the report set named Best Practices against the C:\ volume and send the output to a file named `C:\Report.html`.

SEReport /r "Best Practices" /o C:\ /d C:\Output:
Run the report set named Best Practices against the C:\ volume and send the output to a file in folder `C:\Output`.

SEReport /f C:\Param.txt:
Run a report set using the instructions in the command file named `C:\Param.txt`.

SEReport \\NTDEV /f \\NTDEV\VeritasReportParameters\Param.txt:
Run the command file named `Param.txt`.

When using the SEReport command against a Network Appliance Filer, specify the path to the report object (in the format Filer_name\volume\folder) using the /O option. For example:

SEReport /r “Best Practices” /o \\scnetapp\vol0\Test

This command runs the report set named “Best Practices” against the folder vol0\Test on a Filer named “scnetapp.”

Command SESRM

Use this command to perform functions related to all managed resource policies.

Use the following switches with the SESRM command:

Switch	Description
/LIST	List all managed resource policies.
/SHOW	Show all managed objects.
/A	Add.
/D[Y]	Delete[No confirmation].
/M	Modify.
/O	managed resource name.
/I	Enable auto detect subfolders.
/L	Enable auto detect users.
/P	Policy name.
/U	User or group [Domain\User].
/?	Help.

Use the following syntax with the SESRM command:

```
SESRM [\\server] /LIST

SESRM [\\server] /SHOW

SESRM [\\server] /A  /O "object"  /P "policy"  [[/I | /L] |
[/U "domain\user"]]

SESRM [\\server] /M  /O "object"  /P "policy"  [[/I | /L] |
[/U "domain\user"]]

SESRM [\\server] /D[Y]  /O "object"  [[/I | /L] |
[/U "domain\user"]]
```


SESRM Command Examples

SESRM /a /o C:\Test /p "250MB Limit with blocking":
Adds both an allocation and a blocking object on `C:\Test` using the "250MB Limit with blocking" managed resource policy.

SESRM /a /l /o C:\Test /p "100MB Limit":
Adds an auto detect user object on `C:\Test` using the "100MB Limit" managed resource policy.

SESRM /m /i /o C:\Test /p "100MB Limit":
Modifies the auto detect folder object on `C:\Test` using the "100MB Limit" managed resource policy.

SESRM /d /o C:\Test:
Deletes managed resource on `C:\Test`.

SESRM \\NTDEV /d /i /o C:\Test:
Deletes the auto detect folder object and blocking object on `C:\Test` on computer \\NTDEV if the object exists.

When using the SESRM command against a Network Appliance Filer, specify the Filer name before the first option and specify the path to the qtree (in the format volume\qtree) using the /O option. For example:

SESRM \\scnetapp /a /o vol0\Test /p "250MB limit with blocking"

This command creates a tree quota on qtree vol0\Test on a Network Appliance Filer named "scnetapp". This command also creates a space allocation and a file blocking managed resource on the qtree in Storage Exec. The tree quota and both of the managed objects use the "250MB limit with blocking" managed resource policy.

Command SEClusterConfig

Use this command to configure Storage Exec for a cluster.

Use the following switches with the SEClusterConfig command:

SEClusterConfig swtiches

Switch	Description
/c	Configures Storage Exec for the cluster.
/u	Unconfigures Storage Exec from the cluster.
/a	Adds the Cluster Group while configuring and/or reconfiguring.
/r	Removes the Cluster Group while configuring.

SEClusterConfig Command Examples

SEClusterConfig /c /a SQLGroup, MyGroup

Configures Storage Exec for the cluster and adds the cluster groups SQLGroup and MyGroup.

SEClusterConfig /c /a MyGroup /r SQLGroup

Configures Storage Exec for the cluster, adds MyGroup, and removes SQLGroup

Cluster Support in Storage Exec F

This chapter documents the Storage Exec support for clustered servers. It includes the following topics:

Introduction to Cluster Support

Storage Exec supports clustered Windows servers using Windows 2000 Advanced Server, Windows 2003 Enterprise, or Microsoft Cluster Server. Storage Exec meets IBM's ClusterProven standard.

Storage Exec supports two cluster types: active/passive and active/active.

- **Active/Passive cluster**. To support high availability, the shared cluster resources are made available on one node of the cluster at a time. In the event of a failure on the active cluster node, the shared resources fail over to the passive node and users may continue to connect to the cluster without interruption.
- **Active/Active cluster**. To support load balancing and high availability, the cluster resources are split among two or more nodes. Each node in the cluster is the preferred owner of different resources. In the event of a failure of either cluster node, the shared resources on that node fail over to the remaining cluster nodes and users continue to access these resources without interruption.

How Managed Resources Work in Clusters

Managed resources are stored on the shared cluster disk in a file called `\QAQuotasV4.dat`. Because they are stored on the shared disk itself, the managed resource information is always available to the node in the cluster that is managing the storage. Resources are managed by the Storage Exec services that are installed on each node in the cluster.

In the event of a failover, the cluster service on the secondary node detects the failure and issues a mount request for the shared cluster drives. The Storage Exec driver detects this mount request and begins managing resources on that drive after it comes online. This is possible because the managed resource information is stored on the drive itself. The QuotaAdvisor Server service automatically resumes alarm actions on the remaining cluster node. No intervention by the Administrator is necessary.

A file blocking resource is handled differently. These resources are stored in the registry of each computer. The failover of file blocking resources is handled by the Storage Exec cluster resource.

How SRM Policies, Reports, and File Groups Work in Clusters

The failover of storage policies, reports, and file groups is handled differently depending on whether you selected Active Directory support. When you are using Active Directory, the policies are stored in the Active Directory and are therefore always available. When you are not using Active Directory, the policies are stored in the registry of each computer, and are replicated between the cluster nodes by the Storage Exec cluster resource.

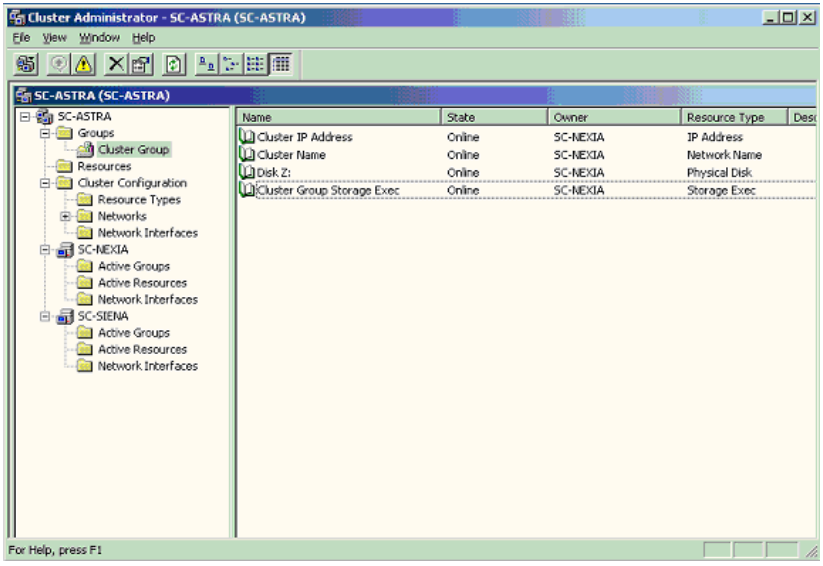
Policy settings that are specific to the resources you are managing are stored in a file called `\SESRMQuota\QAPolicyV5.mdb`. These policies are also in the registry.

To manage all managed resources in your cluster, create a preferred group and add the computer name of each member of the cluster to this group.

Using the Storage Exec Cluster Resource

The failover of policies and other registry-based information is handled by the Storage Exec cluster resource. A resource named "*group-name* Storage Exec" is created for each disk group. This resource verifies that the policy information on each cluster node is identical before and after failover. This ensures that SRM policies continue to function regardless of which cluster node is managing the storage.

Cluster Administrator Dialog Box



Preparing to Use Storage Exec in a Cluster

Before using the Cluster Configuration Wizard to set up Storage Exec in a clustered environment, you should perform the following:

- Ensure that your cluster meets the minimum requirements of Storage Exec (see the section "System Requirements" on page 12).
- Prepare a service account for the Storage Exec services. The account should be a member of the Local Administrators group.
- Install Storage Exec or the Enterprise Administration Option on each node in the cluster. Each node must have the same version of Storage Exec or the Enterprise Administration Option.

- The location of the audit and trend databases must be changed. By default, they are stored locally. However, in a clustered environment they must use a shared database. Follow the instructions in the section "Configuring Microsoft SQL Server as the Centralized Storage Exec Database" on page 30.

Adding Storage Exec Resources for Groups That Have Shared Disks

Use the Cluster Configuration Wizard to add the Storage Exec resource that has shared disks into a clustered environment.

▼ **To add Storage Exec resources:**

1. On the management pane, select **Information Desk**.
2. Under **Configuration**, select **Configuring Storage Exec for a clustered environment**.
3. On the **Welcome** screen, click **Next**.
4. Select **Add, remove, or reconfigure the Storage Exec resource for groups that have shared disks**, and then click **Next**.
5. To add the Storage Exec resource, select the resource group from the **Groups** column, and then click the right arrow to move it to the **Groups with the Storage Exec resource** column. Click **Next**.
6. Click **Finish** to complete the cluster configuration.

Reconfiguring the Storage Exec Resource

You should reconfigure the Storage Exec Resources when any of the following occurs:

- A new shared disk is added to a group. The Cluster Configuration Wizard will detect the new shared disk, but you must reconfigure the group.
- A new partition is created on a shared disk.
- Changes are made to shared disk settings.

▼ **To reconfigure the Storage Exec resource:**

1. On the management pane, select **Information Desk**.
2. Under **Configuration**, select **Configuring Storage Exec for a clustered environment**.
3. On the **Welcome** screen, click **Next**.
4. Select **Add, remove, or reconfigure the Storage Exec resource for groups that have shared disks**, and then click **Next**.
5. If the **Configure** screen displays, click **Next**.
6. From the **Groups with the Storage Exec resource** column, select a group that has changed, and then click the left arrow to move it to the **Selected groups** column. Click **Next**.
7. Click **Finish** to complete the cluster configuration.
8. If a new partition was created on a shared disk or if changes were made to the shared disk settings, proceed to step 9. If a new shared disk was added to the group, you have completed this procedure.
9. On the management pane, select **Information Desk**.
10. Under **Configuration**, select **Configuring Storage Exec for a clustered environment**.
11. On the **Welcome** screen, click **Next**.
12. Select **Add, remove, or reconfigure the Storage Exec resource for groups that have shared disks**, and then click **Next**.
13. If the **Configure** screen displays, click **Next**.
14. From the **Selected Group**s column, select the group that was changed, and then click the right arrow to move it to the **Groups with the Storage Exec resource** column.
15. Click **Next**, and then click **Finish**.

Modifying the Node Dependencies for the Storage Exec Resource

▼ **To change the controlling node:**

1. On the management pane, select **Information Desk**.
2. Under **Configuration**, select **Configuring Storage Exec for a clustered environment**.
3. On the **Welcome** screen, click **Next**.
4. Select **Modify node dependencies for the Storage Exec resource**, and then click **Next**.
5. Select the node from the **<Node name> Groups** column, and then click the right arrow to move it to the **<Node name> Groups with the Storage Exec resource** column. Click **Next**.
6. Click **Finish** to complete the cluster configuration.

Removing the Storage Exec Resource from All Groups

▼ **To remove Storage Exec resources:**

1. On the management pane, select **Information Desk**.
2. Under **Configuration**, select **Configuring Storage Exec for a clustered environment**.
3. On the **Welcome** screen, click **Next**.
4. Select **Remove the Storage Exec resource from all groups**, and then click **Next**.
5. Click **Yes** to verify that you want to remove Storage Exec from the resource groups.
6. Click **Finish** to complete the changes.

VERITAS Cluster Server Support

Storage Exec does not have direct support for VERITAS Cluster Server 2.0. However, the registry replication feature of VCS may be used to maintain consistency of Storage Exec registry information.

The following keys should be replicated:

- HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\Storage Exec\5.0\Definitions
- HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\Storage Exec\5.0\Groups
- HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\Storage Exec\5.0\Policies
- HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\Storage Exec\5.0\ReportSet
- HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\Storage Exec\5.0\Rules
- HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\Storage Exec\5.0\ServerPolicies

For more information, go to the VERITAS web site at www.veritas.com.

Permissions G

This chapter documents the permissions required to access Storage Exec. It contains these sections:

Note Option-specific permissions are documented in the "Storage Exec Enterprise Administration Option" on page 159 and "Working with Network Appliance Filers" on page 173.

Introduction to Permissions

Storage resource management (SRM) functions can be divided in two groups--standard and advanced management.

Standard storage resource management includes the following functions:

- Viewing space allocation and file blocking managed resources
- Executing reports

Advanced storage resource management includes the following functions:

- Creating and modifying policies, managed resources, and report queries
- Applying policies to managed resources

Advanced storage resource management should be limited to system administrators because they understand the effects SRM may have on business continuity and system performance. Specific user rights, permissions to file system resources, registry entries, and Active Directory resources are required to control who may create and apply policies. The administrative control is especially necessary in the configuration, setup, and implementation phases of SRM initiatives. After SRM policies, managed resources, and

administrative and user reports are created, the on-going maintenance of managed resources and report execution may be delegated to the users without full administrative rights.

Storage Exec uses Microsoft Windows security to protect against unauthorized users modifying storage policies, managed resources, and report queries. Additionally, the architecture of the product requires permissions to various resources. To control user access to Storage Exec and its resources, the proper rights and permissions must be assigned to individual users or user groups, such as the Help Desk group. Much of the permissions are assigned by the Storage Exec installation, which sets up a security access scheme using standard Windows global domain groups.

The following is required for Storage Exec to function correctly:

- The correct access for the Windows Management Instrumentation (WMI) must be set on all agent computers. For information about WMI permissions, read the section "Permissions for WMI" on page 239.
- The Task Scheduler on the server must be configured to run under the service account used in the installation. For information about how to set up the Task Scheduler logon account, read the section "Setting Up the Task Scheduler Logon Account" on page 244.

Related Topics:

- "Standard Permissions for Storage Exec" on page 232
- "Permissions for Running SRM Reports" on page 234
- "Permissions for Service Account" on page 236

Standard Storage Exec Security

In this section you will learn about two levels of non-administrative user access to Storage Exec, SCRead and SCWrite groups, and standard permissions for Storage Exec.

Non-administrative users are the users who are not included in the Administrators group. There are two levels of access to Storage Exec for non-administrative users: Read and Full Control. Read access to Storage Exec allows non-administrative users to run storage reports and view policies, managed resources, file blocking groups, report queries, reports, and global settings. Full Control access allows non-administrative users to add, delete, and modify policies, managed resources, file blocking groups, report queries, reports, and global settings, as well as perform the functions allowed by Read access.

Read and Full Control access are assigned through SCRead and SCWrite groups. When the Permissions Utility SEPerm.exe runs automatically during installation, it adds SCRead and SCWrite groups to the SAM domain. The user running the Permissions Utility should

be at least a member of the Domain Admins group. The SCRead group implements Read access level to the registry and Active Directory entries. The SCWrite group implements Full Control access level to the registry and Active Directory entries. The Access Control Lists (ACLs) are set up during the installation for the resources created and used by Storage Exec. These resources reside in the system registry, Active Directory, and installation directory.

The users added to the SCRead group will have at least Read access to Storage Exec while the users added to the SCWrite group will have Full Control access. The membership in the SCWrite group allows the users who are not members of the Administrators group to still manage Storage Exec. This security scheme is designed so that it does not disable the existing access. If users already have Full Control access, assigning them to SCRead group will not limit them to Read access. However, if users have no access to Storage Exec, assigning them to SCRead group will give them Read access.

Note Although the users added to SCWrite group have administrative access to Storage Exec and its resources, it is not the same as administrative access to the entire network system.

Related Topics:

- "Adding Users to the SCRead and SCWrite Groups and Assigning Permissions" on page 242.
- "Adding the SCRead and SCWrite Groups to a New Directory and Assigning Permissions" on page 243.
- "Permissions for WMI" on page 239.
- "Introduction to Permissions" on page 229.

Security for Reports

Any users who receive a storage report and have the OLE Control Extension (OCX) installed will be able to view and drill down on that report, only limited by the restrictions they have on the file system access.

During report generation, temporary files will be created in the %TEMP% directory. If no report directory is specified, reports should be created in the \Reports or \Temp directory. The SCRead and SCWrite groups are set by the permissions utility to have Full Control access to the %TEMP% and reports directory. The %TEMP% directory is dependent on the logon user; therefore, access is set only for the user who installed Storage Exec. Other users must have Full Control access to their %TEMP% directories for report drill-down to function correctly. To learn how to add SCRead and SCWrite groups to the %TEMP% directory, read the section "Adding the SCRead and SCWrite Groups to a New Directory and Assigning Permissions" on page 243.

Service Account

The service account user is set by the permissions utility to have Full Control access. The permissions utility automatically assigns the service account user to the SCWrite group and also assigns the "Adjust memory quotas for a process" right to the SCWrite group, which is inherited by that user. The "Adjust memory quotas for a process" right is required for space limits (quotas) to be properly created. If you are running the Storage Exec Enterprise Administration Option, the service account must be a domain-level user. For more information about the service account permissions, read the section "Permissions for Service Account" on page 236.

Standard Permissions for Storage Exec

Non-administrative users included in SCRead and SCWrite groups can access Storage Exec. The permissions utility `SEPerm.exe` grants the following permissions to SCRead and SCWrite groups:

Group	Permission
SCRead	Enable computer and user accounts to be trusted for delegation.
SCWrite	Adjust memory quotas for a process. Enable computer and user accounts to be trusted for delegation.

The SCRead and SCWrite groups are added to the ACLs (Access Control Lists) for the following resources:

Resource	Permission for SCRead group	Permission for SCWrite group
AD domain WQuinn container	Read	Full Control
Registry HKLM\Software\Storage Exec\5.0	Read	Full Control
Installation- directory\bin	Read & Execute	Read & Execute
Database-directory	Read	Full Control
Reports-directory	Full Control	Full Control
All SCSRMQuota directories	Read	Full Control

Resource	Permission for SCRead group	Permission for SCWrite group
%TEMP% directory	Full Control	Full Control
%TMP% directory	Full Control	Full Control
DCOM interfaces for SERptSvr.exe and SEFileSvr.exe	Allow (to access and launch)	Allow (to access and launch)

Related Topics:

- "Introduction to Permissions" on page 229

Advanced Storage Exec Security

This section presents information regarding advanced Storage Exec security. It includes the following topics:

Advanced Permissions for Help Desk Users

Help desk users can be given Full Control access by assigning them to the SCWrite group. If you want to limit access to this type of user, you can manually assign the access permissions on the server.

Storage Exec

This section describes the permissions needed if you are running Storage Exec.

- "Adjust memory quotas for a process" right. Choose **Start** | **All Programs** | **Administrative Tools** | **Local Security Policy**. In Local Policies choose **User Rights Assignment** to assign this right. This is a requirement for creating or modifying a space allocation managed resource.
- LIST permission to all managed resource directories (that is, `\Users`).
- FULL CONTROL permission to the registry key HKEY_LOCAL_MACHINE\Software and its sub keys.
- FULL CONTROL permission to the `\Program Files\VERITAS` directory and its sub directories.

Permissions for Running SRM Reports

To execute a report, LIST permission is required to all drives and directories that will be reported on. READ permission is required if you want the report to return file ownership information. Although the report may not fail if the user has insufficient permissions, it may be returned blank or not include a list of all files that meet the report query criteria.

The following access permissions are required in the Storage Exec installation directories, assuming a default installation:

Directory	Permission required	Notes
`C:\Program Files\Veritas`	List	Typical install location of the Storage Exec directory.
`C:\Program Files\Veritas\Storage Exec\bin`	Read, Write	This is required because the DCOM server on the server you use to run reports generates a temporary file in this folder during report generation. This assumes that the SERptSvr DCOM server on the server you use to run reports is running under the service account identity. Read the section "Permissions for DCOM" on page 237 for alternatives.

Directory	Permission required	Notes
`C:\Program Files\Veritas\Storage Exec\Reports`	Full Control	When a report is executed, an output file is created in this directory on the server you use to run reports. This is also true when reports are generated interactively. This assumes that the SERptSvr DCOM server on the server you use to run reports is running under the service account identity. Read the section "Permissions for DCOM" on page 237 for alternatives.
`C:\Program Files\Internet Explorer` and its sub-directories	Read and Execute List folder contents Read, Write	This is required for the computer where the report is being launched. This is required to support drill-down capabilities from Active-X reports.
A share \WQReportParameters	Modify	This share must be created and accessible to users running reports. This share must reside on every Storage Exec server you use to run reports. By default, this share is created on the directory `C:\Program Files\Veritas\Storage Exec\Reports` with the Everyone group having Full Control access.
`C:\Windows\TEMP`	Read, Write	This is required because the DCOM server on the server you use to run reports generates a temporary file in this folder during report generation.
Registry and Active Directory	see notes	The proper permissions must be assigned to the registry and Active Directory. For information about these permissions, read the section "Permissions for Registry" on page 236.

Related Topics:

- "Introduction to Permissions" on page 229.

Permissions for Service Account

When the agent is installed, Storage Exec installs two services—QuotaAdvisor Server and FileScreen Server. These services should run under a specified service account. Due to the Auto Detect feature included with Storage Exec, the service account at times does not have an interactive user to impersonate. It is recommended that the QuotaAdvisor Server and FileScreen Server services run under a specified administrative account that has the "Adjust memory quotas for a process" right.

The Permissions Utility SEPerm.exe assigned the “Increased Quota” right for the computer the agents are installed on. You must follow the steps below only if the service account is changed.

▼ **To assign the "Adjust memory quotas for a process" right:**

1. Choose **Start**, select **Programs**, and then select **Administrative Tools**. Select **Local Security Settings**.
2. Select **Local Policies**, and then choose **User Rights Assignment**.
3. Right-click the “Adjust memory quotas for a process” policy and choose **Properties**.
4. Assign the "Adjust memory quotas for a process" right to the service account.
5. Click **OK**.

Related Topics:

- “Introduction to Permissions” on page 229.

Permissions for Registry

An interactive user (a user who runs the user interface) and the two service accounts (QuotaAdvisor Server and FileScreen Server) need the following permissions to access the registry:

- READ permission to the registry key HKEY_LOCAL_MACHINE\Software and its sub keys. This is required for report execution and application of a policy to a managed resource. The properties for reports and policies are stored in the registry if you are not running the Storage Exec Enterprise Administration Option.
- FULL permission to the registry key HKLM\Software\5.0\Devices. This is required, regardless of which option you are running, to create or modify file blocking resources. The list of folders that have a file blocking policy applied to them resides in this registry key.

Related Topics:

- "Introduction to Permissions" on page 229.

Permissions for DCOM

The DCOM application SERptSvr handles reports and is installed on the Storage Exec Server. By default, the SERptSvr DCOM runs under the identity of the account you specified for Storage Exec services (read the section "Permissions for Service Account" on page 236). This account should be a member of the Domain Administrators group. This is very similar to a feature of the Task Scheduler. In the Task Scheduler, you can schedule a job to run as another user. If SERptSvr is running as the Launching User, the report will execute as the user running the user interface. If the report is scheduled, the report will execute as the user that the Task Scheduler is running as.

- Specifying an account for SERptSvr is required if the server on which you run reports is remote to the managed console. The SERptSvr account must have enough permissions for accessing the file system and using DCOM.
- Specifying an account for SERptSvr is recommended if a non-administrative user needs to run reports, or for a server on which many reports will be scheduled.

The Storage Exec DCOM server (SERptSvr) can be configured using the DCOMCNFG utility. If you wish to limit who will run reports, set SERptSvr to the "Launching User." Permissions of an interactive user are used to generate reports. The users without permissions to the directories will be able to run reports, but the output will not include files to which they do not have at least LIST access.

▼ To check or change the DCOM account for SERptSvr:

1. Choose **Start**, and then click **Run**.
2. Type **`dcomcnfg`**, and then click **OK**.
3. From the Component Services dialog box, highlight **Component Services**, then double-click **Computers**.
4. Double-click **My Computer**, and then double-click **DCOM Config**.
5. Right-click **SERptSvr** and click **Properties**.
6. On the **Identity** tab, select **The launching user** option to change the account.

If SERptSvr is set to the "Launching User," you must change the AT service account for scheduled reports.

To change the AT service account:

1. Go to the `\Windows\Tasks` folder.
2. Choose **Advanced/AT Service Account** from the menu.
3. Stop and restart the Scheduler for this change to take effect.

An interactive user (a user who runs the user interface) and the two service accounts (QuotaAdvisor Server and FileScreen Server) need the following permissions to access Storage Exec:

If you are running Storage Exec with no options:

- READ permissions to access the local registry.
- Key [HKEY_LOCAL_MACHINE\SOFTWARE] and its subkeys.

If you are running the Storage Exec Network Appliance Option:

- READ permissions to access the local registry.
- Key [HKEY_LOCAL_MACHINE\SOFTWARE] and its subkeys.
- Full administrator rights to the Filer.

If you are running the Storage Exec Enterprise Administration Option:

- READ permissions to access the local registry.
- Key [HKEY_LOCAL_MACHINE\SOFTWARE] and its subkeys.
- READ permissions to access the Active Directory \Wquinn container.

If you are running the Storage Exec Network Appliance Option and Storage Exec Enterprise Administration Option together:

- READ permissions to access the local registry.
- Key [HKEY_LOCAL_MACHINE\SOFTWARE] and its subkeys.
- READ permissions to access the Active Directory \Wquinn container.
- Full administrator rights to the Filer.

Related Topics:

- "Introduction to Permissions" on page 229.

Permissions for WMI

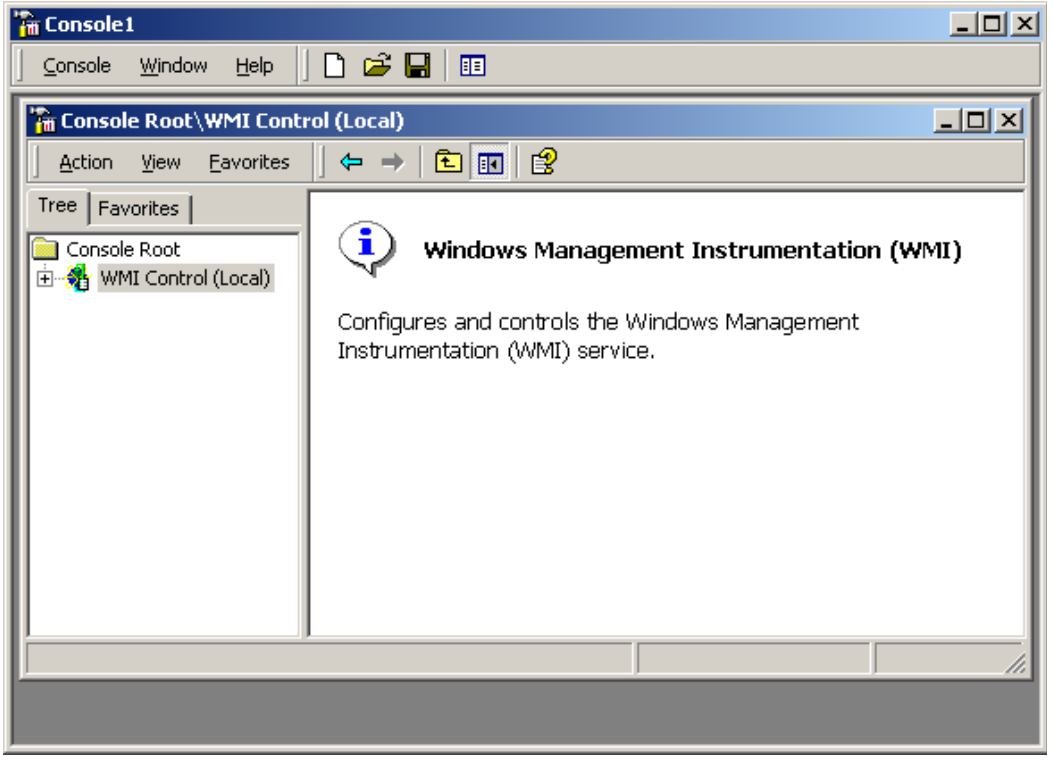
Windows Management Instrumentation (WMI) is used by the Storage Exec wizards in the user interface to enumerate folders to which policies are applied. To be successful, a user running the user interface on a client computer must be added to the security for CIMV2 WMI Control. Non-administrators, such as Help Desk users, that are in the SCWrite group must be added to WMI.

▼ **To add a user or group to the security for CIMV2 WMI Control:**

1. Choose **Start**, and then click **Run**.
2. Type **mmc**., and then click **OK**.
3. The Console1 window displays. From the **File** menu, choose **Add/Remove Snap-in**.
4. Click **Add** on the **Standalone** tab.
5. From the **Add Standalone Snap-ins** list, select **WMI Control**, and then click **Add**.
6. On the Change managed computer dialog box, select **Local computer** and click **Finish**.
7. Close the Add Standalone Snap-ins dialog box.
8. Click **OK** on the Add/Remove Snap-in dialog box to add the WMI Control.

The Administration Console tree should look like this:

Administration Console Tree on a Windows 2000 computer

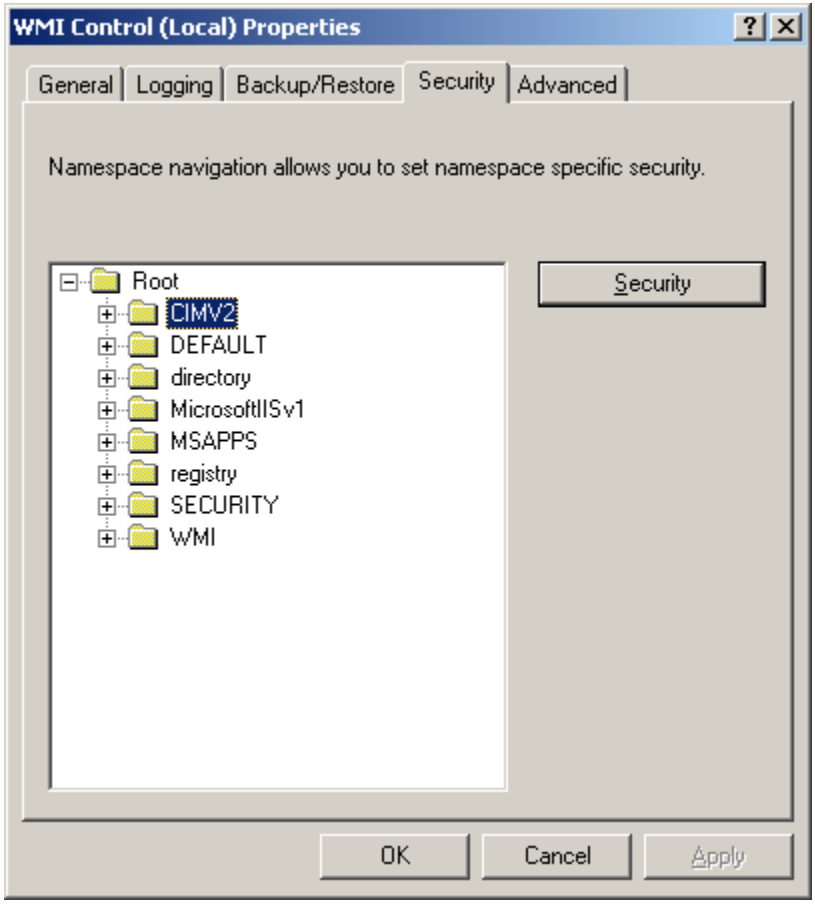


9. Right-click **WMI Control (Local)** in the Administration Console tree, and choose **Properties**.

10. On the WMI Control (Local) Properties dialog box, click the **Security** tab, expand **Root**, select **CIMV2**, and click **Security**.

The **Security** tab is shown in the figure below.

Security Tab of the WMI Control (Local) Properties Dialog Box on a Windows 2000 computer



11. To add a specific user or group, click **Add** on the Security for Root\CIMV2 dialog box.

12. On the Select Users, Computers, or Groups dialog box, select a domain, select a user or group, click **OK**, and click **OK** again.

13. The user or group name displays on the Security for Root\CIMV2 dialog box. To assign permissions, select the user or group in the list and select the **Allow** check box next to the permissions required for that user or group.

14. On the Security for Root\CIMV2 dialog box, click **Advanced**. The Advanced Security Settings for CIMV2 dialog box displays.

15. On the Advanced Security Settings for CIMV2 dialog box, select the newly added user or group and click **Edit**.

16. On the Permission Entry for CIMV2 dialog box, ensure that permissions are applied to "This namespace and subnamespaces." Click **OK**.

Related Topics:

- "Introduction to Permissions" on page 229.

Adding Users to the SCRead and SCWrite Groups and Assigning Permissions

The non-administrative users added to the SCRead group will have Read permission. The non-administrative users added to the SCWrite group will have Full Control permission. You can assign Read or Full Control permissions in two ways:

- By selecting a single user and making him or her a member of the SCRead or SCWrite group.
- By selecting a group (SCRead or SCWrite) and adding a number of users to that group.

▼ **To assign Read or Full Control permissions to a single non-administrative user with no access:**

1. Choose **Start**, select **Programs**, and then select **Administrative Tools**. Click **Active Directory Users and Computers**.

2. Expand the Active Directory structure under the domain node in the left pane and select **Users**.

3. In the right pane, right-click either **SCRead** or **SCWrite** depending on your needs.

4. Click **Properties**.

5. On the Properties dialog box, click the **Member Of** tab.

6. On the **Members** tab, click **Add**.

7. On the Select Users, Contacts, Computers, or Groups dialog box, enter a user name.

8. Click **Check Names**.

9. Click **OK**.

10. Click **Ok** to close either the SCRead or SCWrite properties dialog box.

▼ **To add a number of non-administrative users to SCRead and SCWrite groups:**

1. Choose **Start**, select **Programs**, and then select **Administrative Tools**. Select **Active Directory Users and Computers**.

2. Expand the Active Directory structure under the domain node in the left pane and select **Users**.

3. In the right pane, right-click the SCRead or SCWrite group, and choose **Properties** in the menu.

4. On the group Properties dialog box, select the **Members** tab and click **Add**.

5. On the Select Users, Contacts, Computers, or Groups dialog box, click **Advanced**, click **Find Now**, select one or more users, and click **OK**.

6. Click **OK** on the Properties dialog box to save your changes and exit the window.

Adding the SCRead and SCWrite Groups to a New Directory and Assigning Permissions

When you move report or database directories, you should add the SCRead and SCWrite groups to the new directory's Access Control List (ACL) and then assign proper permissions to these groups.

▼ **To add the SCRead and SCWrite groups to a new directory:**

1. In Windows Explorer, right-click a new directory in the left pane, and choose **Properties**.

2. Click the **Security** tab on the directory Properties dialog box.

3. Click **Add**.

4. The Select Users, Computers, or Groups dialog box displays. Click **Advanced**, click **Find Now**, select the SCRead and SCWrite groups in the list, and click **OK**. Then click **OK** again. The SCRead and SCWrite groups now display in the directory Properties dialog box.

5. Select the **SCRead** group. If this is the `Reports` directory, all permissions should be selected. If this is the `Database` directory, only Read & Execute, List Folder Contents, and Read permissions should be selected.

6. Select the **SCWrite** group. All permissions should be selected for this group. Select the **Allow** check box for Full Control permission. This automatically selects all permissions.

7. Click **Apply**. Then click **OK**. Now you have assigned proper permissions to the SCRead and SCWrite groups in the new directory.

Setting Up the Task Scheduler Logon Account

If the agent does not reside on the server you use to run reports, the Task Scheduler must be configured to run under the service account used in the installation.

▼ **To configure the Task Scheduler logon account:**

1. Open Windows Explorer on the computer used to run reports.

2. From **My Computer**, select **Control Panel**, and then select **Scheduled Tasks**.

3. From the **Advanced** menu, choose **AT Service Account**.

4. On the AT Service Account Configuration dialog box, select **This Account** and enter the service account name and password for Storage Exec. Click **OK**.

5. From the **Advanced** menu, choose **Stop Using Task Scheduler**.

6. From the **Advanced** menu, choose **Start Using Task Scheduler**.

Related Topics:

- "Introduction to Permissions" on page 229

Accessibility and Storage Exec H

VERITAS products meet federal accessibility requirements for software as defined in Section 508 of the Rehabilitation Act:

- http://www.access-board.gov/508.htm

Keyboard shortcuts are available for all graphical user interface (GUI) operations and menu items. VERITAS products are compatible with operating system accessibility settings as well as a variety of assistive technologies. All manuals also are provided as accessible PDF files, and the online help is provided as HTML displayed in a compliant viewer.

The following topics detail accessibility features and compliance in Storage Exec:

Keyboard Navigation and Shortcuts in Storage Exec

All program functions and menu items are accessible using the keyboard exclusively. Storage Exec uses standard operating system navigation keys and keyboard shortcuts.

Items in the task pane that do not have keyboard shortcuts can be accessed by using the operating system's "mouse keys," which allow you to control the mouse through the numerical keyboard.

To see a table of the standard Microsoft navigation keys and keyboard shortcuts, select your version of Microsoft Windows from the table at:

http://www.microsoft.com/enable/products/keyboard.aspx

General Keyboard Navigation Within the GUI

You can navigate and use Storage Exec with only the keyboard. In the GUI, the current active tree or table has a dark blue highlight, and the current active tab, radio button, or check box is enclosed within a rectangle formed by dotted lines. These areas are said to have *focus* and will respond to commands.

All VERITAS GUIs use the following keyboard navigation standards:

- The TAB key moves the focus to the next active area, field, or control, following a preset sequence. SHIFT+TAB moves the focus in the reverse direction through the sequence.
- CTRL+TAB exits any Console area that you internally navigate with the TAB key.
- UP and DOWN ARROW keys move focus up and down the items of a list.
- The ALT key in combination with the underlined mnemonic letter for a field or command button shifts the focus to that field or button.
- Either ENTER or the SPACEBAR activates your selection. For example, after pressing the TAB key to select Next in a wizard panel, press the SPACEBAR to display the next screen.
- SHIFT+F10 provides access to context menus.

Keyboard Navigation Within Dialog Boxes

Dialog boxes contain groups of controls necessary to set options or settings for programs. Here are some general rules about dialog box navigation:

- The TAB key moves focus between controls within the dialog box along a preset sequence.
- Controls displaying a mnemonic (an underlined letter) can be selected regardless of focus by typing ALT and the underlined letter.
- A dark border indicates the default command button. Press ENTER at any time to choose the button with a dark border.
- ESC chooses the **Cancel** button if one exists.
- SPACEBAR chooses a control you select with the TAB key.
- SPACEBAR changes the state of a check box that has focus. Typing a mnemonic (if one is available) will move the focus to the check box and change its state.
- Arrow keys move focus within radio buttons, list boxes, sliders, groups of option controls, or groups of page tabs.

- Items that cannot be changed are not visited by the TAB key sequence. Options that are unavailable are grayed-out and can neither be selected nor given focus.

While the controls described here are typically found in dialog boxes, they also can occur in other contexts. The same navigation standards will apply.

Tabbed Dialog Boxes

Some dialog boxes use tabbed pages to subcategorize groups of many options. Each tabbed page contains different groups of controls. Use TAB to move the focus between tabbed pages within a dialog box. Typing the mnemonic for a tab also moves the focus to the tabbed page and displays its page of controls.

The following table lists keyboard navigation rules within tabbed dialog boxes:

Keyboard Navigation Within Tabbed Dialog Boxes

Keyboard input	Result
CTRL+PAGE DOWN or CTRL+TAB	Switches to the next tab and displays the page.
CTRL+PAGE UP	Switches to the previous tab and displays the page.
RIGHT ARROW or LEFT ARROW	When the focus is on a tab selector, chooses the next or previous tab in the current row and displays the page.

List Boxes

List boxes display a column of available choices. There are different kinds of list boxes with additional navigation conventions:

- *Drop-down list boxes* by default show only the selected item. A small button to the right of the control shows a downward-pointing arrow. Select the arrow to display more items from the list box. If there are more choices than can fit in the preset list box area, a slider appears along the side of the list box. Show or hide the list using ALT+DOWN ARROW, ALT+UP ARROW, or F4. The TAB key selects an item.
- *Extended selection list boxes* support selecting single items, blocks of items, or combinations of the two. After selecting an item, hold down CTRL+navigation keys to select or clear additional items or blocks of items.

Support for Accessibility Settings

VERITAS software responds to operating system accessibility settings.

VERITAS products are compatible with Microsoft's accessibility utilities. In Windows 2000, accessibility options involving keyboard responsiveness, display contrast, alert sounds, and mouse operation can be set through the Control Panel.

▼ To set accessibility options

1. On the Start menu, select Settings, and then select Control Panel.

2. Select Accessibility Options.

Note You can also set accessibility options through the Accessibility Wizard. On the Start menu, select Programs, and then select Accessories. Select Accessibility, and then select Accessibility Wizard.

Note Though all graphics in VERITAS documentation can be read by screen readers, setting your screen reader to ignore graphics may improve performance.

Glossary

Advanced Reporting Option

A Storage Exec option that provides additional capabilities beyond what comes with Storage Exec. The Storage Exec Advanced Reporting Option enables users to create their own report queries, run and send reports by email after an alarm has been activated, produce reports in an Active HTML format, and run additional predefined reports.

alarm

The means by which Storage Exec identifies when some event occurs (such as a user attempting to store too much data in a folder or save an unapproved file type) and takes action (such as notifying the user about the event).

auto detect all users

A space allocation limit set on a folder so that a user who owns a file in the folder will automatically be assigned a space limit. If the auto detect all users space allocation is enabled, any new user who allocates space within the managed resource will be given a user space limit. This space limit is based on a predefined policy.

auto detect subfolders

Storage Exec applies a managed resource policy that the user selects to all subfolders of a folder (that is, a managed resource) that the user specifies.

auto detection

See auto detect all users and auto detect subfolders.

computer policy

A policy for applying managed resource policies to servers. A computer policy includes devices, folders under these devices, and managed resource policies. When a computer policy is applied to a server, the included managed resource policies are applied to that server's devices and folders.

disk space quota

The maximum size a managed resource can be before an associated Storage Exec space allocation alarm triggers.

Enterprise Administration Option

A Storage Exec option that enables enhanced reporting and the use of global policies on multiple computers.

exclude filter

Refines a file blocking policy on a set of folders within a managed resource. For example, you can exclude a specific subfolder from a folder (that is, a managed resource) that Storage Exec is monitoring.

file blocking

One of the key Storage Exec features: The ability to prevent users from storing data based on file type.

file group

A set of files that Storage Exec uses in its file blocking operations. A file group can contain one or more unauthorized file types, one or more authorized file types, and/or specific files to authorize or not authorize. For example, a graphics file group might contain unauthorized files with extensions *.jpg and *.bmp, but authorize the specific file `HomePage.jpg`.

file screening

Used by Network Appliance; a synonym for the term file blocking.

include filter

Refines a file blocking policy on a set of folders within a managed resource.

managed resource

A file, directory, share, or partition with a space allocation or file blocking policy associated with it.

managed resource policy

A set of space allocation or file blocking properties that help define a managed resource.

Network Appliance Option

The Storage Exec option that enables users to monitor and report on Network Appliance Filers.

notification

The means by which Storage Exec informs the user (by pop-up message and/or email) that an alarm has been activated.

overdraft limit

The amount of space by which the space allocation limit can be exceeded before Storage Exec takes action, such as issuing a notification. The space allocation limit will not be enforced until the space allocation limit plus the overdraft limit has been reached.

passive limit

A space allocation limit that, when crossed, Storage Exec notes but does not enforce. For example, a passive space allocation limit will notify users when they attempt to store too much data, but will not prevent them from storing the data.

policy

See computer policy and managed resource policy.

preferred computer

Computers included in a preferred group for quick access.

preferred group

A named logical entity that contains one or more computers. Creating a preferred group groups commonly used computers in one place.

propagation

The process by which changes are automatically spread throughout Storage Exec. For example, after a managed resource policy (space allocation or file blocking) becomes part of a managed resource, all future changes to the policy are reflected in the managed resource. Also, if you are running the Storage Exec Enterprise Administration Option and change a managed resource policy in the central repository, Storage Exec automatically makes that change in each managed resource that uses the policy, regardless of what computer the managed resource resides on.

quota

A synonym for disk space quota.

Remote Server Agent

A Storage Exec agent that enables users to perform space allocation and file blocking on Windows-based servers.

Remote Workstation Agent

A Storage Exec agent that enables users to perform file blocking on Windows-based workstations.

report query

Defines the content and appearance of a report.

scoping

If you are running the Storage Exec Enterprise Administration Option, managed resource policies stored in the central repository will be available to every computer that uses the repository. Also, a managed resource policy created on a computer in the central repository will be available to only that computer's managed resources. Other computers in the central repository's domain will not be able to see or use that managed resource policy.

space allocation

One of the key Storage Exec features: The ability to limit the amount of data stored in resources that Storage Exec manages. Storage Exec can enforce limits on individual users or on a file, folder, or partition.

space allocation limit

A synonym for disk space quota.

SRM

Acronym for storage resource management.

storage resource management

An element in an organization's efforts to keep its computers available for business functions. Storage Exec helps organizations achieve this goal by enabling them to prevent folders from getting too large, block unwanted files from being stored, and run reports that report on disk consumption.

threshold

The amount (or percentage) of disk space that can be used before a Storage Exec space allocation alarm triggers.

Index