

HP OpenView Storage Data Protector Media Operations User's Guide

Manual Edition: September 2004



i n v e n t

Manufacturing Part Number: B7128-90003

Release 5.5

© Copyright 2004 Hewlett-Packard Development Company, L.P.

Legal Notices

© Copyright 2004 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

UNIX® is a registered trademark of The Open Group

Microsoft®, Windows® and Windows NT® are U.S. registered trademarks of Microsoft Corporation.

Java™ is a U.S. trademark of Sun Microsystems, Inc.

1. Media Operations Overview

In This Chapter	2
Audience for This Manual	3
Media Operations Concepts.	4
Media Lifecycle	4
Backup Manager Integration.	6
Integration via XML Gateway	6
Integration via XML File Import	8
Components.	8
User Interface	9
Windows Client	9
Web Client	10
Environmental Requirements.	11
Platform Support	11
Barcode Scanner Support.	11
Barcode Printer Support	12
Offsite Vendor Support.	12
Supported Languages.	13
Key Media Operations Features and Benefits	14
Controllable.	14
Efficient:.	14
Resilient.	14
Available:.	14
Extensible	14
Scalable:.	14

2. Getting Started Using Media Operations

Chapter Overview	18
Using Media Operations	19
Connecting to a Server	19
Recent Tab	19
TCP/IP Tab	19
Custom Tab	19
Logging On to Media Operations	20
Logging On to Media Operations Manager	20
Logging On to Media Operations Web Interface	21
Adding Sites and Backup Managers	22
Add Site Wizard	23

Contents

Add Backup Manager Wizard	36
Editing an Existing Site	43
Info	43
DNS	44
Vaults	45
Data Centers	48
Vaulting Policies	50
Offsite Vendors	53
Users	57
Remote Accounts	59
Import Data	60
Deleting a Site	63
Editing a Backup Manager	63
XML Gateway Group	64
Deleting Backup Manager Objects	68

3. Configuring Media Operations

Chapter Overview	72
Configuring for the Physical Environment	73
Site Management	73
Adding a Site	73
Editing a Site	74
Vaults	75
Offsite Vendors and Accounts	76
Data Centers	77
Grids	77
Security Management	78
Product Administrators	78
Top-Level Administrator	78
Site-Level Administrator	79
Super Operator-Level Administrator	79
Operator-Level Administrator	80
Remote Accounts	80
Configuring Backup Processes and Objects	81
Automatic Backup	81
Manual	82
Process Flow — Manually Created Environments	82
Implementing the Manual Backup Process	84

Backup Managers	84
XML Gateway Interface	85
XML File Import Directory	88
Database Backup	89
Tuning Backup Objects	89
Refining Physical Locations	89
Refining Media Compressions	90
Adding and Modifying Media Types	90
Defining Policies	92
Configuring Media Vaulting Policies	92
Media Vaulting Policy Hierarchy	93
Basic Vaulting Policy Concepts	94
Vaulting Templates	95
Active Vaulting Policies	95
Defining Barcode Labeling Policies	98
Configuring Scratch Media Policies	99
Configuring Premount Jobs	99
Tuning Scratch Media Levels	100
Understanding Reactive Mount Requests	100
Server Parameters	101
Vaulting Jobs	103
Scratch Bin Maintenance	103
Premount Jobs	103
Audit History	103

4. Performing Daily Media Operations

Overview	106
Job Status Indicators	107
Premount Jobs	108
Premount Job Listing	109
Scratch Listing	109
Confirmation	110
Mount Listing	111
Dismount Listing	111
Load/Eject Media	112
Free/Scratch Pool Handling	114
Vaulting Jobs	115
Vaulting Job Listings	116

Contents

Vaulting Job Confirmation	117
Containers	121
Multiple Users	122
Multiple Sites	122
Scratch Media	124
Scratch Jobs Listing	125
Scratch Bin Job Confirmation	127
Containers	129
Multiple Users	130
Multiple Sites	130
Scratch Init	131
Initializing a Standalone Drive	131
Initializing Using a Barcode Library	132
Media Reorder	133
Configuring	134
Confirmation	135
Checkout Request (COR)	137
Submit a Checkout Request	137
Checkout Request Job Listing	139
Checkout Request Confirmation	140
Containers	141
Multiple Users	141
Multiple Sites	142
Exception	143
Mount Request	144
Mount Request Listing	144
Mount Request Job Confirmation	145
Manual Vaulting Jobs	146
Viewing Job History	147
History	147
Web Interface	149

5. Status and Reporting Interfaces

Overview	152
Viewing Current SLA Status	153
SLA Status Configuration	158
Viewing Alerts	161
Reports	163

Contents

Vault Audit	163
Scratch Media	164
Media Movement	164
Additional Reports	165
Backup Media History	165
Notifications	166
Configuring Notification Interfaces	166
Email Interface Configuration	167
OVO Interface Configuration	167
Configuring Notification Triggers	168
Alerts	168
SLA	169
Jobs	170
Metrics	171
Metric Report Description	173
Job Status	173
Job Metrics	174
Pool Health Metrics	175
Premount Metrics	175
Vaulting Metrics	176
Scratch Metrics	177
Remote Metrics	177
Vendor Metrics	177
Vault Metrics	178
Location Metrics	178
Location Audits	179
Select Site	179
Select Location	179
Scratch Bin	180
COR Holding Area	180
Device/Vault	181
Holding Bin	182
View	183
Query	184
Print	184
Reset Audit Flags	185
Audit Highlighted	185
Import Export	185

Contents

Export Remote Account Report	185
Import Offsite Vendor File	186
Import Audit List	186

A. Installing and Licensing

Installing the Media Operations Server	188
Installation Overview	188
Installing Media Operations	189
Installing Media Operations Manager Overview (Optional)	191
Installing the Media Operations Manager	191
Installing XML Gateway Overview	193
Installing XML Gateway on Windows	193
Installing DP XML Gateway on HP-UX	194
Prerequisites	194
Installation	194
Uninstall	195
Installing XML Gateway onto Sun/Solaris	195
Prerequisites	195
Uninstall	196
Licensing Media Operations	197
Viewing Licences	198

B. External Interfaces

Overview	200
XML File Import Interface	201
File Import	201
Creating Files	201
Usage	202
XML Import File Format	202
XML Offsite Vendor Interface	203
Usage	203
Generic Input Parameters for All Request Types	204
Media Transit Requests	205
Request and Receive Audit Requests	205
Status Checking Requests	206
XML Offsite Vendor File Format	206
Reactive Mount Request Utility	206
Bulk Configuration File Import	213

Data Center Grids.	213
System Grid Locations	213
Media Locations	213
Device Definitions.	214
Import Manual Media.	214

C. Diagnostics and Tuning

Overview.	218
Media Operations Server Logs	219
Media Operations Manager Logs	219
XML Gateway Configuration, Logs, and Tuning	220
Configuration	220
XML Gateway Configuration File	220
Cleanup	221
File Locations	221
Logging	221
Threading	222
Logs	222
Log Levels	223
Kernel Tuning for XML Gateway on HP-UX	223
Data Management Communications	224
Service Logs	224
Changing the Logging Level.	224
Log File Locations	225
Changing Communications Port Numbers	225

D. Application Managers

Overview.	228
Scratch Init	228
Load Eject	228
Copy Support.	228
Mixed Pools	229
Media Subtype	229
Location Update	229
Remote Gateway.	229
HP OpenView Omniback/HP OpenView Storage Data Protector	230
VERITAS NetBackup	230
Virtual Media	230

Contents

Permissions	230
Initialization	230
Silo	231
Gateway Configuration File	231

Glossary

1 Media Operations Overview

In This Chapter

Media Operations Manager is a graphical management interface for the HP OpenView Storage Data Protector Media Operations product and provides the ability to remotely configure, monitor, and run your media vaulting and scratch media policies.

The *HP Media Operations User's Guide* describes how to configure and use the Media Operations product. Before you can configure Media Operations, it must be properly installed. See “Installing and Licensing” on page A-187.

This chapter consists of the following topics:

“Audience for This Manual” on page 3

“Media Operations Concepts” on page 4

“Environmental Requirements” on page 11

“Key Media Operations Features and Benefits” on page 14

Audience for This Manual

This manual is intended for network administrators responsible for maintaining and backing up systems. There are four levels of administrators with varying security/access levels:

- top-level administrator
- site-level administrator
- super operator-level administrator
- operator-level administrator

See “Security Management” on page 78 for a detailed description of administrators and their functions.

Media Operations Concepts

HP OpenView Storage Data Protector Media Operations is a software product that provides tracking and management of offline storage media, such as magnetic tapes, resulting in more reliable backups, faster data recovery, improved staff efficiency, and reduced costs. Unlike homegrown tools, Media Operations offers a professional solution for IT operations that manages thousands of removable media. It tracks all media, whether online, offline or offsite, ensuring vital data is never lost. Data retention and media recycling policies are enforced for assured service quality. To guarantee backup success, Media Operations monitors media quality and preloads libraries with the required number of scratch tapes.

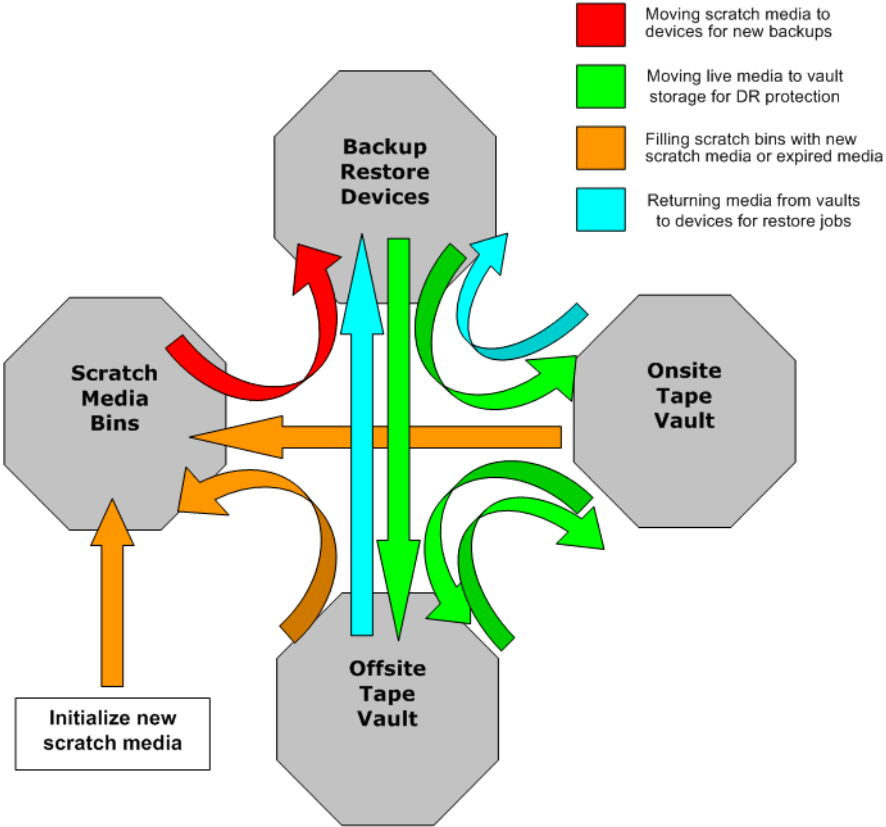
Unlike competing products, Media Operations maximizes the effectiveness of media procedures by creating daily task lists, organizing tapes for logical data center walk-throughs, and enabling operator control of tape libraries, barcode scanners, and media label printers.

Media Lifecycle

Media Operations is designed to allow management of the end-to-end lifecycle of a physical piece of removable medium (see Figure 1-1 on page 5). This lifecycle does not include the lifecycle of the data held on the medium; this is the responsibility of the Backup Manager that wrote the data to the medium. The Media Operations product scope does not overlap with the data retention policies managed by the Backup Manager. The scope of the physical media lifecycle includes:

- Moving live media from backup/restore devices (tape libraries and standalone tape drives) to onsite or offsite tape vaults for disaster protection.
- Moving scratch media from scratch bins into backup/restore devices to provide usable media for upcoming backup jobs. The scratch media in the scratch bins are generated by returning expired media from the tape vaults back to the scratch bins and by creating new scratch media as needed.
- Moving live media from onsite or offsite tape vaults to backup/restore devices to meet recovery requests.

Figure 1-1 Media Lifecycle



Backup Manager Integration

Media Operations integrates with the Backup Manager in two ways:

- Integration between Media Operations and the Backup Manager via the XML Gateway
- Integration via XML file import

Media Operations uses these Backup Manager integration interfaces to extract configuration information from the Backup Manager, which autoconfigures devices, media pools, systems, and backup specifications. In addition, it extracts current media information. The XML Gateway interface also allows Media Operations to trigger barcode and media scans in any of the Backup Server's tape libraries/devices. This ensures the up-to-date information is available on the current contents of these devices. It uses library mail slots to move media into and out of the library.

Integration via XML Gateway

Media Operations provides an integration interface called the XML Gateway that links Media Operations directly with supported Backup Managers (such as HP OpenView Storage Data Protector or VERITAS NetBackup). This type of interface provides the fastest response time, because it is a request-response type of interface rather than polling. It does not require any complex communication path setup, because it runs over a standard HTTPS connection, which normally passes through firewalls without any special configuration.

Media Operations specifies which Backup Manager to connect to and specifies all required security parameters; therefore, the XML Gateway does not require any configuration.

If the XML Gateway supports remote connectivity, you can install the XML Gateway directly on the Backup Manager (such as the HP OpenView Storage Data Protector Cell Manager) as well as onto the Media Operations Server or another server.

NOTE

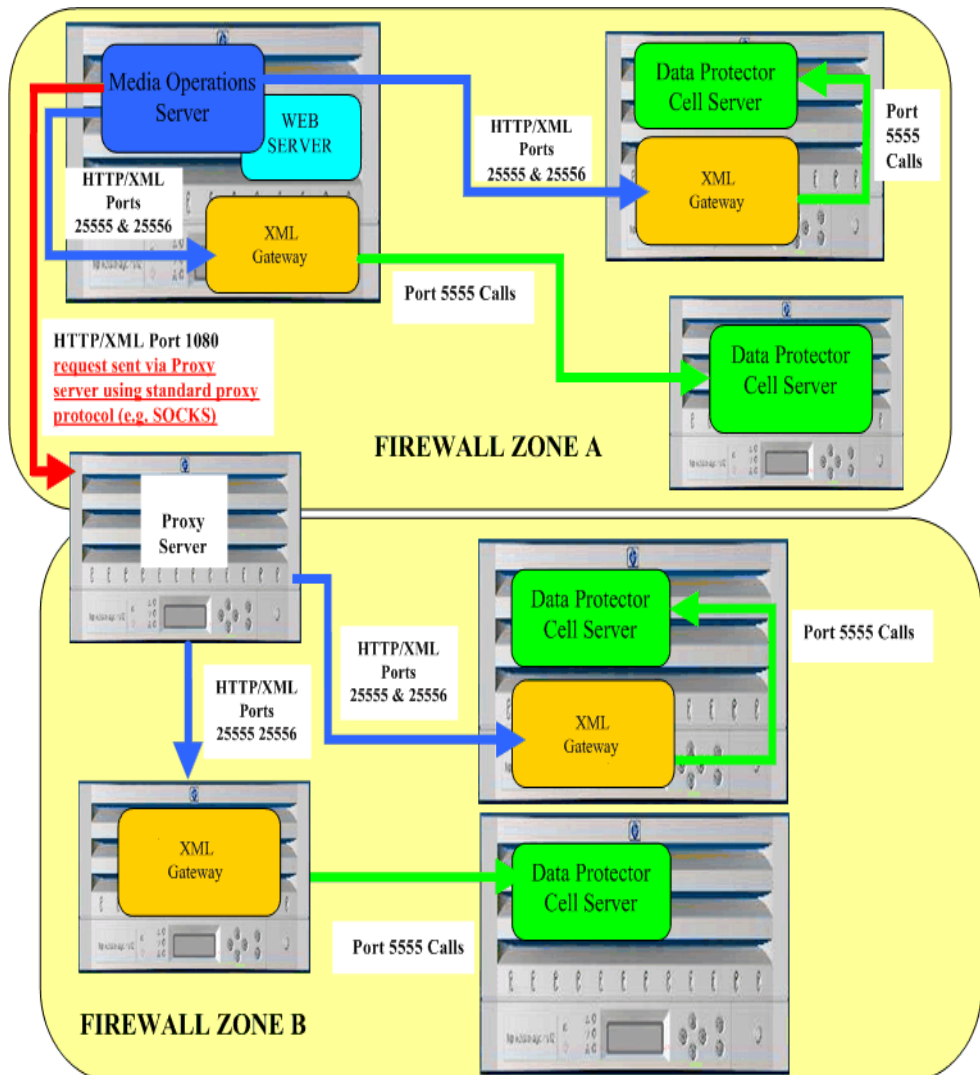
Communication between the XML Gateway and Data Protector does not normally pass through firewalls, so the XML Gateway running on the Media Operations Server or another server can only communicate with a Backup Manager within the same firewall zone.

If the XML Gateway and Data Protector Cell Manager are behind a firewall, the Media Operations Server must communicate with the XML

Gateway by passing requests on to the XML Gateway via a Proxy Server (such as SOCKS).

The following diagram shows the various deployment options for the XML Gateway with a Media Operations Server managing media from multiple site locations (each site with its own firewall).

Figure 1-2 Media Operations Deployment Options with Data Protector



NOTE

VERITAS NetBackup master server commands must be executed locally on the master system. Because of this, the XML Gateway must be installed on the VERITAS NetBackup master server's system.

If the XML Gateway does not support remote connectivity, you can only install off the Backup Manager and nowhere else.

Integration via XML File Import

Media Operations supports an alternative interface method (see “External Interfaces” on page B-199) that allows integration with other types of Backup Servers that are not supported by the XML Gateway. This file-import interface uses files formatted in HTTP/XML protocol.

- Backup/Restore Device Information file
- Media Pool Information file
- Backup Specification Information file
- Backup Manager Configuration Information file
- Media Information file
- Used Media Information file

Components

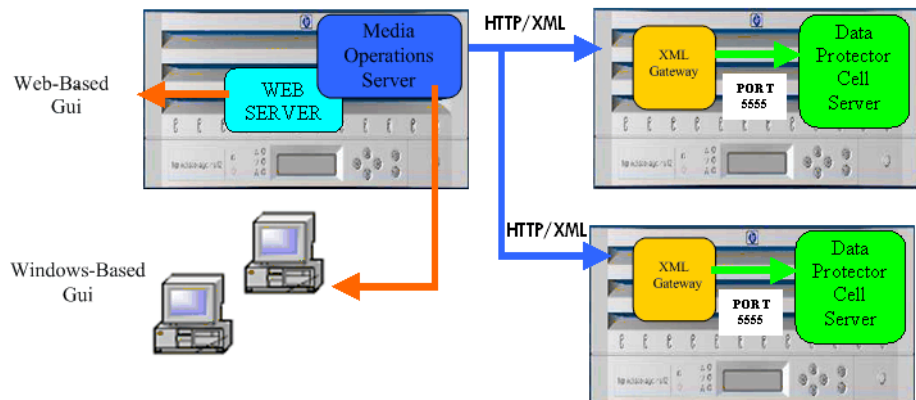
The following diagram shows the major components of the Media Operations product, including:

- **Media Operations Server:** The server is the core component of the Media Operations solution and contains the database that stores the various data objects (devices, media pools, media, and so on) and their attributes. In addition, it contains all of the business logic to process the administrator-defined vaulting and scratch policies, and convert these into lists of tape movements to be performed. All scheduling and service level agreement (SLA) monitoring functions are also contained in the server.
- **Media Operations Manager Systems:** The client graphical user interface (GUI) provides administrative and user functions remotely from the server. Windows-based and web-based versions of the GUI are available for day-to-day operations. The Media Operations Manager also provides the ability to attach a barcode scanner to the

client system in order to input barcodes from large numbers of media as they are moved from physical location to physical location.

- **XML Gateway:** A component that provides tight integration between Media Operations and Backup Managers. For Media Operations 5.5, the XML Gateway supports HP OpenView Storage Data Protector 5.5, 5.1, 5.0 and its predecessor HP OpenView Omniback 4.1. VERITAS NetBackup 4.5 is also supported. An XML file import interface is provided to facilitate integration of Backup Managers not currently supported by the XML Gateway.
- **Backup Manager:** After installing the Media Operations software on the Media Operations Server System, you can track media from a variety of Backup Managers. A Backup Manager is the product that controls backup functions (such as HP OpenView Storage Data Protector). Media Operations interacts with Backup Managers to track and provide for medium use.

Figure 1-3 Components



User Interface

Media Operations provides graphical user interfaces (GUIs) that are available from the client system (Windows client) and from the internet (web client).

Windows Client

The graphical user interface is provided for Microsoft Windows 98, NT,

and 2000 platforms.

Through its graphical user interface, Media Operations allows you to administer your complete media lifecycle environment from a single system. Your interface does not have to be used from the Server System; you can install it on your desktop system.

For ease of operation, you can install the GUI on various systems, allowing multiple users to access Media Operations via their locally installed consoles.

Web Client

In addition to the Windows-based graphical user interface, a web-based GUI is available. The web client provides operator functions only. Site configuration functions must be performed from the Windows client.

Environmental Requirements

The following environmental requirements are described in this section:

- “Platform Support” on page 11
- “Barcode Scanner Support” on page 11
- “Barcode Printer Support” on page 12
- “Offsite Vendor Support” on page 12
- “Supported Languages” on page 13

Platform Support

Table 1-1

Host	Operating System Platforms	Supported Processor Platforms
Media Operations Server	Windows NT (service pack 6 or above) Windows/2000 Advanced Server Windows 2003	Intel, AMD, IA-32 systems Intel, AMD, IA-32 systems Intel, AMD, IA-32 systems
XML Gateway	HP/UX v11.x and above Windows NT (service pack 6 or above) Windows/2000 Server and Advanced Server Windows 2003 Solaris v7, v8 and v9	PA-RISC systems Intel, AMD, IA-32 systems SPARC systems
Media Operations Manager	Windows/98 (2nd edition) Windows/NT Workstation (service pack 6 or above) Windows/2000 Professional Windows 2003 Windows/XP	Intel, AMD, IA-32 systems Intel, AMD, IA-32 systems Intel, AMD, IA-32 systems Intel, AMD, IA-32 systems Intel, AMD, IA-32 systems
Media Operations web client	Internet Explorer v5.x and above Netscape Navigator v7.0 and above	Intel, AMD, IA-32 systems Intel, AMD, IA-32 systems and PA-RISC systems

Barcode Scanner Support

The Media Operations Server supports any barcode scanner that behaves like a keyboard and emulates `Enter` (not carriage return) after scanning.

Barcode Printer Support

The Media Operations Server supports the following barcode label printer models. These barcode label printer models are also supported when attached to a supported Media Operations Manager (see Table 1-1 on page 11).

- any Zebra 300dpi label printer

The Media Operations Server supports the following tape libraries for use with the barcode labels it prints: (Other libraries are not supported.)

- HP SureStore 2/20, 4/40, 6/60, 10/100, 6/140, 10/180, and 20/700 libraries
- HP StorageWorks SSL, MSL, and ESL libraries

See “Defining Barcode Labeling Policies” on page 98 for more information regarding barcode support.

Offsite Vendor Support

Media Operations supports electronic links to offsite vendors. This electronic link allows Media Operations to send electronic verification of media being shipped to offsite storage and also provides electronic requests to return media from offsite storage to the data center (such as for recovery jobs). This provides a more reliable link to the offsite vendor than tracking media in and out of vendor storage via paper lists.

You have the ability to add your own offsite storage vendors and accounts manually, and then select these custom offsite locations as part of the media vaulting policies.

There are three offsite vendor types:

- **Media Operations:** A Media Operations vendor type is used when the offsite vendor is using Media Operations to manage their offsite media storage. The electronic link is between your Media Operations Server and the offsite vendor’s Media Operations Server.
- **Generic:** A generic vendor type is used for all other non-Media Operations vendors, including offsite vendors that have their own proprietary electronic link interface. When configuring offsite accounts for such an offsite vendor, you can write scripts to take information from Media Operations and convert it to your offsite vendors electronic link protocol.

- **Iron Mountain:** An Iron Mountain vendor type is used when the offsite vendor is using Iron Mountain to manage their offsite media storage.

Supported Languages

Media Operations Clients and Servers in languages that use Western European character sets (such as ISO extended ASCII) can communicate with one another with no issues. Media Operations Clients and Servers in languages that use double-byte character sets (for Media Operations 3.0, only SJIS (Japanese) and EUC-KR (Korean) are supported) can communicate successfully only with another Media Operations installation using the same character set. This means Japanese clients must link to Japanese servers, Korean to Korean, and so on.

Table 1-2

Client/Server

Client Locale	Server Locale
Shift JIS (Japanese)	Shift JIS (Japanese)
EUC-KR (Korean)	EUC-KR (Korean)
Western/US	Western/US

The following matrix applies to intersite transfers between two Media Operations Servers where one server acts as an offsite location to the other server.

Table 1-3

Server-to-Server Transfer Support Matrix

Source	Destination
Shift JIS (Japanese)	Shift JIS (Japanese)
EUC-KR (Korean)	EUC-KR (Korean)
Western/US	Western/US
Western/US	Shift JIS (Japanese)
Western/US	EUC-KR (Korean)

Key Media Operations Features and Benefits

Controllable

Efficient:

- creates daily task lists and organizes tapes for logical data center walk-throughs
- empowers operator control of removable backup devices for tape loads and ejects
- automates data exchange with backup applications, offsite vaulting services, and removable media suppliers
- supports barcode scanners and media label printing

Affordable:

- eliminates the cost of supporting homegrown tools for less than 3% of your total media bill

Resilient

Available:

- accurately tracks all media regardless of location

Recoverable:

- enforces data retention and media recycling policies
- ensures backup completion through library preloads

Extensible

Scalable:

- tracks from tens to hundreds of thousands of individual pieces of medium

Flexible:

- works with HP OpenView Storage Data Protector and other leading backup and recovery applications

Media Operations Overview

Key Media Operations Features and Benefits

Chapter Overview

- First properly install the Media Operations software. See “Installing and Licensing” on page A-187.

This chapter helps you get started using Media Operations by describing the steps required to begin using the Media Operations Server. This chapter describes a few key areas to get you started:

- “Connecting to a Server” on page 19
- “Logging On to Media Operations” on page 20
- “Adding Sites and Backup Managers” on page 22
- “Editing an Existing Site” on page 43
- “Editing a Backup Manager” on page 63

Using Media Operations

Connecting to a Server

To launch the Media Operations Manager, double-click the Media Operations Manager icon that is now on your desktop. You will see the 4D Server Connection screen containing three tabs (see Figure 2-1 on page 20):

Recent Tab

The `Recent` tab lists all the Media Operations Servers used recently. The list is sorted alphabetically. To connect to a server from this list, double-click its name, or select it and click `OK`.

To remove a server from the list, select it and press `Delete` or `Backspace`.

TCP/IP Tab

The Media Operations Server includes a built-in TCP/IP broadcasting system that publishes the name of the server databases over the network. These names are listed under the `TCP/IP` tab.

The list is sorted alphabetically. To connect to a server from this list, double-click its name, or select it and click `OK`.

Custom Tab

The `Custom` tab allows you to assign a published server on the network using its IP address and attribute a customized name to it.

If your Media Operations Manager is in a different network subnet from the Media Operations Server, your network router connecting the two subnets may be configured to block TCP/IP broadcasts. In this case, the Media Operations Server name will not appear under the `TCP/IP` tab on the client side. However, if you know the IP address of the server whose name is not broadcast, you can type its IP address.

- `Database name` — lets you define the name of the server database, which is used under the `Recent` tab when referring to the database.
- `Network address` — lets you type the IP address of the machine

Getting Started Using Media Operations Using Media Operations

where the server was launched.

By default, the publishing port of the server is 19813.

NOTE

If a database was selected under the `Recent` or `TCP/IP` tab at the moment you clicked the `Custom` tab, the two fields display the corresponding information.

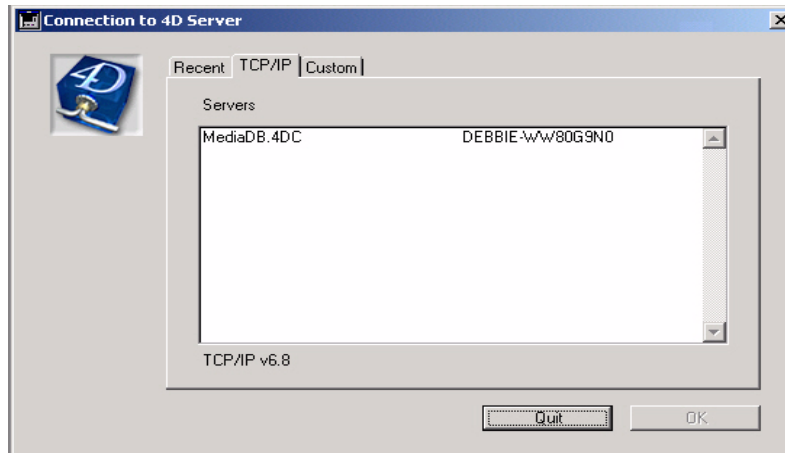
Once this tab assigns a server, click `OK` to connect to the server. The server is then listed under the `Recent` tab.

Logging On to Media Operations

Logging On to Media Operations Manager

Double-click the `Media Operations Manager` icon on your desktop. You will see the `4D Server Connection` screen.

Figure 2-1 4D Server Connection Screen

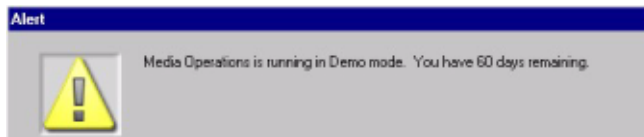


Select the server to which you want to connect from a list of recently used servers, the `TCP/IP` address, or a custom server. The `User Log In` screen appears. Type your username and password, and click `Sign In`.

If you are running `Media Operations` in “demo” mode and you have media configured in `Media Operations`, you will receive an alert telling you how many days are left before the product is switched to “expired” mode (see “`Licensing Media Operations`” on page A-197).

Figure 2-2

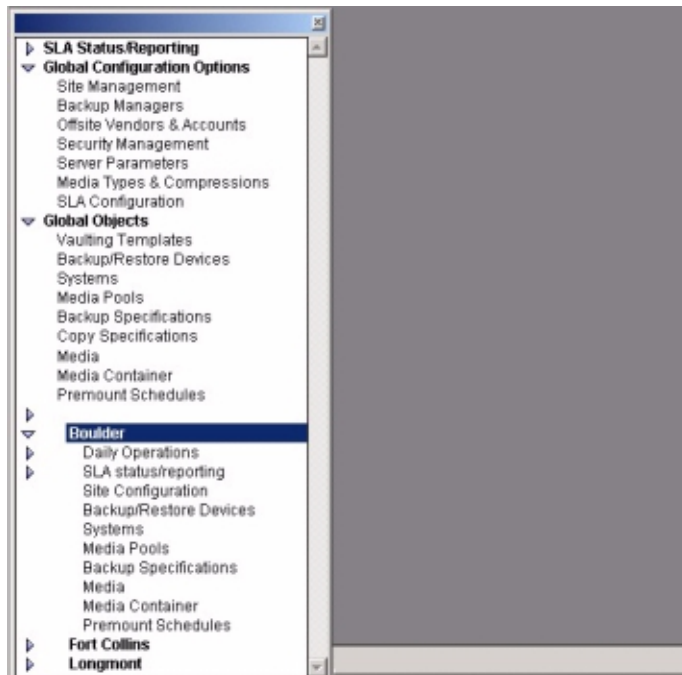
Alert



You are now at the Media Operations graphical user interface (GUI).

Figure 2-3

Media Operations Graphical User Interface



Once you have successfully installed the Media Operations software and logged on, create a site as described in the following sections.

Logging On to Media Operations Web Interface

1. Start Media Operations.
2. From another computer, launch a web browser (such as Netscape or Microsoft Internet Explorer).
3. Type the network name or IP address of your Media Operations Server in the Location area of the web browser. See important note

Getting Started Using Media Operations Using Media Operations

below.

The web version of Media Operations appears.

4. Type your login name and password on the web browser.

IMPORTANT

If the Media Operations Server is running on a system that also hosts another web server, make sure to type the network name or IP address followed by a colon 3612. For example:

`http://worker.xyz.ab.com:3612`

Adding Sites and Backup Managers

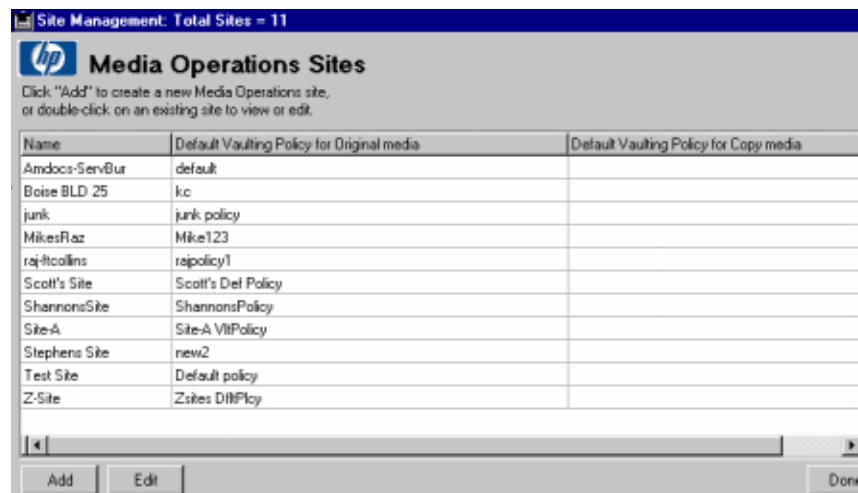
The design of Media Operations allows you to manage physical media policies across multiple physical sites.

Global Configuration Options > Site Management allows you to create, modify, and delete the sites the Media Operations Server manages.

If you have no sites configured, you will be automatically taken to the Add Site Wizard screen when you log in. To create additional sites, go to Global Configuration Options > Site Management. You will see the Media Operations Sites screen.

Figure 2-4

Media Operations Sites Screen



The screenshot shows the 'Media Operations Sites' screen with a table listing sites and their vaulting policies. The table has three columns: Name, Default Vaulting Policy for Original media, and Default Vaulting Policy for Copy media. Below the table are 'Add', 'Edit', and 'Done' buttons.

Name	Default Vaulting Policy for Original media	Default Vaulting Policy for Copy media
Amdocs-ServBur	default	
Boise BLD 25	kc	
junk	junk_policy	
MikesFlaz	Mike123	
raj@collins	rajpolicy1	
Scott's Site	Scott's Def Policy	
ShannonsSite	ShannonsPolicy	
Site-A	Site-A_VitPolicy	
Stephens Site	new2	
Test Site	Default_policy	
Z-Site	Zsites DfNPloy	

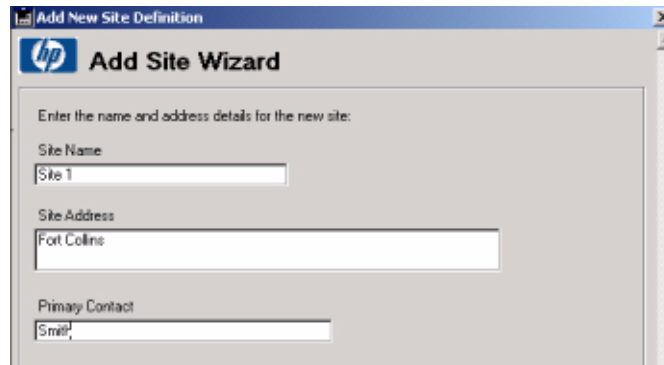
Click **Add** to add a new site or **Edit** to edit an existing site. The **Add**

Site Wizard screen is displayed.

Add Site Wizard

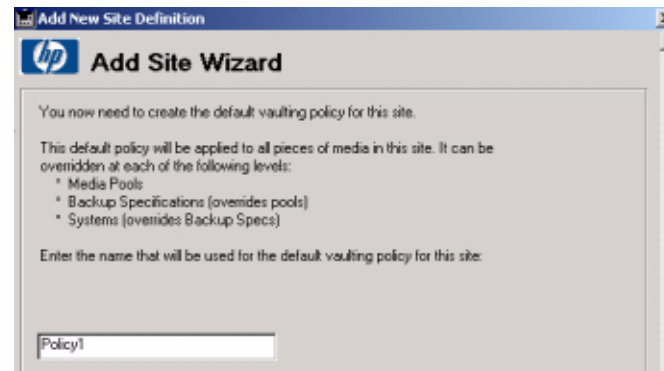
When you click Add, you will see the Add Site Wizard screen.

Figure 2-5 Add New Site Definition



Type a site name, site address, and primary contact. Click **Next** to create the default vaulting policy for the new site.

Figure 2-6 Create a Default Vaulting Policy



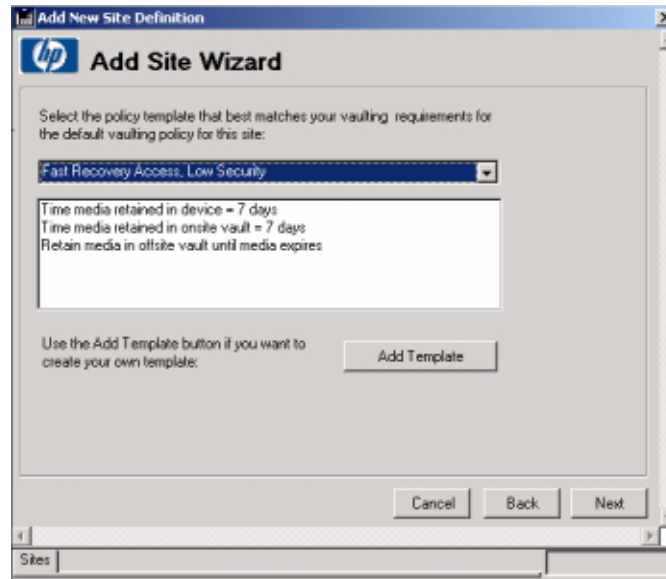
This default vaulting policy is applied to all media for this site. It can be overridden at each of the following levels:

- media pools
- backup specifications (overrides media pools)
- system (overrides backup specifications)

Getting Started Using Media Operations Using Media Operations

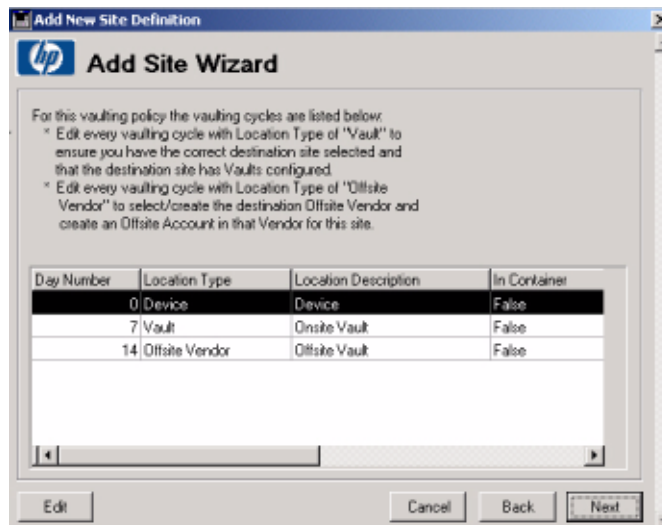
Type the name of the new defined vaulting policy for this site. Then click **Next** to select a vaulting policy for the new site.

Figure 2-7 **Select a Policy Template**



Select a policy template from the drop-down list or click **Add Template** to define your own policy. Once you have selected the policy template, click **Next** to edit the vaulting cycles.

Figure 2-8 Vaulting Cycle



Edit the location type to ensure you have the correct destination site selected and the destination site has vaults configured. To edit the location type and location destination, you can double-click Location Type or Location Description, or click Edit. You will be taken to the Vaulting Cycle Action screen. You will need to add an offsite vendor if one has not been defined.

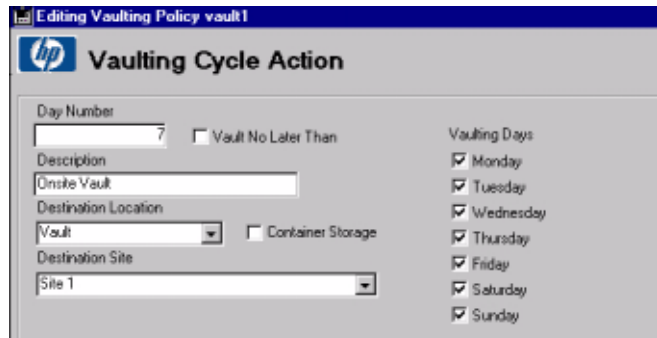
NOTE

If you attempt to advance by clicking Next without editing the vaulting cycles with an offsite vendor destination, you will receive the following alert.



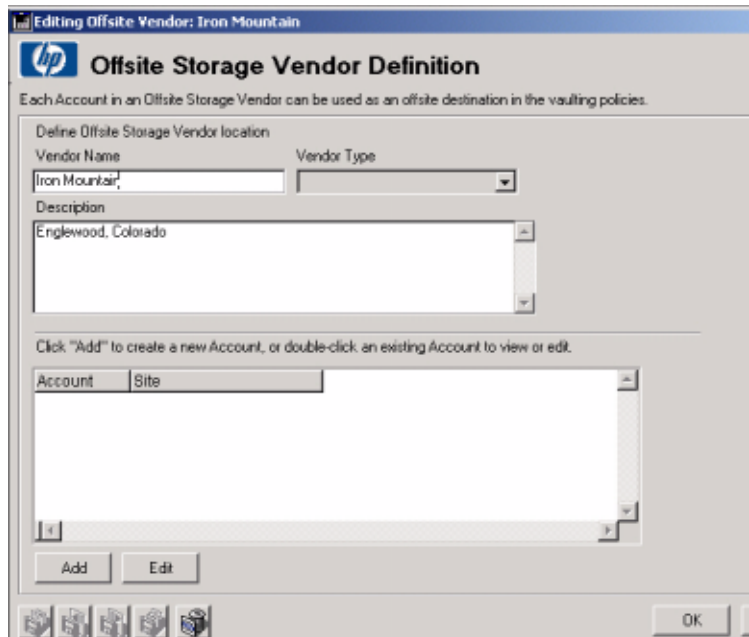
You now need to edit the vaulting cycle referred to in the alert either by double-clicking on that cycle on the list, or by selecting it on the list and clicking Edit.

Figure 2-9 Vaulting Cycle Action Screen



This vaulting cycle has an offsite vendor destination, so you need to define the destination offsite vendor and an offsite vendor account. To do this, select an offsite vendor for `Destination Offsite Vendor`. Once you have chosen a vendor, select an offsite vendor account. Since you are adding a new site, there are no offsite vendors defined and you will need to create them. To add an offsite vendor, click `Add Offsite Vendor`. You will go to the `Offsite Storage Vendor Definition` screen.

Figure 2-10 Offsite Storage Vendor Definition Screen



Type the vendor name. Select the vendor type. Type the contact details. Select the address.

There are three offsite vendor types:

- **Media Operations:** A Media Operations vendor type is used when your offsite storage location is another Media Operations Server. With this vendor type, there is an automatic electronic link between the two Media Operations Servers, which automatically creates jobs on the offsite server for outgoing and returning media, and provides status information on the offsite portion of jobs. In addition, there are auditing options that allow you to synchronize the two Media Operations Servers if they get out of sync for any reason.
- **Generic:** A generic vendor type is use when your offsite storage location is not another Media Operations Server. This type of vendor may have its own proprietary electronic link interface. When configuring offsite accounts for such an offsite vendor, the Media Operations administrator can write scripts to take information from Media Operations and convert it to the offsite vendor's electronic link protocol.
- **Iron Mountain:** An Iron Mountain vendor type is use when your offsite vendor is Iron Mountain and you are using Iron Mountain FTP electronic link (SecureBase). (Note) if you are not using the FTP link, use the generic vendor type.

Click Add to create one or more accounts in this new offsite vendor. You will be taken to the Vendor Account Definition screen. (There are three types of screens depending on the offsite vendor type you have selected.)

Figure 2-11 Vendor Account Definition for Media Operations Type Screen

The screenshot shows a dialog box titled "Editing Offsite Vendor: Iron Mountain" with the HP logo and "Vendor Account Definition" header. It contains three main sections: "Define vendor account" with fields for "Account ID" (IM0001) and "Site" (Fort Collins); "Define which days of the week media is sent offsite to the vendor" with a "Vaulting Days" section where all days (Monday through Sunday) are checked; and "Define interface to Offsite Media Operations Server" with fields for "Hostname" and "Account Password". At the bottom are buttons for "Request Audit", "Resend Offsite Media", and "OK".

If you are creating an account for a Media Operations type of offsite vendor, type the account ID, hostname (defines the system name of the Media Operations Server being used to store the offsite media), and password. To authenticate this interface, the account ID is used as the username and an account password must also be typed. This account ID and password must also match a remote account on the offsite Media Operations Server. If the connection to your offsite Media Operations Server passes through a firewall, you can type the proxy settings for this connection.

The `Vaulting Days` check boxes allow you to define any restrictions on the days of the week the vendor will accept offsite shipments. Vaulting days on this screen takes precedence over vaulting days set in Vaulting Policies (see “Vaulting Policies” on page 50).

Figure 2-12 Vendor Account Definition for Generic OSV Type Screen

The screenshot shows a Windows-style dialog box titled "hp Vendor Account Definition". The window title bar reads "Editing Offsite Vendor: Iron Mountain ML". The dialog is divided into several sections:

- Define vendor account:** Includes an "Account ID" text field and a "Site" dropdown menu currently set to "Site1".
- Vaulting Days:** A group box containing seven checked checkboxes for "Monday", "Tuesday", "Wednesday", "Thursday", "Friday", "Saturday", and "Sunday".
- Offsite Vendor Proxy Settings:** A group box containing:
 - "Proxy Type" dropdown menu set to "No Proxy".
 - "Proxy Port" text field with "0".
 - "Proxy Hostname" text field.
 - "Proxy Username" and "Proxy Password" text fields.
- Define interface to Offsite Storage Vendor:** A group box containing four sections, each with a text field and an "Enabled" checkbox:
 - "Outgoing Media command line script" (checkbox is disabled).
 - "Return Media command line script" (checkbox is disabled).
 - "Status Verification command line script" (checkbox is disabled).
 - "Audit Management command line script" (checkbox is disabled).

At the bottom of the dialog are four buttons: "Request Audit Listing", "Send Audit Listing", "OK", and "Cancel".

If you are creating an account for a generic type of offsite vendor, type the account ID. If your offsite vendor supports some or all of the electronic link capabilities, you can enable them and type the scripts you have written that connect the Media Operations offsite vendor API to your offsite vendors propriety protocols. If the connection to your offsite vendor passes through a firewall, you can type the proxy settings for this connection.

1. Select the Enabled check box for Outgoing/Return Media command line script if the offsite storage vendor supports an interface to manage outgoing and returning media. Then type the script/utility command line to link Media Operations to the vendor.
2. Select the Enabled check box for Status Verification command line script if the offsite storage vendor supports an interface to notify when previously submitted outgoing and returning media jobs are complete. Then type the script/utility command line to link Media Operations to the vendor.
3. Select the Enabled check box for the Audit Management command

Getting Started Using Media Operations Using Media Operations

line script if the offsite storage vendor supports an interface to audit stored media. Then type the script/utility command line to link Media Operations to the vendor.

The Vaulting Days check boxes allow you to define any restrictions on the days of the week on which the vendor will accept offsite shipments. Vaulting days on this screen takes precedence over vaulting days set in Vaulting Policies (see “Vaulting Policies” on page 50).

Figure 2-13 Vendor Account Definition for Iron Mountain Type Screen

The screenshot shows a Windows-style dialog box titled "Editing Offsite Vendor: IRM Test". The main heading is "Vendor Account Definition" with the HP logo. The dialog is divided into several sections:

- Define vendor account:** Includes an "Account ID" text box and a "Site" dropdown menu.
- Vaulting Days:** A group box containing seven checkboxes, all of which are checked: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday.
- Offsite Vendor Proxy Settings:** A group box containing a "Proxy Type" dropdown menu (set to "No Proxy"), a "Proxy Port" text box (set to "0"), a "Proxy Hostname" text box, a "Proxy Username" text box, and a "Proxy Password" text box.
- Define electronic interface to Iron Mountain FTP Server (SecureBase format files):** A group box containing three text boxes: "Host Name of destination FTP server", "FTP Account Name", and "FTP Account Password".

At the bottom of the dialog are four buttons: "Request Audit Listing", "Send Audit Listing", "OK", and "Cancel".

If you are creating an account for an Iron Mountain type of offsite vendor, type the account ID, hostname (defines the system name of the Iron Mountain Server being used to store the offsite media), FTP account name, and FTP password. If the connection to your offsite Iron Mountain Server passes through a firewall, you can type the proxy settings for this connection.

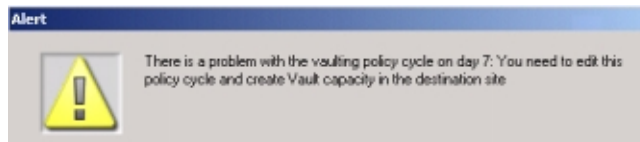
The Vaulting Days check boxes allow you to define any restrictions on the days of the week the vendor will accept offsite shipments. Vaulting Days on this screen takes precedence over vaulting days set in Vaulting Policies (see “Vaulting Policies” on page 50).

Once you have configured your offsite vendor account, click **OK** to return to the **Offsite Storage Vendor Definition** screen (see **Figure 2-10** on page 26). Then click **OK** to save the new offsite vendor and its accounts, and return to the **Vaulting Cycle Action** screen (see **Figure 2-9** on page 26).

You now want to specify the destination offsite vendor and account. Click **OK** to save the vaulting policy cycle. You are now back to the **Vaulting Cycle** screen (see **Figure 2-8** on page 25).

NOTE

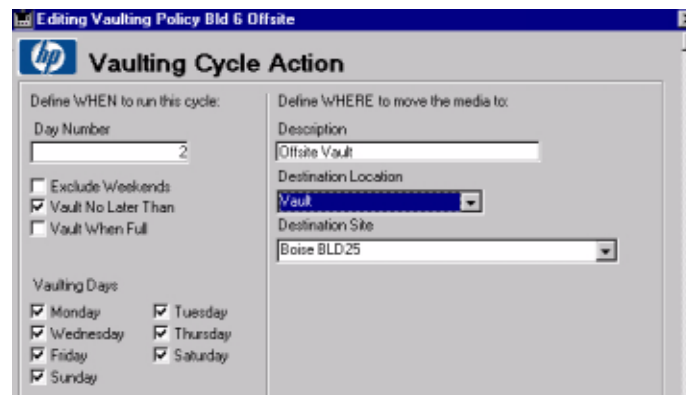
If you attempt to advance by clicking **Next** without editing the vaulting cycles with a vault destination, you will receive the following alert.



You now need to edit the vaulting cycle referred to in the alert either by double-clicking on that cycle, or by selecting the cycle and clicking **Edit**.

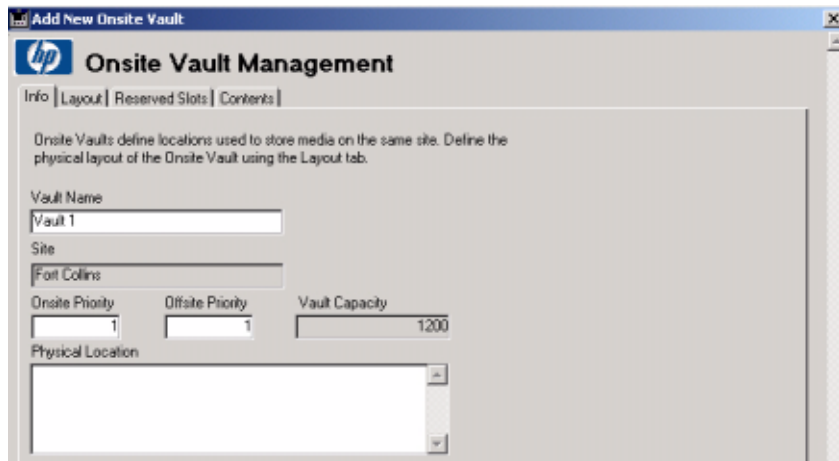
Figure 2-14

Vaulting Cycle Action — Capacity Screen



This screen is slightly different from the one in **Figure 2-9** on page 26. You now have to create vault capacity in the destination site. If your destination site is not this site, select the correct destination site. Click **Add Vault** to create vault capacity in the destination site. You are now at the **Onsite Vault Management** screen.

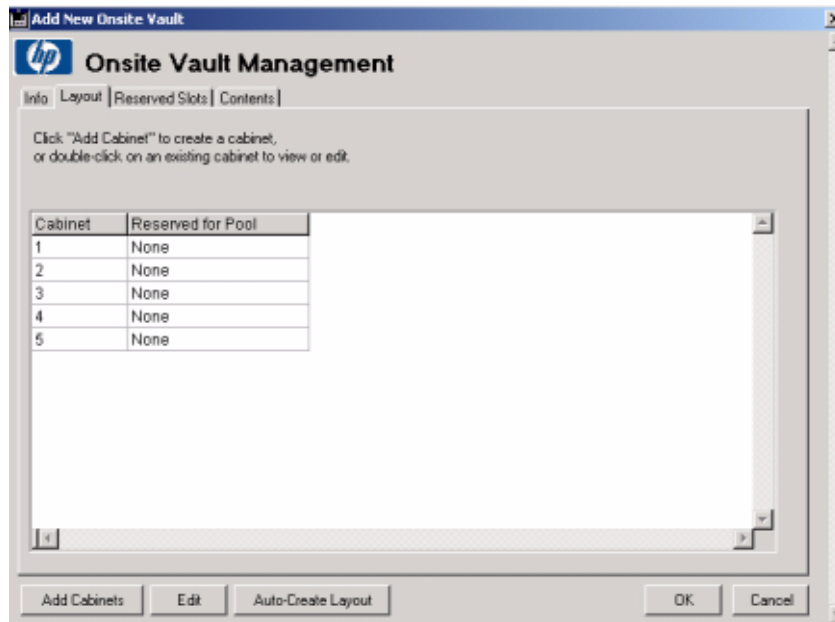
Figure 2-15 OnSite Vault Management — Info Screen



Type a vault name and then click the `Layout` tab to define the vault's configuration and capacity. You will see the following screen.

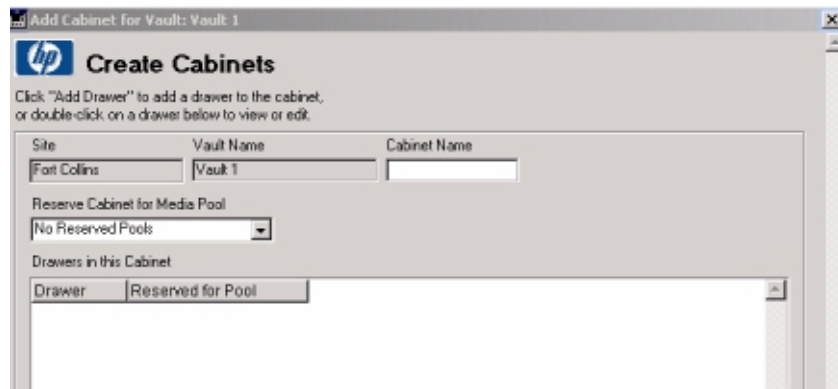
You can either add one cabinet manually by clicking `Add Cabinets` or automatically create the entire vault layout by clicking `Auto-Create Layout`.

Figure 2-16 Onsite Vault Management — Layout Screen



If you choose to manually create a cabinet, you will go through a series of screens prompting you for specific cabinet information. After clicking Add Cabinets, you will be at the Create Cabinets screen. Create a unique cabinet name and then click Add Drawers or Auto-Create Drawers.

Figure 2-17 Create Cabinets Screen



Presuming you are going to continue to manually create the drawers,

Getting Started Using Media Operations Using Media Operations

rows, and slots, because you opted to create the cabinet manually, you are now prompted for the first drawer name. Type a drawer name and then click Add Rows.

Figure 2-18 Create Drawers Screen

Row	Start Slot	End Slot	Capacity	Reserved for Pool
Row1	1	5	5	None
Row2	1	5	5	None
Row3	1	5	5	None

At the Create Rows screen, type the name of the first row in the drawer, starting slot number, ending slot number, number of media, and type of media.

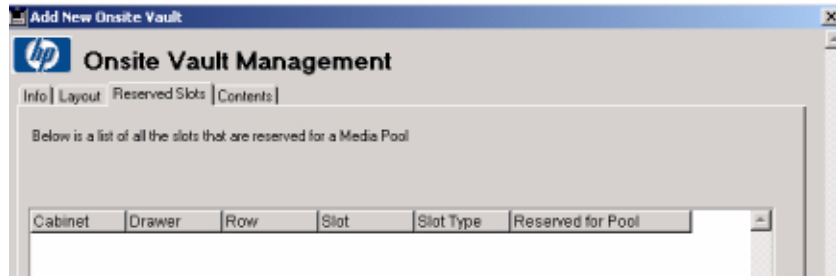
Figure 2-19 Create Rows Screen

Starting Slot Number	Ending Slot Number	Total Vault Slots/Row
1	5	5

Repeat until all rows are created. When you are done, click Cancel to return to the Create Drawers screen. Continue to create new drawers until all drawers are created. When you are finished creating drawers, click Cancel to return to the Create Cabinets screen. Continue to create cabinets until you have created all of the cabinets for that vault. Click Cancel to return to the Onsite Vault Management screen.

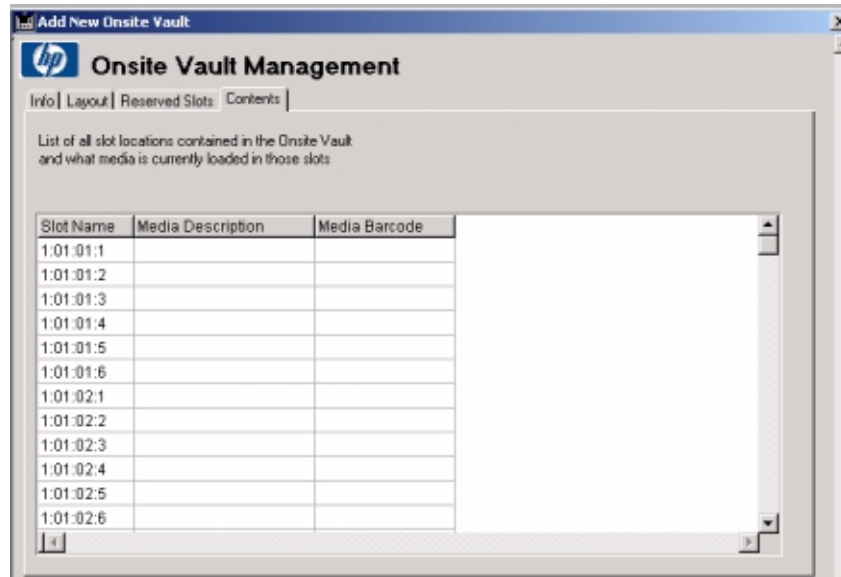
Click the `Reserved Slots` tab to see a list of all slots reserved for single media pools (as opposed to general slots).

Figure 2-20 Onsite Vault Management — Reserved Slots Screen



Click the `Contents` tab to view a list of all the media storage locations contained in the onsite vault and what media are contained in those vault slots.

Figure 2-21 Onsite Vault Management — Contents Screen

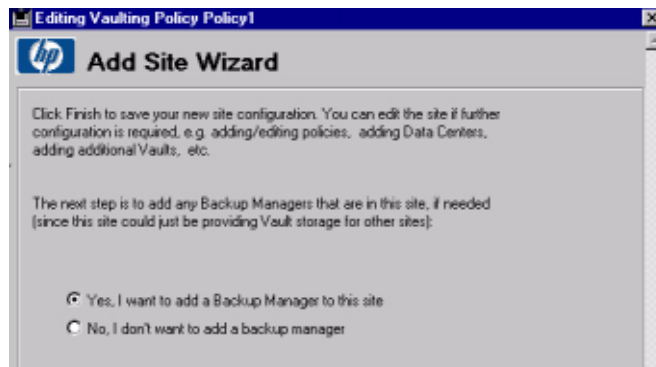


Once you have configured your vault, click `OK` to save the new vault and return to the `Vaulting Cycle Action` screen (see Figure 2-9 on page 26).

Click `OK` to save the vaulting policy cycle. You are now back to the

Vaulting Cycle screen (see Figure 2-8 on page 25).

Figure 2-22 **Finish Adding a Site**



Click **Finish** to save your new site configuration. Depending on whether you have selected to add a Backup Manager, you will be taken to the Site Management screen or the Add Backup Manager Wizard screen.

Add Backup Manager Wizard

The Add Backup Manager Wizard can either be launched from the Add Site Wizard screen or go to Global Configuration Options > Backup Managers.

Figure 2-23 **Adding a Backup Manager**



Select the type of Backup Manager you are adding. Then click **Next**. You will now need to type the network name of the Backup Manager System.

Figure 2-24 **Add Network Name**



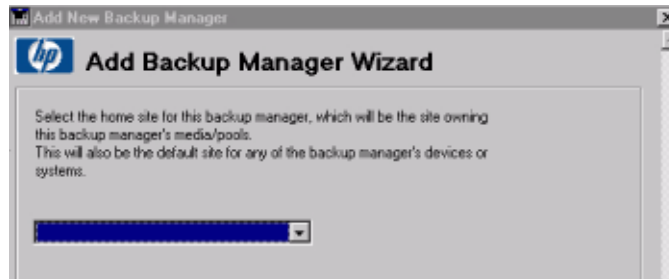
Type the network name of the Backup Manager System (such as `bkpserver1.xyz.com`) for Backup Manager Name. If this network name is not the same as the primary network name of its host system (for example, the host system has multiple network interfaces), you can select the host system's primary network name from the list of current systems in Media Operations by clicking the Backup Manager Host System arrow. Click Next to continue.

Getting Started Using Media Operations Using Media Operations

If you have more than one site configured, you will be taken to the screen that allows you to specify the home site for this Backup Manager. If you only have one site configured, the home site selection is skipped, as the software will automatically configure the Backup Manager's home site.

Figure 2-25

Define Home Site



Select the home site for this Backup Manager. Then click **Next**.

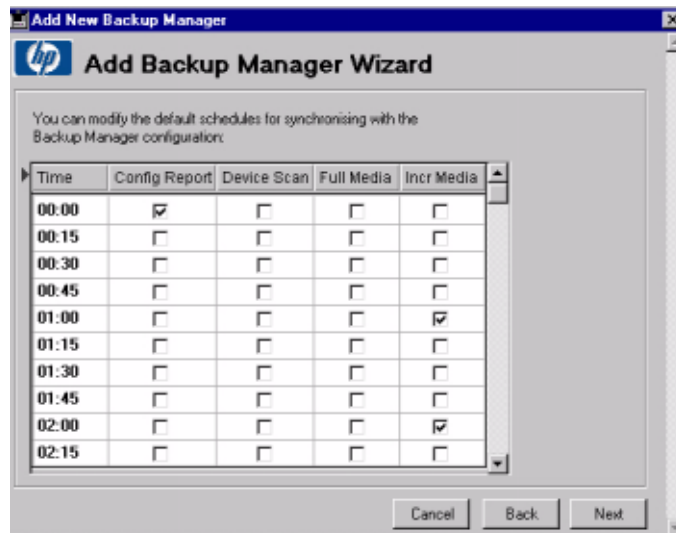
Figure 2-26

Define Security Settings



Type the security settings to connect to your Backup Manager. You can also change the port number. Then click **Next**.

Figure 2-27 **Schedule**

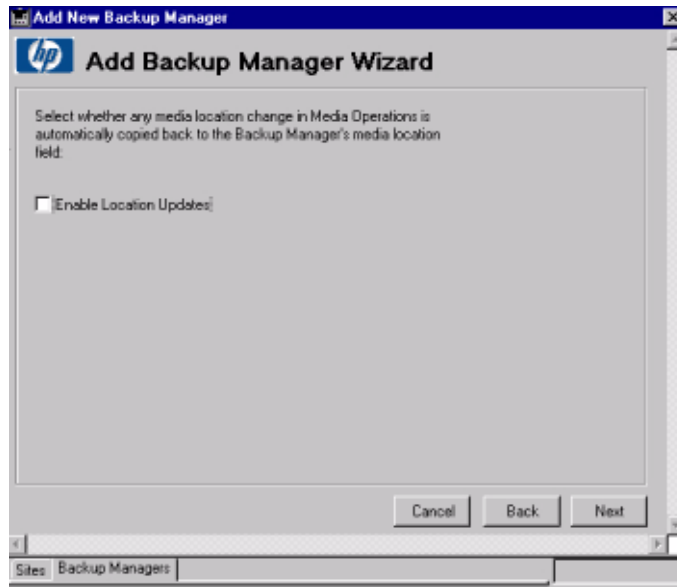


Make any schedule changes by selecting the appropriate check boxes and then click **Next**.

The scheduled events are used to keep Media Operations in sync with the Backup Manager.

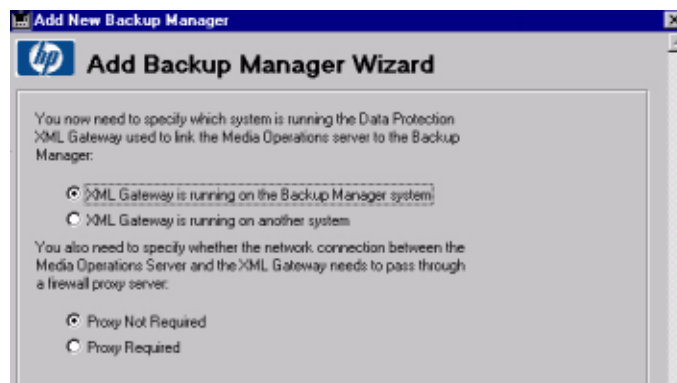
- **Config Report** — collects the clients on the Backup Manager, its MMDB configuration, media pools, devices, and backup specifications.
- **Device Scan** — scans all devices to determine what media are loaded in them.
- **Full Media** — retrieves a full media listing from the Backup Manager.
- **Incr Media** — retrieves all media modified in the past hour along with usage information on the media.

Figure 2-28 Enable Location Updates



Any request to change a media location in Media Operations is automatically copied back to the Backup Manager's media location, select the `Enable Location Updates` check box. Then click `Next`.

Figure 2-29 XML Gateway



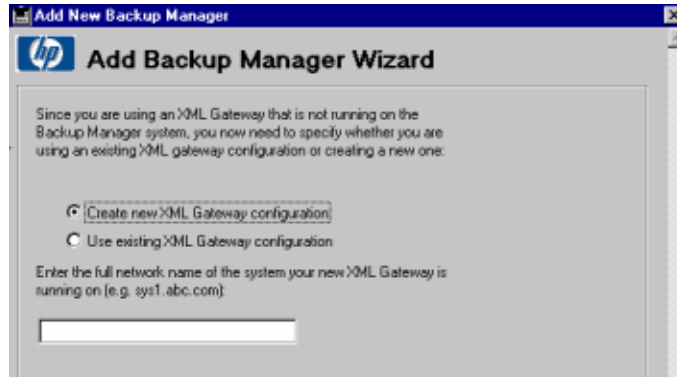
Select the radio button that specifies which system is running the XML Gateway used to link the Media Operations Server to the Backup Manager. If the XML Gateway is running on another system, select a radio button to specify whether you will be using an existing

configuration or creating a new one.

NOTE

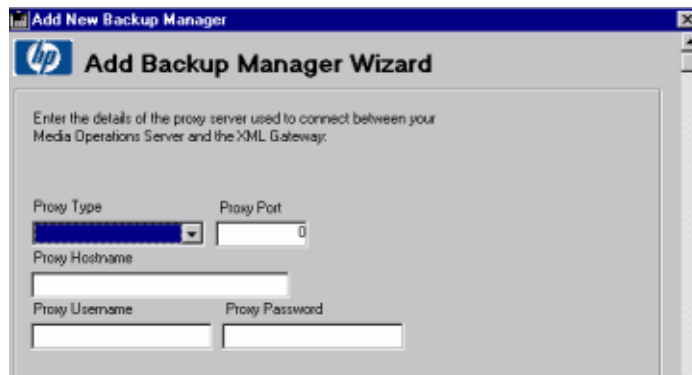
The NetBackup gateway should always be present on the Master server.

Figure 2-30 XML Gateway Configuration



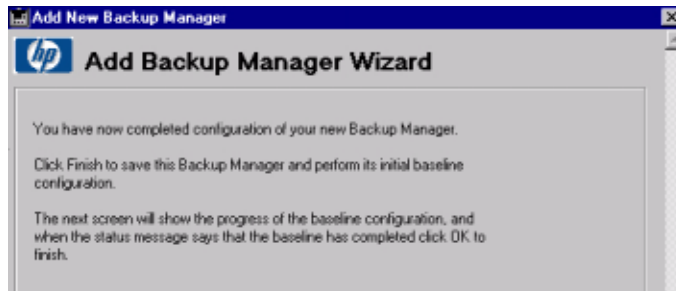
Select a radio button to indicate whether you want to create a new XML Gateway configuration or use an existing one. Type the full network name of the system your new XML Gateway is running on. Click **Next** and you will see either see the **Proxy Settings** screen (if you selected **Proxy Required** on the previous screen) or the **Save Backup Manager** screen.

Figure 2-31 Proxy Setting



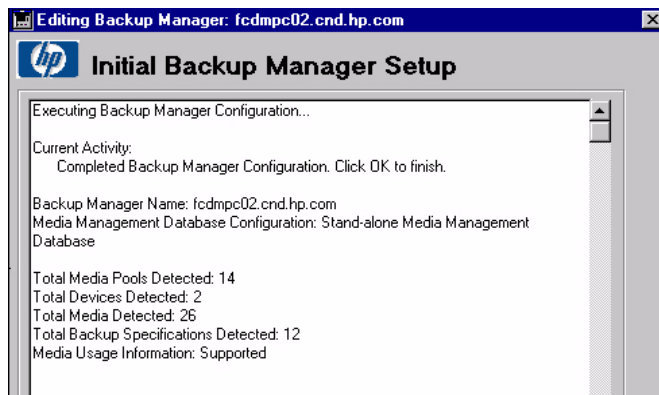
Type the details of the Proxy Server used to connect the Media Operations Server and the XML Gateway. Click **Next** to continue to the **Save the Backup Manager** screen.

Figure 2-32 Save the Backup Manager



Click **Finish** to save the Backup Manager and perform the initial baseline configuration. The next screen will show the progress of the baseline configuration. When the status message says the baseline has completed, click **OK**.

Figure 2-33 Backup Manager Configuration



You have now successfully configured a site and added a Backup Manager to that site. You can now edit the site and Backup Manager objects to further tune the configuration. For example:

- ✓ Add additional vaulting policies to the site and apply them to pools, backup specifications, or systems for cases where you want a different policy from the default site-level policy.
- ✓ Edit each media pool and set the correct media compression for the media in that pool. For example, an LTO pool could contain LTO1 or LTO2 media. You need to set which one, so that premount jobs calculate the required media for this pool based on the correct media capacity.

Editing an Existing Site

You can edit an existing site either from Global Configuration Options > Site Management or Site Configuration under the specific site.

There are nine tabs on the Site Definition screen:

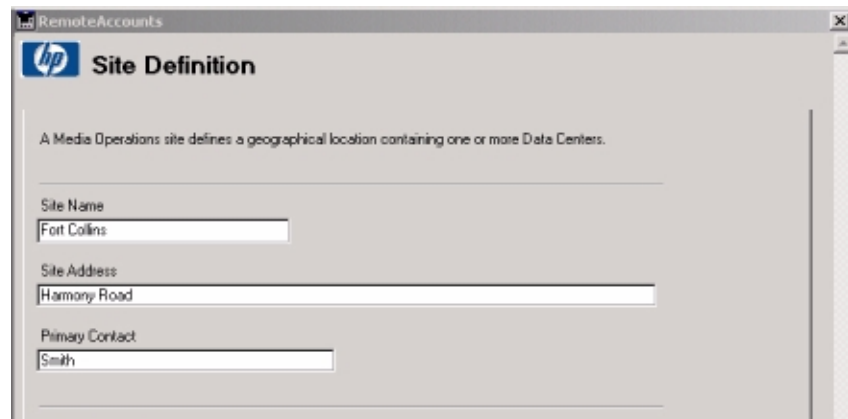
- Info
- DNS
- Vaults
- Data Centers
- Vaulting Policies
- Offsite Vendors
- Users
- Remote Accounts
- Import Data

Info

The Site Definition - Info screen shows the geographical location that contains data centers for that site. Every site has at least one default data center, but you can configure additional centers if needed. Each site is defined with a unique site name and a default vaulting policy. You can optionally define additional data centers and onsite vaults, and also associate the site with a set of DNS suffixes so systems within that suffix can be automatically assigned to the appropriate sites.

Figure 2-34

Site Definition — Info Screen



RemoteAccounts

hp Site Definition

A Media Operations site defines a geographical location containing one or more Data Centers.

Site Name
Fort Collins

Site Address
Harmony Road

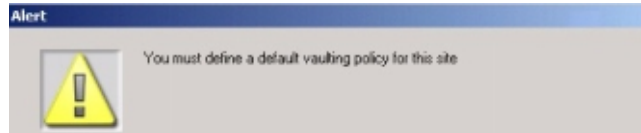
Primary Contact
Smith

Getting Started Using Media Operations Using Media Operations

If you attempt to exit this screen without defining a vaulting policy, you receive the following alert.

Figure 2-35

Alert



When you click `Create`, you are required to:

- ✓ type the name of the vaulting policy you are adding,
- ✓ select a template to use,
- ✓ type any site specific vaulting location information (such as if you have a vaulting cycle implementation with an offsite vendor destination), and
- ✓ select which offsite vendor and offsite vendor account.

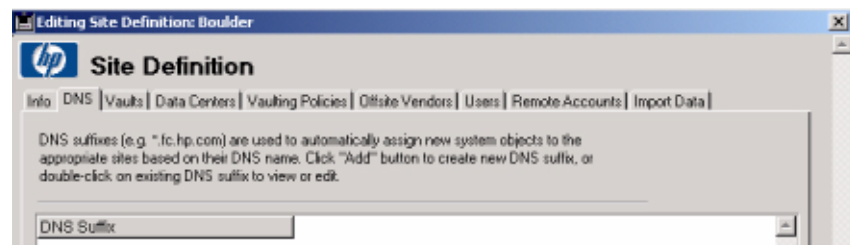
After you have entered the information, click `OK`. There are six predefined templates available, or you can define and add additional ones as required. See “Vaulting Templates” on page 95.

DNS

The `Site Definition - DNS` screen allows you to associate the site with a set of DNS suffixes (such as `*.fc.hp.com`) so that system objects added to the Media Operations configuration are automatically assigned to the appropriate sites based on their DNS name. Click `Add` to create a new DNS suffix for this site or `Edit` to view or edit.

Figure 2-36

Site Definition — DNS Screen



Vaults

The Site Definition - Vaults screen defines the onsite vaults in a site that defines the physical locations that can be used to securely store media. Click Add or

Add Many to create a new vault, or double-click a vault to view or edit.

Figure 2-37 Site Definition — Vaults Screen

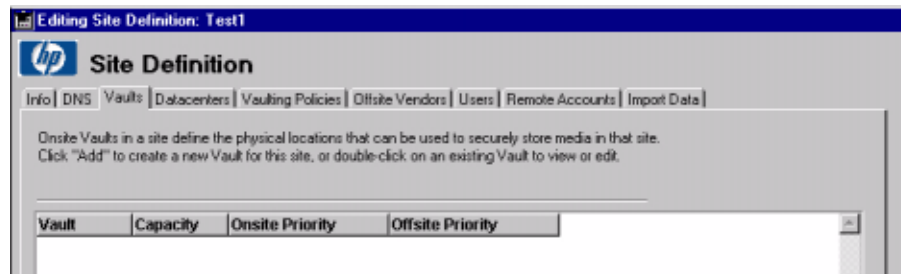
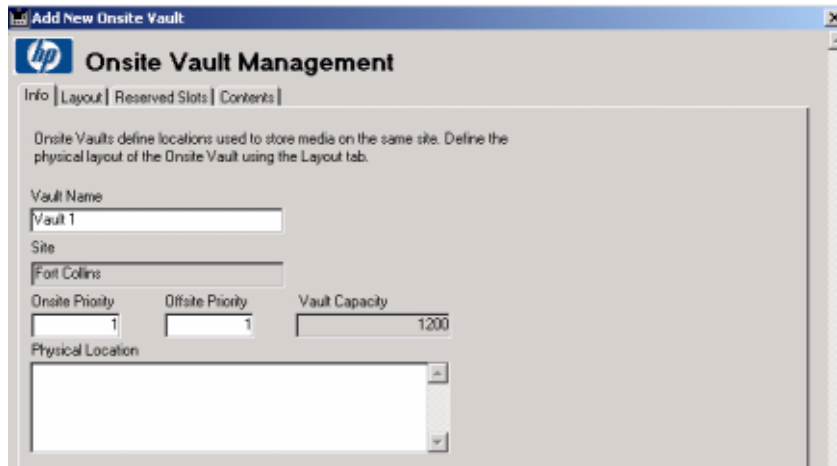


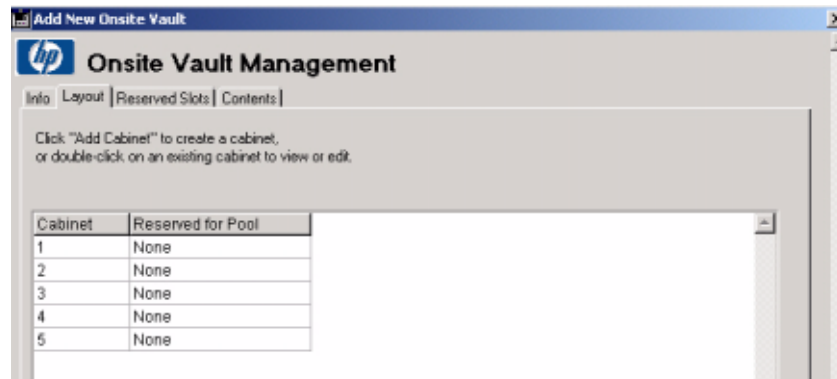
Figure 2-38 OnSite Vault Management — Info Screen



Type the name of the vault first. Then click the `Layout` tab to define the vault's configuration and capacity.

You can either add one cabinet manually by clicking `Add Cabinets` or automatically create the entire vault layout by clicking `Auto-Create Layout`.

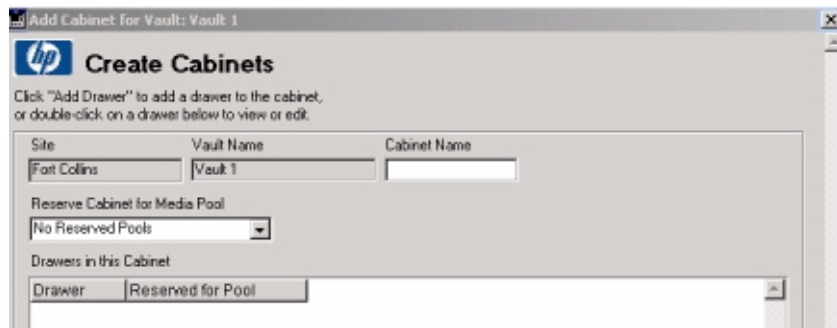
Figure 2-39 Onsite Vault Management — Layout Screen



If you choose to manually create a cabinet, you will go through a series of screens prompting you for specific cabinet information. After clicking Add Cabinets, you will be at the Create Cabinets screen.

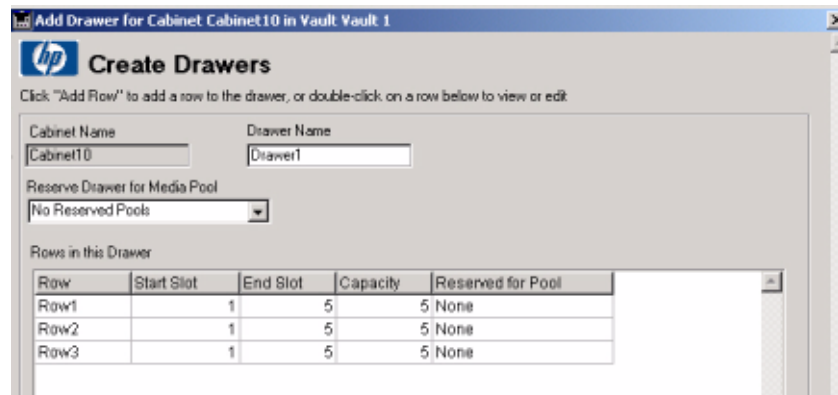
Create a unique cabinet name and then click Add Drawers or Auto-Create Drawers.

Figure 2-40 Create Cabinets Screen



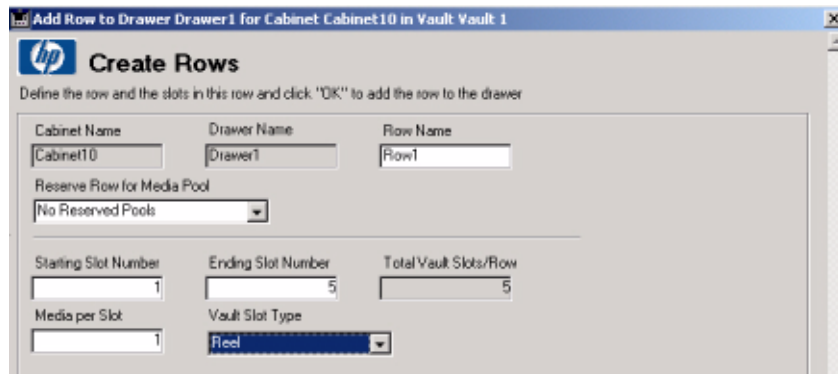
Presuming you are going to continue to manually create the drawers, rows, and slots, because you opted to create the cabinet manually, you are now prompted for the first drawer name. Type the drawer name and then click Add Rows.

Figure 2-41 Create Drawers Screen



At the `Create Rows` screen, type the name of the first row in the drawer, starting slot number, ending slot number, number of media, and type of media.

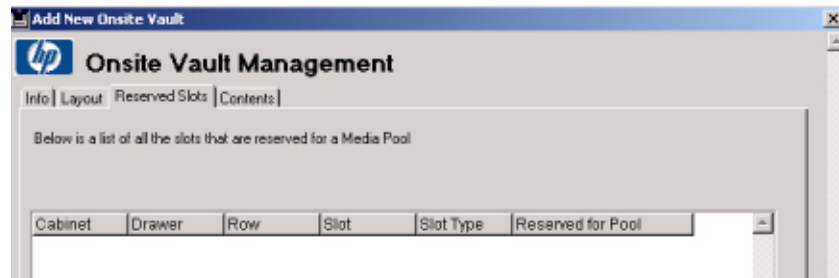
Figure 2-42 Create Rows Screen



Repeat until all rows are created. When you are done, click `Cancel` to return to the `Create Drawers` screen. Continue to create new drawers until all drawers are created. When you are finished creating drawers, click `Cancel` to return to the `Create Cabinets` screen. Continue to create cabinets until you have created all the cabinets for that vault. Click `Cancel` to return to the `Onsite Vault Management` screen.

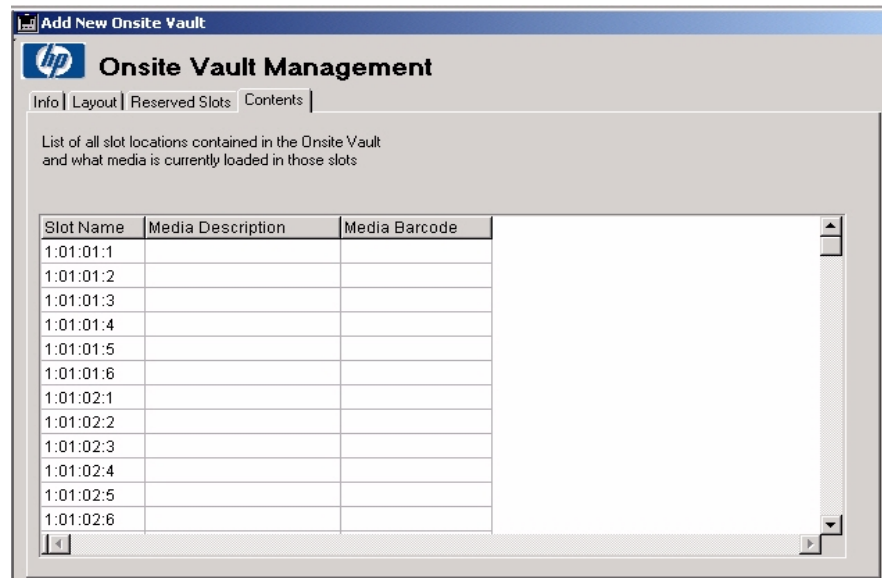
Click the `Reserved Slots` tab to see a list of all slots reserved for single media pools (as opposed to general slots).

Figure 2-43 **Onsite Vault Management — Reserved Slots Screen**



Click the **Contents** tab to view a list of all the media storage locations contained in the onsite vault and what media are contained in those vault slots.

Figure 2-44 **Onsite Vault Management — Contents Screen**



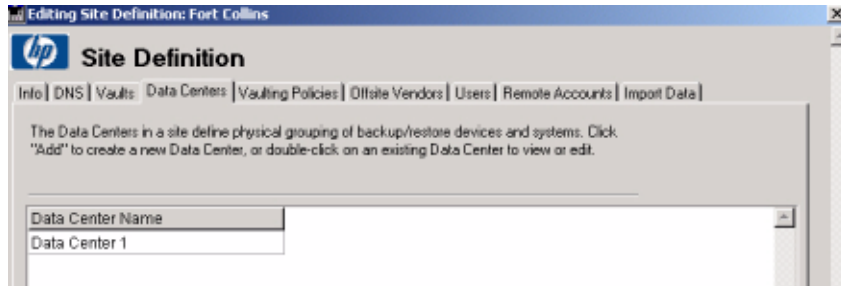
When you are defining the vaults, click **OK** to return to the **Site Management** screen.

Data Centers

The **Site Definition - Data Centers** screen defines the physical grouping of backup/restore devices and systems. Click **Add** to create a

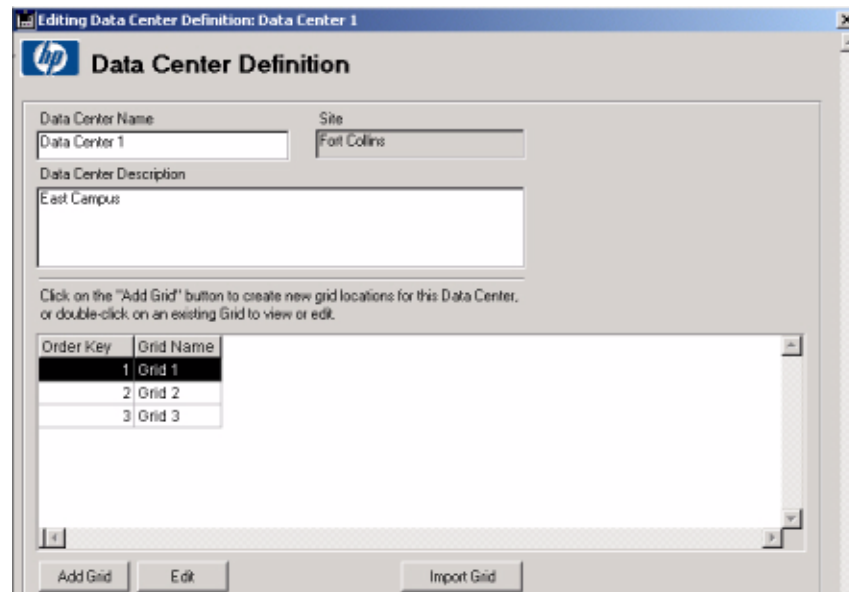
new data center, or click Add Many to create multiple data centers within a site.

Figure 2-45 Site Definition — Data Center Screen



You now need to define the data center by typing a unique name for the data center and a description (such as the location of the data center).

Figure 2-46 Data Center Definition Screen



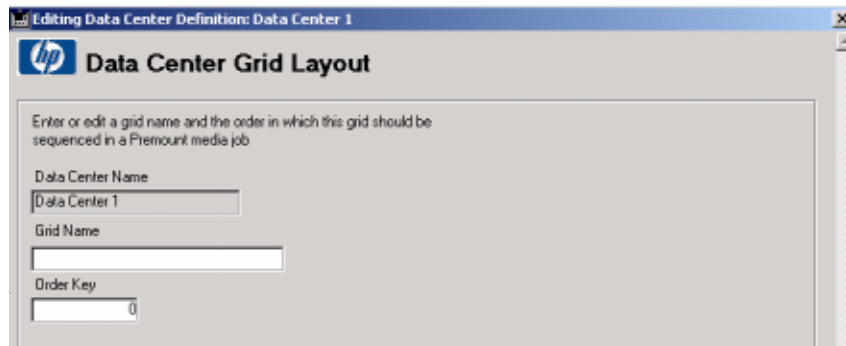
Getting Started Using Media Operations

Using Media Operations

Data center grids are used to define the physical layout of the data center and the grid walk-through order, so you can assign locations to systems and devices in that data center and use this to optimize the walk-through order of devices during premount jobs.

In addition to the basic data center description, you can either add grids manually or import a grid definition file. See “Import Data” on page 60 for import instructions.

Figure 2-47 Data Center Grid Layout Screen



Editing Data Center Definition: Data Center 1

hp Data Center Grid Layout

Enter or edit a grid name and the order in which this grid should be sequenced in a Premount media job

Data Center Name
Data Center 1

Grid Name
[Empty]

Order Key
0

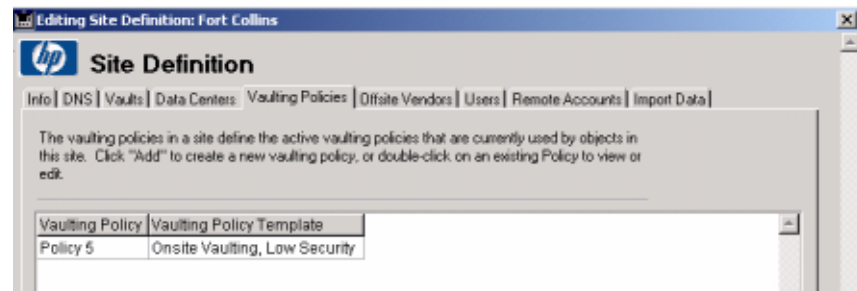
Type the grid name and order key. The order key is the walk-through order of the grids in the data center. The order key is the step number in the walk-through order. For example, the first grid location in the data center is key number 1 and the second grid location (in the walk-through order) is key number 2, and so on. This is used to order the grid names into the walk-through order for the premount jobs.

Continue to add the grids until they have all be defined. Click **Cancel** to exit the screen. Click **Cancel** again to return to the Site Definition screen (see Figure 2-34 on page 43).

Vaulting Policies

The Site Definition - Vaulting Policies screen defines the active vaulting policies that are currently used by objects in this site.

Figure 2-48 Site Definition — Vaulting Policies Screen

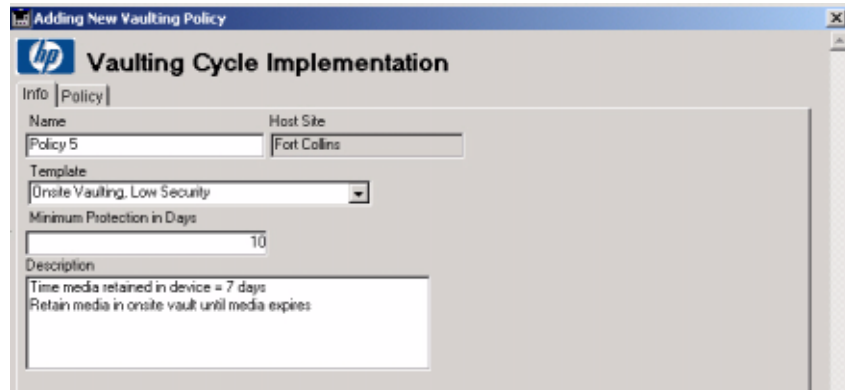


Six vaulting templates are predefined. These modifiable templates provide a starting point for vaulting policies. The default templates are:

- **No Vaulting, Low Media Security:** Medium stays in the device until it is scratched.
- **Onsite Vaulting, Low Media Security:** Medium is retained in the device for seven days and retained in an onsite vault until it expires.
- **Onsite Vaulting, Medium Media Security:** Medium is not retained in the device. It is retained in an onsite vault until it expires.
- **Fast Recovery Access, Low Media Security:** Medium is retained in the device for seven days and retained in an onsite vault for seven days. Medium is retained in an offsite vault until it expires.
- **Medium Recovery Access, Medium Media Security:** Medium is not retained in the device. It is retained in an onsite vault for seven days and in an offsite vault until it expires.
- **Slow Recovery Access, High Media Security:** Medium is not retained in the device or in an onsite vault. Medium is retained in an offsite vault until it expires.

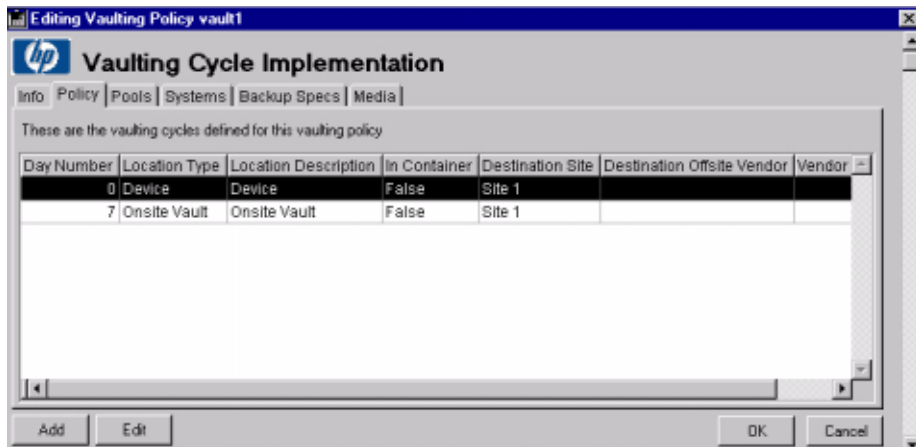
Click **Add** or **Add Many** to add new vaulting policies. If there are vaulting policies already defined, you can click **Edit** or double-click a policy to view or edit.

Figure 2-49 Vaulting Cycle Implementation — Info Screen



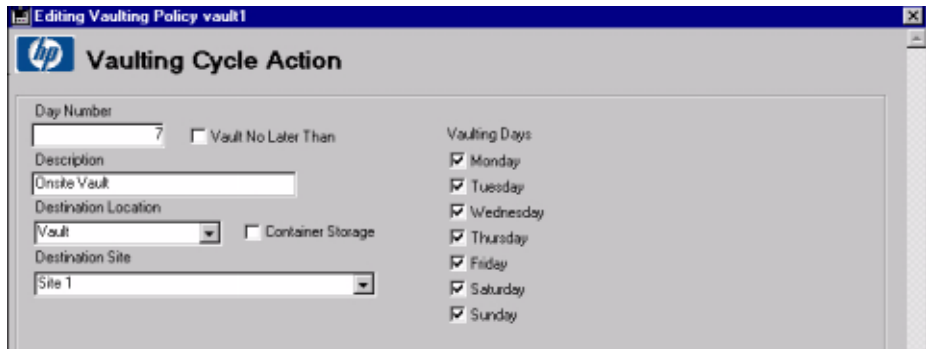
Type a name for the new vaulting policy. Select a template to use. Type the minimum number of days protection is required. Click the **Policy** tab. This takes you to the Vaulting Policy Implementation - Policy screen where you can add or edit the vaulting cycles.

Figure 2-50 Vaulting Policy Implementation — Policy Screen



Click **Add** to add a new vaulting cycle or **Edit** to edit an existing vaulting cycle. You can also select a vaulting cycle and double-click to edit.

Figure 2-51 Vaulting Cycle Action Screen

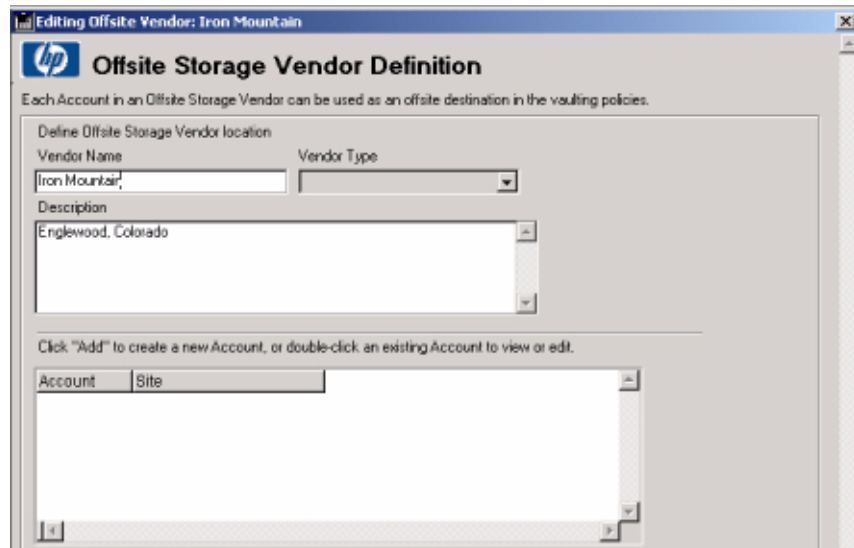


Type the day number. Select the destination location and the destination site. To select the days of the week for the cycle to occur, select the appropriate Vaulting Days check boxes. Click OK to return to the previous screen. Click OK again to return to the Site Definition screen (see Figure 2-34 on page 43).

Offsite Vendors

The Offsite Storage Vendor Definition screen defines locations used to store media securely offsite.

Figure 2-52 Offsite Storage Vendor Definition Screen



Getting Started Using Media Operations Using Media Operations

The offsite vendor location is defined by a unique vendor name. The offsite vendor type can be a Media Operations vendor, Iron Mountain vendor, or generic vendor (see page 26). The `Contact Details` field is used to describe the vendor. This is a flexible field and you can type unique information for that vendor (such as the vendors location, building number, suite, floor, and contact information).

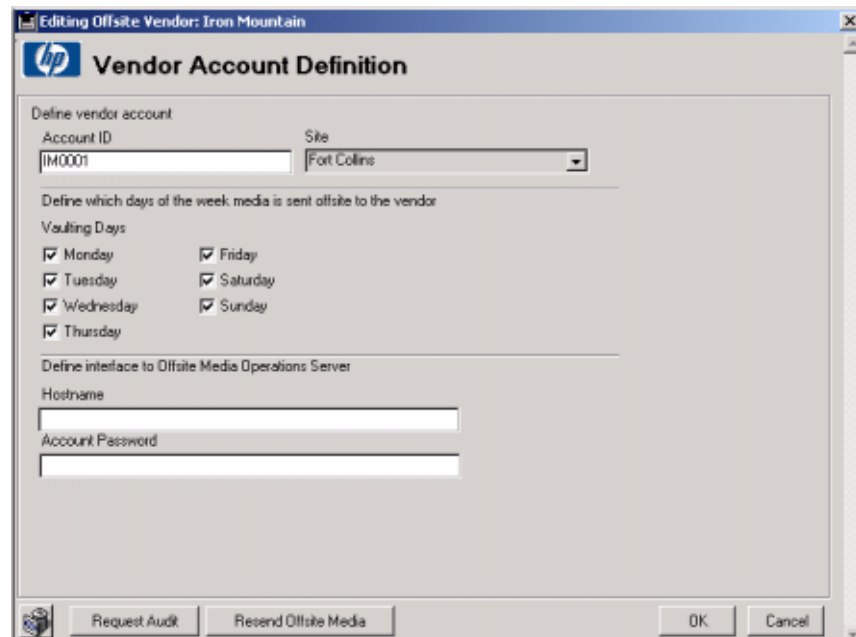
Each offsite vendor location can be used by multiple sites with each site having a unique account in that offsite storage vendor.

NOTE

A vendor can be used by multiple sites. Each site must have at least one account name unique to that vendor.

Figure 2-53

Vendor Account Definition — Media Operations Type Screen



The screenshot shows a window titled "Editing Offsite Vendor: Iron Mountain" with the HP logo and "Vendor Account Definition" header. The form is divided into three sections:

- Define vendor account:** Includes an "Account ID" text box containing "IM0001" and a "Site" dropdown menu set to "Fort Collins".
- Define which days of the week media is sent offsite to the vendor:** Labeled "Vaulting Days", it features checkboxes for Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday, all of which are checked.
- Define interface to Offsite Media Operations Server:** Includes a "Hostname" text box and an "Account Password" text box.

At the bottom of the window are four buttons: "Request Audit", "Resend Offsite Media", "OK", and "Cancel".

If you are creating an account for a Media Operations type of offsite vendor, type the account ID, hostname (defines the system name of the Media Operations Server being used to store the offsite media), and password. The account ID defines a unique ID for this vendor. The hostname defines the system name of the Media Operations Server being used to store the offsite media. To authenticate this interface, the account ID is used as the username and an account password must also

be typed. The account ID and account password must match a remote account on the offsite Media Operations Server. Therefore, the account ID is the account name of the remote account at the offsite Media Operations Server. The hostname is the system on which the offsite's Media Operations system resides.

The Vaulting Days check boxes allow you to define any restrictions on the days of the week the vendor will accept offsite shipments. Vaulting Days on this screen takes precedence over vaulting days set in Vaulting Policies (see “Vaulting Policies” on page 50).

Click OK to complete the operation or Cancel to abort. You are returned to the Offsite Storage Vendor Definition screen. Click OK when you have finished adding offsite vendors. You are returned to the Site Definition screen (see Figure 2-34 on page 43).

Figure 2-54

Vendor Account Definition — Iron Mountain Type Screen

The screenshot shows a Windows-style dialog box titled "Editing Offsite Vendor: IRIM Test". The main heading is "Vendor Account Definition" with the HP logo. The dialog is divided into several sections:

- Define vendor account:** Includes an "Account ID" text box and a "Site" dropdown menu.
- Vaulting Days:** A group of seven checkboxes, all of which are checked: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday.
- Offsite Vendor Proxy Settings:** Includes a "Proxy Type" dropdown menu (set to "No Proxy"), a "Proxy Port" text box (set to "0"), a "Proxy Hostname" text box, a "Proxy Username" text box, and a "Proxy Password" text box.
- Define electronic interface to Iron Mountain FTP Server (SecureBase format files):** Includes three text boxes: "Host Name of destination FTP server", "FTP Account Name", and "FTP Account Password".

If you are creating an account for an Iron Mountain type of offsite vendor, type the account ID, hostname (defines the system name of the Iron Mountain Server being used to store the offsite media), FTP account name, and FTP password. If the connection to your offsite Iron Mountain Server passes through a firewall, you can type the proxy settings for this connection.

The Vaulting Days check boxes allow you to define any restrictions on

Getting Started Using Media Operations

Using Media Operations

the days of the week the vendor will accept offsite shipments. Vaulting Days on this screen takes precedence over vaulting days set in Vaulting Policies (see “Vaulting Policies” on page 50).

Use the media link Filename Format on the Vendor Definition screen if you need to provide FTP files to Iron Mountain using the old MediaLink file name format. (Note) the FTP contents are always SecureBase format, so this only affects the file name.

Click OK to complete the operation or Cancel to abort. You are returned to the Offsite Storage Vendor Definition screen (see Figure 2-52 on page 53). When you have finished adding offsite vendors, click OK. You are returned to the Site Definition screen (see Figure 2-34 on page 43).

Figure 2-55 Vendor Account Definition — Generic Type Screen

The screenshot shows a Windows-style dialog box titled "Editing Offsite Vendor: Generic". The main content area is titled "Vendor Account Definition" and features the HP logo. It is divided into three main sections:

- Define vendor account:** Includes an "Account ID" text field and a "Site" dropdown menu currently set to "Site 1".
- Define which days of the week media is sent offsite to the vendor:** Labeled "Vaulting Days", this section has seven checkboxes, all of which are checked: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday.
- Define interface to Offsite Storage Vendor:** This section contains four text input fields for command line scripts, each with an "Enabled" checkbox to its right:
 - Outgoing Media command line script
 - Return Media command line script
 - Status Verification command line script
 - Audit Management command line script

At the bottom of the dialog, there are four buttons: "Request Audit Listing", "Send Audit Listing", "OK", and "Cancel".

If you are creating an account for a generic type of offsite vendor, type the account ID. The account ID defines a unique ID for this vendor. There is also a set of optional configuration settings used when the offsite vendor has their own proprietary electronic link interface.

The Vaulting Days check boxes allow you to define any restrictions on the days of the week the vendor will accept offsite shipments. Vaulting Days on this screen takes precedence over vaulting days set in Vaulting Policies (see “Vaulting Policies” on page 50).

When configuring offsite accounts for a generic vendor type, the Media Operations administrator can write scripts to take information from Media Operations and convert this to their offsite vendors electronic link protocol.

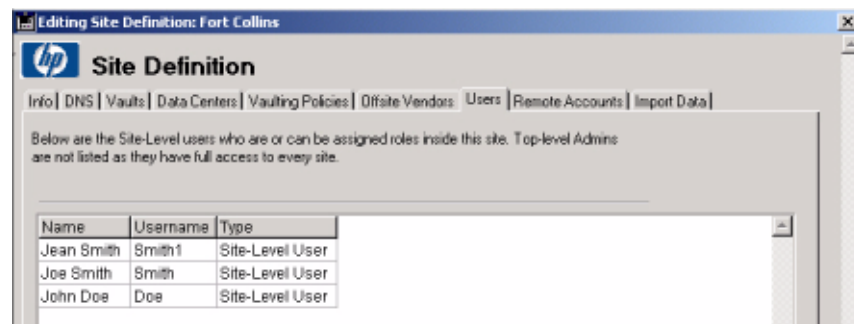
1. Select the Enabled check box for the Outgoing/Return Media command line script if the offsite storage vendor supports an interface to manage outgoing and returning media. Then type the script/utility command line to link Media Operations to the vendor.
2. Select the Enabled check box for the Status Verification command line script if the offsite storage vendor supports an interface to notify when previously submitted outgoing and returning media jobs are complete. Then type the script/utility command line to link Media Operations to the vendor.
3. Select the Enabled check box for the Audit Management command line script if the offsite storage vendor supports an interface to audit stored media. Then type the script/utility command line to link Media Operations to the vendor.

Users

The Site Definition - Users screen defines site-level users who are or can be assigned roles inside a site. Top-Level administrators are not listed as they have full access to every site.

Figure 2-56

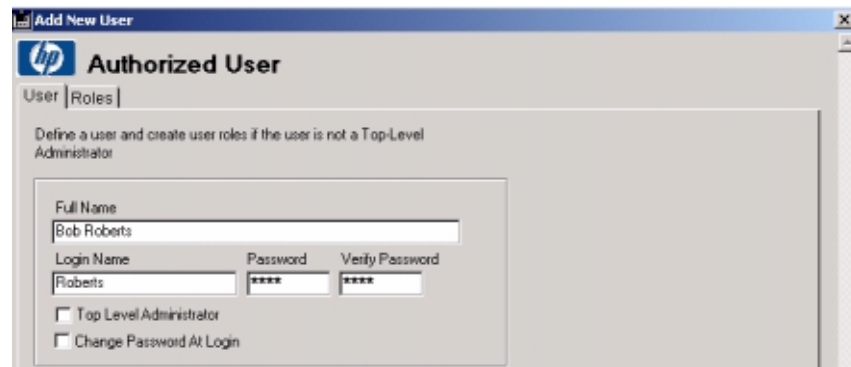
Site Definition — User Screen



Getting Started Using Media Operations Using Media Operations

Click **Add** to add a new user or **Edit** to edit or view a user.

Figure 2-57 Authorized User — User Screen



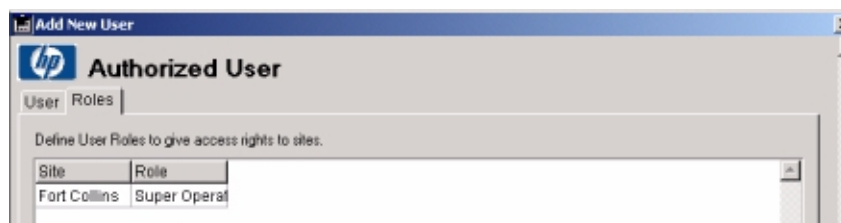
The screenshot shows a window titled "Add New User" with a sub-header "Authorized User". Below the sub-header are two tabs: "User" (selected) and "Roles". The main area contains the following fields and options:

- Full Name: Bob Roberts
- Login Name: Roberts
- Password: [masked with asterisks]
- Verify Password: [masked with asterisks]
- Top Level Administrator
- Change Password At Login

Type the username, login name, and password. Select the **Change Password at Logon** check box if you want to force the user to change their password the first time they login. If the user will not be a top-level administrator, you now have to assign a role for the user. Click the **Roles** tab.

If the user will be a top-level administrator, select the **Top Level Administrator** check box. With this check box selected, the user will have full rights to perform any operations. Only top-level administrators have full access to the **Global Configuration Options** of the user interface.

Figure 2-58 Authorized User — Roles Screen

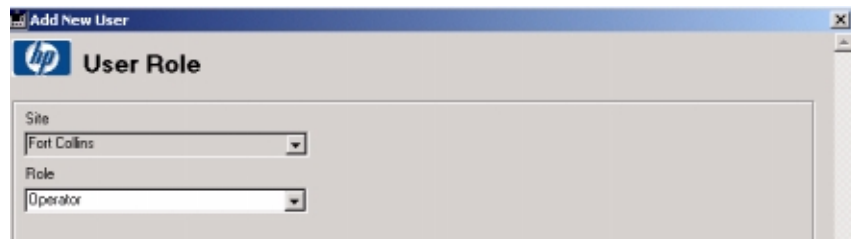


The screenshot shows the same "Add New User" window, but with the "Roles" sub-tab selected. The main area contains the following table:

Site	Role
Fort Collins	Super Operat

Click **Add** to add a role for a user. Click **Edit** or double-click a user to view or edit.

Figure 2-59 **User Role Screen**

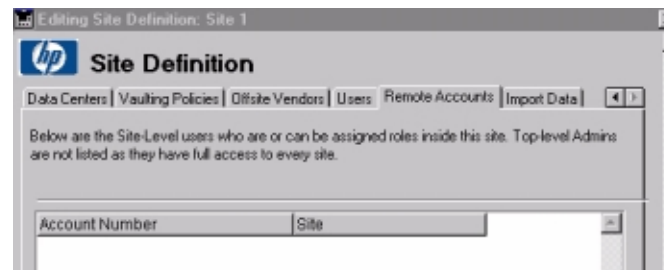


Select a role for the user. Click **Cancel** to return to the Authorized User screen. Click **OK** to return to the Site Definition - User screen.

Remote Accounts

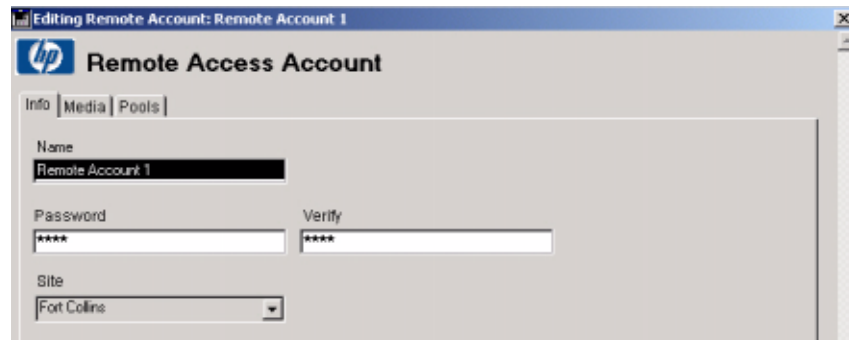
The Site Definition - Remote Accounts screen defines accounts used by other Media Operations Servers who are permitted to store media in this site. These are the accounts matched within the vendor account records on the other Media Operations Server.

Figure 2-60 **Site Definition — Remote Accounts Screen**



Click **Add** or **Add Many** to add a remote account. Double-click an existing account or click **Edit** to edit or view.

Figure 2-61 Remote Access Account — Info Screen

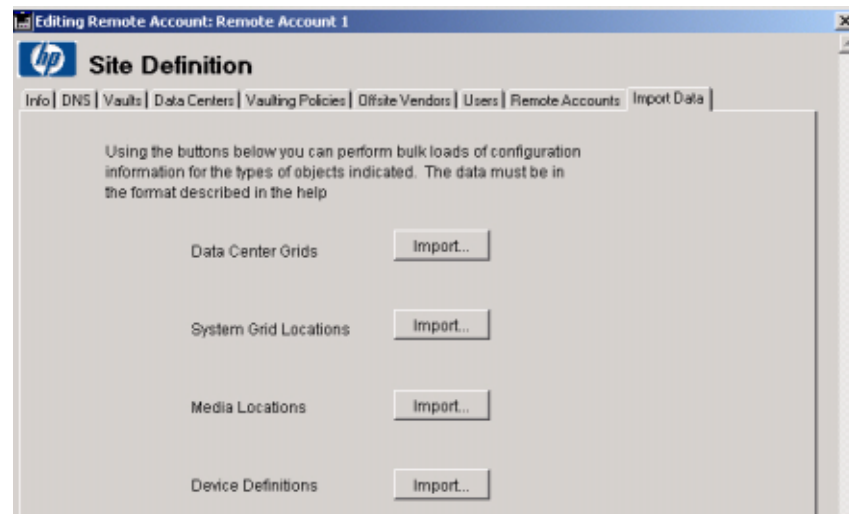


Type the remote access account name and password, verify the password, and then click OK to return to the Site Definition screen (see Figure 2-34 on page 43).

Import Data

The Site Definition - Import Data screen allows you to perform bulk loads of configuration information for data center grids, system grid locations, media location, and device definitions.

Figure 2-62 Site Definition — Import Data Screen



Click `Import` and select the file to be imported.

Import Data Center Grid Information To import data center grid information, it must be contained in a comma-delimited text file and match the format described below.

The fields values are Site, Data Center, Grid and Order Key. They must be bounded by quotation marks (" ") and separated by commas. There must be no more than one record per line.

For example:

```
"Site", "Data Center", "Grid", "Order Key"  
"London #1", "North", "B16", "25"
```

System Grid Locations To import system grid information, it must be contained in a comma-delimited text file and match the format described below.

The fields values are System, Site, Data Center and Grid. They must be bounded by quotation marks (" ") and separated by commas. There must be no more than one record per line.

For example:

```
"System", "Site", "Data Center", "Grid"  
"boi1036.boi.hp.com", "junk", "Brad's DataCenter", "A6"  
"boi1037.boi.hp.com", "junk", "Brad's DataCenter", "A7"  
"boi1038.boi.hp.com", "junk", "Brad's DataCenter", "A8"
```

Media Locations To import media location information, it must be contained in a comma-delimited text file and match the format described below.

The fields values are Media, Location, Site, Vault, Slot, Vendor and Account. They must be bounded by quotation marks (" ") and separated by commas. There must be no more than one record per line.

For example:

```
"Media", "Location", "Site", "Vault", "Slot", "Vendor", "Account"  
"AB0001", "Vault", "Akron BLD 3", "closet", , "1"  
"AB0002", "Vault", "Akron BLD 3", "closet", , "1"  
"AB0003", "Offsite", "Akron BLD 3", , "Vendor1", "1000"
```

Getting Started Using Media Operations

Using Media Operations

Import Device Definitions To import device definition information, it must be contained in a comma-delimited text file and match the format described below.

The fields values are System, Device, Type, Media Type and Compression. They must be bounded by quotation marks (" ") and separated by commas. There must be no more than one record per line. The fields values are:

For example:

```
"System", "Device", "Type", "Media Type", "Compression"  
"slc1036.abc.xy.com", "L0", "Library", "LTO-Ultrium", "LTO2"  
"slc1036.abc.xy.com", "L1", "Library", "LTO-Ultrium", "LTO2"  
"slc1036.abc.xy.com", "L2", "Library", "LTO-Ultrium", "LTO2"
```

Import Manual Media To import new manual media definitions (for example, media not associated with any Backup Manager, such as legacy media already stored in offsite or vault locations), they must be contained in a comma-delimited text file and match the format described below.

The fields values are MediaLabel, Media Barcode and Pool (the name of a manually created pool in this site to which you want to import the media). They must be bounded by quotation marks (" ") and separated by commas. There must be no more than one record per line. The fields values are:

For example:

```
"MediaLabel", "MediaBarcode", "Pool"  
"AB001", "AB001", "DLT_Pool"  
"AB002", , "DLT_Pool"
```

NOTE

When creating manual media through this import function, media are created as scratch media, but their last used date is set to when the import was performed. This means, if the vaulting policy for the manual pool that these media are in has a minimum retention time set, the manual media will have the vaulting policies applied to them even though they are scratch media.

Deleting a Site

- You cannot delete a site unless you delete or move the Backup Managers using that site (for example, the Backup Managers with that site as their home site).
- Sites that contain any “remote” devices or systems (such as devices or systems on a Backup Manager that have a home site in a different site) are automatically moved to the home site of their Backup Manager, including copying vaulting policies and premount job schedules to their destination sites if necessary.
- Any manually created objects are deleted when the site is deleted. (You receive a warning prior to the deletion starting, so you can manually move the manual pools, devices, systems, backup specifications via Global Object Lists.)

NOTE

Modifying the site details (name, description, address and so on) has no effect on any Backup Servers or objects defined in that site.

Editing a Backup Manager

This section describes the Backup Manager option under the Global Configuration Options menu. See “Backup Managers” on page 84 for additional information regarding Backup Managers/Servers.

The definition of each Backup Server managed by the Storage Media Operations Server is displayed on the following Backup Managers screen.

Figure 2-63

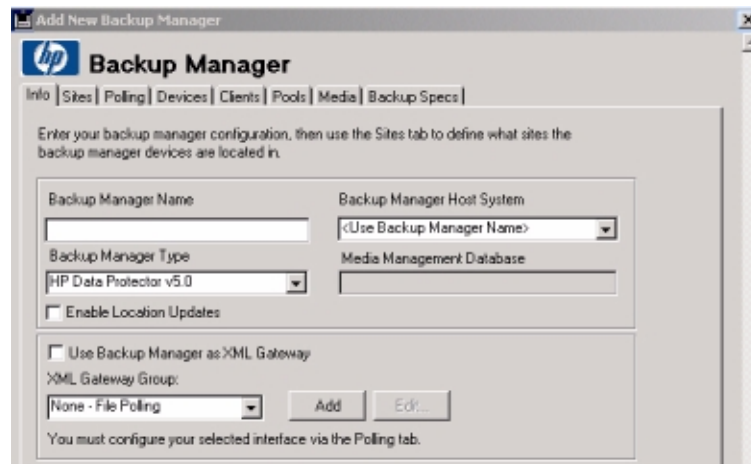
Backup Managers Screen

The screenshot shows a window titled "Backup Manager Configuration: Total Backup Managers = 55". The window contains a table with the following columns: Name, Type, Data Source, System Name, Media Mgmt DB Name, and Mgr Of Mgr Name. The table lists various backup managers, including those for HP OpenView Storage Data Protector v5.0 and HP OpenView Dinnback v4.1.

Name	Type	Data Source	System Name	Media Mgmt DB Name	Mgr Of Mgr Name
192.168.0.1	HP OpenView Storage Data Protector v5.0	External	boies150@ol.external.hp.com	boies150@ol.external.hp.com	
192.168.0.1	HP OpenView Dinnback v4.1	banban_proxy	192.168.0.1	nokeyast	
banban.ond.hp.com	HP OpenView Dinnback v4.1	peveudb	banban.ond.hp.com	banban.ond.hp.com	
bobobun01a.boies.itc.hp.com	HP OpenView Storage Data Protector v5.0	Building25	bobobun01a.boies.itc.hp.com	bobobun01a.boies.itc.hp.com	bobobun01a.boies.itc.hp.com
bobobun02a.boies.itc.hp.com	HP OpenView Storage Data Protector v5.0	Building25	bobobun02a.boies.itc.hp.com	bobobun01a.boies.itc.hp.com	bobobun01a.boies.itc.hp.com
blpnan1	Other	c:\polling	blpnan1	blpnan1	
blpnan1.spc.com	HP OpenView Storage Data Protector v5.0	Config2.abc.com	BLZZARD		
bobobun01a.boies.itc.hp.com	HP OpenView Storage Data Protector v5.0	Building25	bobobun01a.boies.itc.hp.com	bobobun01a.boies.itc.hp.com	bobobun01a.boies.itc.hp.com
bobobun02a.boies.itc.hp.com	HP OpenView Storage Data Protector v5.0	Building25	bobobun02a.boies.itc.hp.com	bobobun01a.boies.itc.hp.com	bobobun01a.boies.itc.hp.com

Double-click an existing Backup Manager or click **Edit** to edit or view.

Figure 2-64 Backup Manager — Info Screen



Provide the Backup Manager configuration information.

Type the descriptive name (or alias) of the Backup Manager System for Backup Manager Name.

Select the primary network name of the host system that is running the Backup Manager (such as `machine.company.com`) for Backup Manager Host System. If the Backup Manager System you want does not appear in the drop-down list, you can either type it in the Backup Manager Name field or add it manually under Global Objects > Systems.

Select the Backup Manager type from the list of supported Backup Managers for Backup Manager Type. If your Backup Manager is not included in the list, select Other to use the XML file import interface.

XML Gateway Group

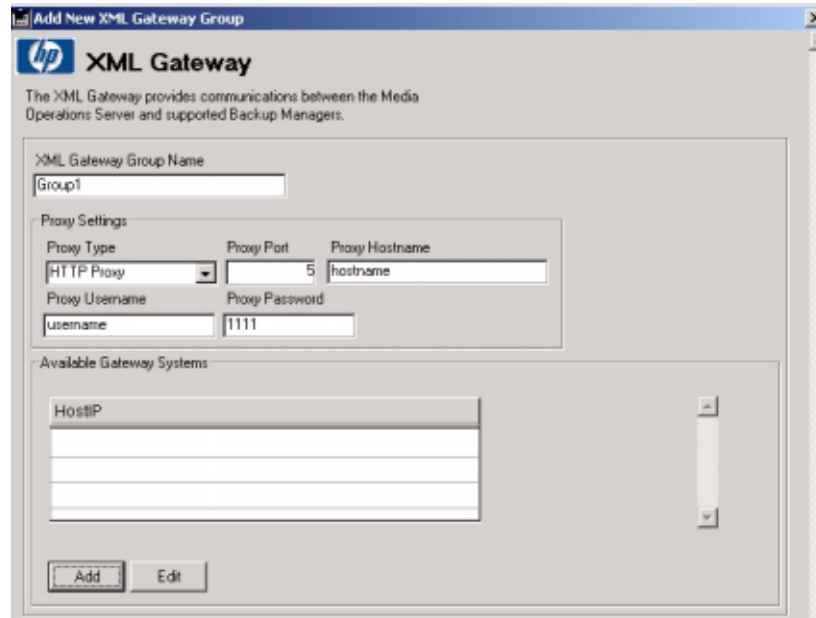
If the selected Backup Manager type is a Backup Manager that is supported by the XML Gateway, either install the XML Gateway onto the tape Backup Manager System or use the XML Gateway group used to communicate with the Backup Manager. If the selected Backup Manager type is Other, the interface mechanism is XML file import.

NOTE

The NetBackup gateway should always be present on the Master server. The XML gateway group option is not always possible.

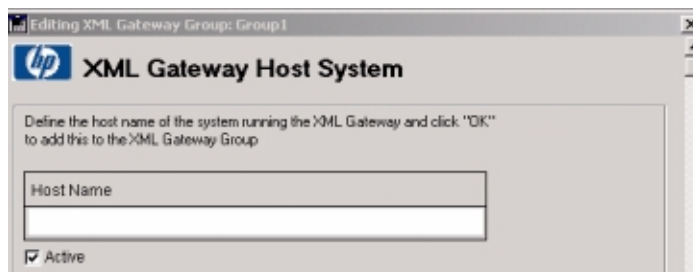
Click Add to add a new XML Gateway group. If the Cell Manager has the XMLGW installed and you do not want to use a XMLGW group, select the Use Backup Manager as XML Gateway check box. The drop-down list and Add buttons will be disabled.

Figure 2-65 XML Gateway Screen



Type the name of the XML Gateway group, which is made up of one or more XML Gateway systems. (Media Operations automatically load balances communications across all the XML Gateway systems in the group.) Type the proxy settings and then click Add.

Figure 2-66 XML Gateway Host System Screen

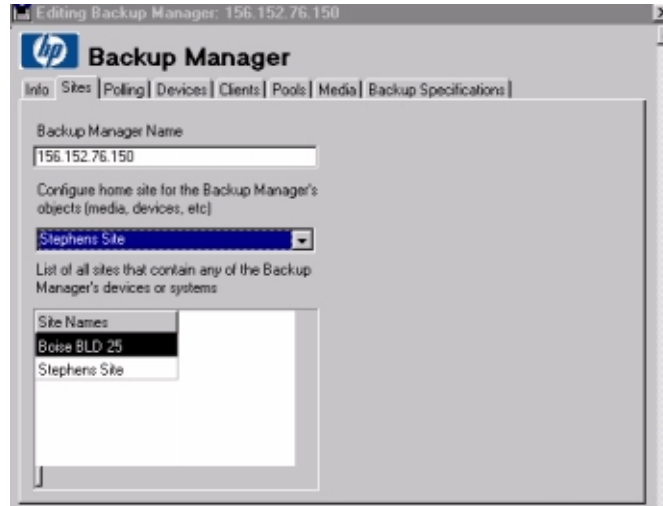


Type the host name and then click OK. You will return to the

Getting Started Using Media Operations Using Media Operations

XML Gateway screen (see Figure 2-65 on page 65). Click **OK** to return to the Backup Manager - Info screen (see Figure 2-64 on page 64). To associate a site with the Backup Manager, click the **Sites** tab.

Figure 2-67 Backup Manager — Sites Screen



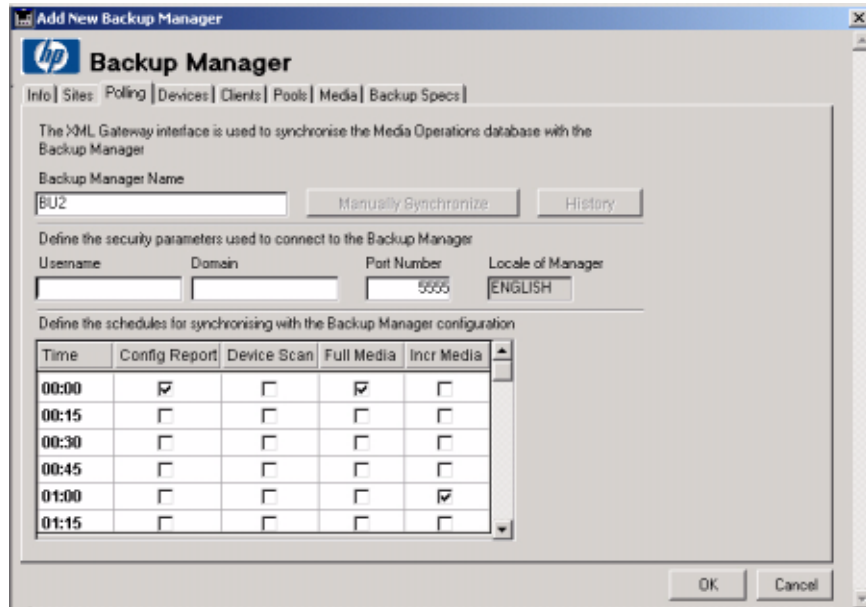
Each Backup Manager has a “home site” where its media and pools are always located and where its systems, devices, and backup specifications are placed by default if there is no appropriate site in which to locate them (such as if the sites have DNS suffixes defined). When any device or system associated with a Backup Manager is moved to another site, there is a list of used sites, shown on the Backup Manager - Sites screen, that shows all of the sites that contain objects from that Backup Manager.

You can change the home site for a Backup Manager (by clicking the **Sites** tab on the Backup Manager screen) resulting in all of that Backup Manager’s objects (media, pools, systems, devices, and backup specifications) in the original home site to be moved to the new home site. Any vaulting policies (along with any associated offsite vendor accounts) and premount job schedules associated with the moved objects are automatically copied over to the new home site (unless they already exist). If a policy exists in the new home site with the same name, but with different rules as the policy being copied, the copied policy name is made unique by propounding the original home site name to it. (This is also true for any premount job schedules.)

If the Backup Manager XML interface is set to one of the XML Gateway

groups or set to Backup Manager as XML Gateway, the Backup Manager - Polling screen is displayed.

Figure 2-68 Backup Manager — Polling Screen



To perform an immediate synchronization of all the configuration information from the Backup Manager (pools, media devices, systems, and backup specifications), click **Manually Synchronize**.

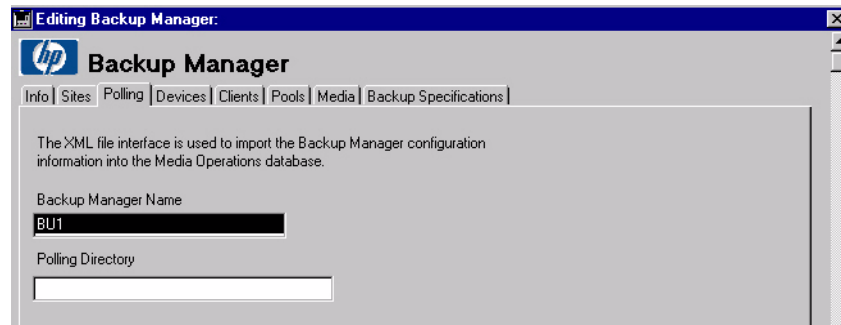
The scheduled events are used to keep Media Operations in sync with the Backup Manager:

- **Config Report** — collects the clients on the Backup Manager, its MMDB configuration, media pools, devices, and backup specifications.
- **Device Scan** — scans all devices to determine what media are loaded in them.
- **Full Media** — retrieves a full media listing from the Backup Manager.
- **Incr Media** — retrieves all media modified in the past hour along with usage information on the media.

If the Backup Manager type is **Other**, the following screen appears.

Figure 2-69

Backup Manager — Polling (Type = Other) Screen



Configure a directory path for Media Operations to use to import the XML configuration files.

Deleting Backup Manager Objects

You cannot delete Backup Manager objects (media, pools, devices, systems, and backup specifications) from the Media Operations graphical user interface (GUI), because they are automatically synchronized with the Backup Manager. This is why the `Delete` button is grayed out on these objects. (Objects you have manually created yourself can be deleted.)

A Backup Manager object is automatically deleted from Media Operations when the object is deleted from the Backup Manager by the administrator. Media Operations detects objects that have been deleted from the Backup Manager during the `Config Report` and `Full Media` scheduled polling events, so there is a delay between deleting the object in the Backup Manager and the subsequent deletion in Media Operations. However, when Media Operations detects that an object has been deleted from the Backup Manager, there are some cases where the objects are not immediately deleted in Media Operations as described below.

- The medium is *not* immediately deleted, but is instead set to pending delete and is added to a blank media vaulting job the next time vaulting jobs are created (such as the next morning). The blank media vaulting job is intended to retrieve the deleted medium from its current storage locations and return it back to the blank media bin for reuse or destruction. The medium is fully deleted from Media Operations once it has been added to a blank media vaulting job.
- Any media pools containing the pending delete media are retained

until the media are fully deleted.

- When a medium is deleted from a Backup Manager and is added to a blank media vaulting job, and the vaulting job retrieves the deleted medium from another Media Operations Server acting as an offsite vendor, the medium is automatically deleted from the offsite server after it is retrieved.
- If a backup specification is deleted from the Backup Manager, it is not deleted from Media Operations if there is still media present in the Backup Manager that contains backups from that backup specification. (This is to allow you to locate media for a checkout request based on the backup specification even though they are no longer running in the Backup Manager.) In this case, the backup specification is shown as disabled in the Media Operations GUI.

Getting Started Using Media Operations
Using Media Operations

3 **Configuring Media Operations**

Chapter Overview

This chapter describes the tasks you need to perform to configure the Data Protector. These tasks include:

“Configuring for the Physical Environment” on page 73

“Configuring Backup Processes and Objects” on page 81

“Defining Policies” on page 92

Configuring for the Physical Environment

Site Management

A site is a geographic location consisting of one or more data centers. The data centers for any one site are assumed to be in close enough proximity that they have a common set of operators. Media Operations allows you to configure and manage multiple physical sites with different service level agreements (SLAs).

You must configure at least one site.

Adding a Site

Each site is configured to define the physical layout of the site's devices and the available onsite and offsite vault locations for the site.

Sites can only be added from `Global Configuration Options > Site Management` by top-level administrators. See “Adding Sites and Backup Managers” on page 22 for details.

There are a number of aspects to creating a site. When you are adding a site, add/configure the following site objects:

NOTE

There is no specific order in which you have to accomplish these tasks, with the exception of that discussed in “Site Default Vaulting Policy” on the following page.

- **Vaults**

If the site contains secure media storage, you can reflect that physical layout in Media Operations in terms of vaults, where each vault has cabinets, drawers, rows, and slots.

You can manually add your own vault configuration to the site and then select onsite vaults as part of the media vaulting policies.

- **Offsite Storage Vendors**

You can manually add your own offsite storage vendors and accounts and then select these custom offsite locations as part of the media vaulting policies.

- **Data Centers**

Configure data centers so you can optimize premount jobs. Operators can perform the premount jobs more efficiently when the premount walk-through is grouped in a logical order by physical location. (In other words, the premount job is faster and more efficient if the operator is following the shortest/quickest path from device to device.)

You can further optimize the device walk-through order in each data center by creating data center grid locations (that have a walk-through order) that you can then assign to systems and devices.

- **Site Default Vaulting Policy**

Every site must have a default vaulting policy; you cannot create a site without assigning one. This policy is used by default when new media pools are created or added. If your default policy is going to have destination locations for vaults or offsite vendors, create the vaults and vendors before you create the vaulting policy.

Editing a Site

Once added, you can modify the physical layout of the site's devices and the available onsite and offsite vault locations for the site to reflect changes.

Sites can be edited from:

- Global Configuration Options > Site Management by top-level administrators
- Global Configuration Options > Server Parameters on the Sites tab by top-level administrators
- The Site Configuration option under each site in the shortcut bar by top-level administrators and site-level administrators for that site

“Editing” a site might mean that you are deleting it. If you delete a site, the vaults, offsite vendor accounts, data centers, and site-level user roles associated with that site are also deleted. Any manually added backup objects created within that site are deleted. Additionally, any backup objects within that site that were automatically created by a Backup Manager that is specific to the deleted site are either moved to another site (if you specify one) or the Backup Manager can be deleted with the site. If the Backup Manager is not specific to the site (for example, it is spread across multiple sites), its objects are moved to another of the Backup Manager's sites.

Vaults

Vaults are a reflection of the physical layout of the secure media storage in a site. Vaults are defined in terms of cabinets, drawers, rows, and slots — which are created in that order. See “Vaults” on page 45.

A vault has no capacity until you create rows and, by extension, slots. When you create a row, you specify the vault slot type that describes the physical characteristics of the slots in the row. In other words, you are describing what kind of media will fit in the slots. If you add a new media type to the system that does not fit into any of the defined vault slot types, add a new slot-type definition for the new media type. Then you can define rows that accept that media type. See “Adding and Modifying Media Types” on page 90 for more information.

You can either create your vaults manually a section at a time — cabinets, drawers, rows, and then slots — or you create the entire vault automatically if your vault has a structured addressing scheme for the components.

You can edit vaults only from the *Site Configuration* screen. Any user with permissions to edit sites can edit vaults. If you delete a vault, all the media contained in that vault are moved (within Media Operations) to the holding bin for the deleted vault’s site.

Vault Priorities

When you configure your vaulting policies to move media into a vault location type, Media Operations automatically puts the media into the most appropriate vault in the destination site. “Appropriate” is determined by whether the vaults support the vault-slot type for the media (will the media physically fit in the slots), whether there are free slots within the vault, the vault onsite and offsite priorities, and the reserved slots configuration.

You can assign onsite and offsite priority to each vault. Onsite priority determines which of the onsite vaults is the preferred recipient of media from the local site that are being moved into a vault. Offsite priority determines which of the onsite vaults is the preferred recipient of media from the offsite sites that are being moved into a vault.

Reserving Slots

You can reserve a range of slots for use with a specified media pool. In this case, the slots can be used only for media from the specified pool and the media from that pool can only be stored in the reserved slots assigned to them. You can use this option to control media placement by forcing media into a particular vault.

Configuring Media Operations

Configuring for the Physical Environment

You can apply this configuration at the row, drawer, or cabinet level. Everything under the reserved level is reserved for the specified pool. Click on the `Reserved Slots` tab on the `Onsite Vault Management` screen to view the list of all currently reserved slots in a vault.

Offsite Vendors and Accounts

Offsite vendors are secure media locations that are not under the control of your Media Operations Server. Offsite vendors can be other Media Operations Servers within your own company or external vendors. (Note) offsite vendors are not site specific; once defined, they can be used for any site. Each site, however, has its own unique account with the offsite vendor, so that the offsite vendor can easily identify the owner of each piece of medium. In other words, offsite vendors define locations that can be used to store media securely offsite.

Media Operations provides support for electronic links to offsite vendors. This electronic link allows Media Operations to send electronic verification of media being shipped to offsite storage and also provides electronic requests to return media from offsite storage back to the data center (such as for recovery jobs). This provides a much more reliable link to the offsite vendor compared to tracking media into and out of the offsite vendor via paper lists.

The Media Operations administrator has the ability to manually add their own offsite storage vendors and accounts and then select these custom offsite locations as part of the media vaulting policies.

These are three possible offsite vendor types (see page 26 for details):

- Media Operations
- Generic
- Iron Mountain

See “Offsite Vendors” on page 53 for detailed instructions on configuring offsite vendors. See “External Interfaces” on page B-199 for more information about using electronic link interfaces.

Data Centers

Data centers are collections of systems and backup devices within a site. For example, if your site has several buildings on the same campus, each building may have its own data center. A default data center is automatically created in each site. You cannot delete this data center, because it is the default repository for any device or system created without a specified data center (such as automatically created devices and systems).

Any system or device (whether automatically or manually created) is, by default, placed in the default data center for the system or device's currently assigned site. If you have created additional data centers in that site, you can change the data center assignment for systems and devices. See “Refining Physical Locations” on page 89 for specifics.

Grids

You can further optimize the device walk-through order in each data center by creating data center “grids” (that have a walk-through order) that you can then assign to systems and devices. Each data center grid represents a physical location (such as a grid tile). It has a unique walk-through “order key,” which determines the order in which operators are to proceed around the data center during premount jobs.

There are two ways to add or edit grids:

- while adding or editing a data center, add or edit a grid
- while adding or editing a site definition, import data center grid information by bulk file import (see “Bulk Configuration File Import” on page B-213)

Security Management

Security management is centered around a flexible, user-roles-based scheme. There are two basic kinds of users:

- product administrators
- remote accounts

You can access users in a variety of ways:

- **From Global Configuration Options > Security Management or the Users tab, or from the Remote Accounts tab on the Global Configurations Options > Server Parameters screen. These are the only points from which you can create or view top-level administrators. You defined an initial top-level administrator on installation; edit the initial administrator or add new ones with these screens.**
- **From the Site Configuration screen, the Users tab and Remote Accounts tab give you site-level access to users. You cannot view or add top-level administrators from these tabs. You can only edit or add user roles to a site-level user for the current site.**

See “Users” on page 57 for additional information about creating users.

Product Administrators

Product administrators can either be top-level or site-level administrators. For site-level administrators, the user has a role defined for each site to which they have access. A user may have different roles in different sites. The roles are listed below

Top-Level Administrator

There must always be at least one top-level administrator. The responsibilities of a top-level administrator include:

- **ability to access Global Configuration Options and Global Objects, and make additions, modifications, and deletions**
- **full rights to perform any operation for any site**
- **creates other top-level administrators**
- **maps unassigned devices to a site in a multi-site Backup Server configuration**

Site-Level Administrator

A site-level administrator has rights to one or multiple sites and can view the sites to which he or she has rights. The responsibilities of a site-level administrator include:

- full rights to perform any site-level operation
- can assign site-level, super operator-level, and operator-level administrator roles for any site they have access rights to for new or existing Media Operations users

Super Operator-Level Administrator

A super operator-level administrator performs the day-to-day operations of Media Operations. He or she can be given access to one or multiple sites and can only view the sites to which he or she has access. A super operator-level administrator does not have access to site-specific site configuration options.

The responsibilities of a super operator-level administrator include:

- performs any site-level daily operation, including premount, vaulting, scratch bin maintenance, checkout request, exception list, and mount request functions
- modifies media-level vaulting policies
- overrides media locations
- manually adds new media into manual media pools
- reassigns systems/devices between data centers in the same site
- has read-only access to some site-level information

Operator-Level Administrator

An operator-level administrator performs the day-to-day operations of Media Operations. He or she can be given access to multiple sites and can view information for the sites to which he or she has access. An operator-level administrator does not have access to site configuration options. The responsibilities of an operator-level administrator include:

- performs site-level daily operations, including premount jobs, vaulting jobs, scratch bin maintenance, checkout requests, exception list actions, and mount requests
- has read-only access to some site-level information

Remote Accounts

Remote accounts are “users” set up for the purpose of giving secure access to the current Media Operations Server from another Media Operations Server. This is so that another Media Operations Server can link to this server electronically when using the current server as an offsite vendor.

This means the “other” server will have an offsite vendor account (configured with the name of the current Media Operations Server, account ID, and password) that matches a remote user account on the current server. This ensures that any external transit requests (requests to use the current server as offsite storage and requests to retrieve previously stored media) received by this server are secure.

When you define the remote account, define which site will be used to store the media from the other server. The vaults configured on the designated site are used to store the remote account media.

Each remote account has its own media pools created automatically when media are received. A media pool is created for each different media type. For example, if the remote account name is KLAXON, the pool for LTO media would be KLAXON-LTO.

This allows you to audit what media you are storing currently and Media Operations is tracking for the remote account. You can look at media pools information from the global level or from the site level for the site to which that account is associated. You can also access this information from the `Media` tab and the `Pools` tab on the `Remote Accounts` screen.

Configuring Backup Processes and Objects

Backup processes can be of two types: automatic and manual.

Media Operations deals primarily with media lifecycle components (the media itself, the media pools, backup specifications, devices, and systems) controlled and automatically created by Backup Managers. There are, however, cases where the media and their lifecycle exist outside the control of the Backup Manager. Media Operations lets you also manage these “manually created” media.

Automatic Backup

Configuration of automatic backup processes and objects is achieved through integration with supported Backup Managers. Configuration of automatic copy processes (such as scheduled copy jobs) and objects is achieved through integration with those supported Backup Managers that have copy operation support.

NOTE

Currently HP OpenView Storage Data Protector 5.1 and 5.5 have copy operation support in Media Operations.

There are two ways of integrating with Backup Managers:

- The XML Gateway links Media Operations directly with supported Backup Managers (such as HP OpenView Storage Data Protector). This interface provides fast response time, because it is a request-response type of interface rather than polling. It does not require any complex communication path setup, because it runs over a standard HTTPS connection, which normally passes through firewalls without any special configuration. The XML Gateway is the communication component of Media Operations; it passes requests to the Backup Managers and receives responses from them. This allows it to initiate device actions (such as device scans, media initialization, and library load/eject of media) through the Backup Manager.
- The XML file import interface is an alternative interface method (see “External Interfaces” on page B-199 for details) that allows integration with other types of Backup Servers not supported by the XML Gateway.

NOTE

Automatically created backup components cannot be deleted from Media Operations while they still exist in the Backup Manager. Also, the attributes generated by the Backup Manager cannot be edited.

Manual

When you model your manual backup environment, you are doing it on a system-by-system basis. This implies that each system (or piece of a system, such as a directory or volume) must have its own manually created backup specification that represents the manual backup process for that system.

Process Flow — Manually Created Environments

- Create the media resources:
 1. Manually create a media pool. You can do this from the `Global Objects > Media Pools` list (if you are a top-level administrator) or the site-level `Media Pools` list (if you are a site-level administrator). Specify the media characteristics of the pool; media type (such as LTO), media compression type (such as LTO-1), and, optionally, barcode labelling policy.
 2. Manually create media within the pool. (You can only add media from within the pool.) You can do this from the `Media` tab of the `Media Pools Add/Edit` screen. Media created in this way acquires the characteristics of their parent media pool.
- Model the backup for the system:
 1. Manually create the system (if the system has not been created by a Backup Manager). You can do this from the `Global Objects > Systems` list (if you are a top-level administrator) or the site-level `Systems` list (if you are a site-level administrator). Specify the characteristics of the system, such as data center and grid location, in the site to which you assigned the system.

2. Manually create devices to be used for this manual backup process (if the devices to be used for the system you are modeling have not been created by a Backup Manager). You can do this from the Global Objects > Backup\Restore Devices list (if you are a top-level administrator) or the site-level Backup\Restore Devices list (if you are a site-level administrator).

Specify the characteristics of the device, such as host system (manually created devices *can* be associated with automatically created systems), media pool, and device type. (Device type must match a manual pool in the same site as the device.)

For SAN-connected devices that may be visible to multiple device hosts, you can configure separate drives to represent the different logical views of the device. Where there are multiple drives configured for a device, the device host is based on the drive that is flagged as the master.

3. Manually create a backup specification identifying the system being protected, drives to be used, and media pools from which to draw media. Manual backup specifications must also define the retention/protection period of the media. You can do this from the Global Objects > Backup Specifications list (if you are a top-level administrator) or the site-level Backup Specifications list (if you are a site-level administrator).

If you are creating the backup specification from the site level, the drives you associate with the specification must be in the same site as the specification. If you are creating it from the global level, the specification's site is set based on the first drive you associate with the specification. All drives thereafter must be from the same site. The pools associated with the drives must be manual pools that match the drive media type and must be in the same site.

Implementing the Manual Backup Process

As part of a media's lifecycle, it goes from being scratch to being used by a backup. There are two basic methods for managing this part of the lifecycle for manual media:

- When you are editing manual media, click **Mark as Used** and **Mark as Scratch** under the **Vaulting** tab on the **Media** screen. Clicking **Mark as Used** lets you specify the date of use and the relevant backup specification. Clicking **Mark as Scratch** lets you force a piece of used manual medium to return to scratch status.
- You can use the `Reactive Mount` command line utility to create a reactive mount job for a manual backup specification. When you mark that job as complete, the media selected for that job are marked as having been used by that backup specification.

NOTE

Manual backup specifications are not currently supported by scheduled premount jobs.

Backup Managers

A Backup Manager is the product that controls backup functions (such as HP OpenView Storage Data Protector). Media Operations interacts with Backup Managers to track and provide for media use.

See “Editing a Backup Manager” on page 63 for instructions on adding a Backup Manager. When adding a new Backup Manager, include a definition of the sites that contain its backup/restore devices. (This option returns an error when no sites are defined.)

The Media Operations integrates with the Backup Manager in two ways:

- integration via the XML Gateway (available for supported Backup Managers)
- integration via XML file import (Backup Manager type “Other”)

See “Backup Manager Integration” on page 6 for an overview

XML Gateway Interface

Install the XML Gateways before you configure the Backup Manager. You should consider your environment carefully before deploying the XML Gateway. See Figure 1-2 on page 7 for a representation of deployment options. The XML Gateway can be installed on a variety of server platforms, such as Microsoft Windows, HP-UX, or Solaris.

For optimum Media Operations performance, install an XML Gateway on each Backup Manager System. However, if this causes Backup Manager performance concerns, you can put the XML Gateway on other, preferably dedicated, servers. In this configuration, you can group the XML Gateways, allowing Media Operations to dynamically balance the request load and to failover transparently to a surviving XML Gateway should an XML Gateway fail. (The failed XML Gateway is re-integrated in the group when it returns on line.)

Finally, you can install the XML Gateway on the Media Operations Server System. This is recommended only if the server is a multiprocessor system or for small configurations.

NOTE

With NetBackup, the gateway should always be present on the Master server.

If you use HP OpenView Storage Data Protector or HP OpenView Omniback's Manager-of-Manager configuration and you add a Backup Manager Server that is part of the Manager of Managers (MoM), the Backup Manager and all the systems in its corresponding Media Management Database (MMDB) cluster are added automatically.

Monitoring XML Gateway Communications When you add a Backup Manager, a baseline synchronization runs. If there are any communications problems between the XML Gateway and the Backup Manager, they are revealed during the synchronization. The issues are noted onscreen and/or in the log.

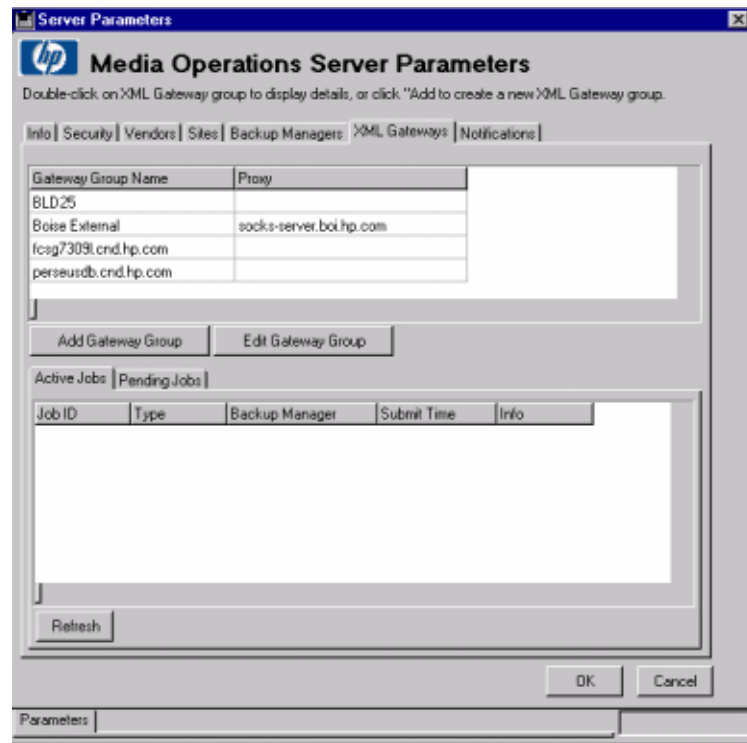
Any errors that occur while parsing the extensible markup language (XML) received from the XML Gateway are written to the alert logs. See "Viewing Alerts" on page 161 for more information.

If you want to test synchronization or force an update, you can do this by clicking **Manually Synchronize** under the **Polling** tab on the Backup Manager screen.

Configuring Media Operations Configuring Backup Processes and Objects

Clicking **History** displays a list of all previous communications from the Backup Server to the XML Gateway. This list is simply a log of whether the request from the Media Operations Server successfully reached the XML Gateway. This is used to diagnose communications problems between the Media Operations Server and its XML Gateways.

Figure 3-1 Server Parameters — XML Gateways Screen



You can monitor the XML Gateway job queue by clicking the **XML Gateways** tab on the **Server Parameters** screen. You can view active jobs and pending jobs. In addition, you can cancel pending jobs if needed.

XML Gateway Groups If you have installed the XML Gateway anywhere but on the Backup Managers, configure XML Gateway groups. You can create or edit XML Gateway groups from the `Info` tab on the `Add/Edit Backup Manager` screen or the `XML Gateways` tab on `Global Parameters > Server Parameters`.

Add more than one XML Gateway to a group to activate load balancing and failover.

Media Operations can communicate with the XML Gateway group using the proxy settings defined for that group. This makes it possible for the Backup Manager, its XML Gateway, and the Media Operations Server to be in separate networks separated by a firewall.

Media Operations supports the following proxy types: SOCKS4 basic, SOCKS4 with username/password, SOCK5 with username/password, and HTTPS Web Proxy. These proxy parameters are used for all communications to the XML Gateway group.

NOTE

If you install the XML Gateway on the Backup Manager, you can select `Use Backup Manager as XML Gateway`. You do not have to create an XML Gateway group. However, the XML Gateway group is required for support of a proxy connection from the Media Operations Server to the XML Gateway.

Polling Schedule The polling schedule defines when during the day the configuration information is extracted from the Backup Manager through the configured XML Gateways. You can create or edit a polling schedule from the `Polling` tab on the `Add/Edit Backup Manager` screen if you have XML Gateway selected as the interface type.

Because the polling schedule is used to synchronize the Media Operations configuration with the Backup Manager, you need to tune the schedules to match your backup processes.

Media Operations polls for four reports:

- **Configuration Report:** The configuration report contains the Backup Manager, media pools, devices, and backup spec information. There must be at least one Configuration Report event defined in the Backup Server polling schedule.

Configuring Media Operations

Configuring Backup Processes and Objects

- **Device Scan:** This event scans the media contents of *all* devices on the Backup Server. This event performs library barcode scans for every barcode-capable tape library on the Backup Server and will perform a media scan on all stand-alone tape drives, every library slot (except cleaning slots) in a non-barcode capable libraries, and every slot containing “blank” or “unknown” media in a barcode-enabled library. This scan should be scheduled to run (and finish) before the premount calculation process starts (see the `Info` tab on the `Global Configuration > Server Parameters` screen for this time), so that it can accurately determine how much scratch media are required and what to unload. Also, it should be scheduled to run after all the premount jobs have finished, so that the Backup Manager is aware of the new scratch media in the devices.
- **Full Media Information:** This is a list of all media in a Cell Manager. There must be at least one Full Media Information event defined in the Backup Server polling schedule.
- **Incremental Media Information:** This is a list of all media in a Cell Manager that has been used since the last full or incremental Media Information event. This report includes usage information about what backup specifications have used the media in the report, allowing Media Operations to associate media with backup specifications and the systems protected by the specifications.

XML File Import Directory

If the Backup Manager type is `Other` and the XML Gateway group is set to `None - File Polling`, the Backup Server definition includes a `Polling` tab that is used to set a unique directory on the Data Protector Server. This directory is used for the XML File Import interface for the specified Backup Server. The Data Protector software monitors this directory for any new incoming files and imports each new file detected. It automatically updates the Data Protector Database from information in the file.

You can change the polling frequency for this directory from `Global Configuration Options > Server Parameters`.

NOTE

If the XML format of the incoming files is incorrect (for example, tag ordering in the DTD is ignored by the external interface provider) or if the Backup Server name encoded in any incoming files does not match the defined Backup Server name for that file-passing directory, the

incoming file is ignored.

Any errors that occur while parsing the extensible markup language (XML) are written to the alert logs. See “Viewing Alerts” on page 161 for more information.

Database Backup

The Data Protector Server must be protected by a tape backup scheme to protect against loss of the Data Protector Database information in the event of a disaster or a failure of the Data Protector Server System.

Go into the Media Operations Server console to configure and schedule backups of the server database. See the server’s online help for more information.

IMPORTANT

The server backup process creates a copy of the server database files. It is strongly recommended that you include the server backup files in your tape backup scheme.

Tuning Backup Objects

This section discusses various methods of “tuning” or optimizing backup objects. There are two basic approaches:

- refining the physical locations of devices and systems
- refining the media compression types for pools to ensure accurate premount job estimates for the amount of required scratch media

Refining Physical Locations

You configure data centers so that you can optimize premount jobs. Operators can perform the premount jobs more efficiently when the premount walk-through is grouped in a logical order by physical location. (In other words, the premount job is faster and more efficient if the operator is following the shortest/quickest path from device to device.)

Any system or device (whether automatically or manually created) is, by default, placed in the default data center for the system or device’s currently assigned site. If you have created additional data centers in that site, you can change the data center assignment for systems and devices. Also, if you created data center grid locations for a data center

Configuring Media Operations

Configuring Backup Processes and Objects

and assign a system or device to the data center, you can also specify its grid location.

You can modify the locations for systems and devices by going to `Global Objects > Backup/Restore Devices`, `Global Objects > Systems`, or `Backup/Restore Devices` and `Systems` at the site level and edit the system or device to be tuned.

If the systems and devices are assigned to a Backup Manager, you can also edit them from the `Devices` and `Hosts` tabs on the `Edit Backup Manager` screen.

Finally, you can import system grid locations under the `Import` tab on the `Site Configuration` screen. Once you have imported the system grid locations, any devices attached to those system automatically inherit the host system's grid location.

Refining Media Compressions

All device and media objects have a media compression attribute (such as LTO-1 for a basic LTO media type). By default, the smallest media compression is set in all automatically created pools and devices.

NOTE

The media compression attribute for media pools is essential to estimating scratch media needs correctly during premount jobs.

Leaving the attribute in its default setting results in the premount job significantly overestimating the amount of media needed.

You can modify the compressions for pools and devices by going to `Global Objects > Backup/Restore Devices`, `Global Objects > Media Pools`, and `Backup/Restore Devices` and `Media Pools` at the site level and editing the pool or device to be tuned.

If the pools and devices are assigned to a Backup Manager, you can also edit them from the `Devices` and `Pools` tabs on the `Edit Backup Manager` screen.

Adding and Modifying Media Types

Media Operations contains a set of predefined media types and media compressions for most current tape technologies. You may, however, need to add to or modify these types.

If you add a media type to Media Operations that is not one of the

predefined types and you are using a supported Backup Manager or the XML File Import interface, Media Operations automatically creates the basic media type. The administrator, however, must create the new compression types for the new media. Also, if the new media type does not match an existing vault slot type, configure a new vault slot type.

You can do this from Global Configuration Options > Media Types and Compressions.

Defining Policies

There are four basic types of media policies provided to enable you to manage your physical media processes.

- **Configuring Media Vaulting Policies:** The media vaulting policy defines how long media is retained in the various device, onsite vault, and offsite vault locations.
- **Configuring Scratch Media Policies:** The scratch media policy defines “premount jobs” that manage the loading of new scratch media into the backup/restore devices for future backup jobs and at the same time remove from the devices any media that need to be vaulted (based on the vaulting policies).
- **Server Parameters:** The schedule settings indicate when processing for vaulting, scratch, and premount jobs runs.

Configuring Media Vaulting Policies

Vaulting policies are the rules that govern what happens to a piece of medium after it has been used for backup. The policies that are configured in each site are built on the framework of global vaulting policy templates. You can deploy these policies in a site at various levels to control which media in that site are affected by which policies.

If you modify a template, the modification applies immediately to every vaulting policy to which the template was originally applied. This saves you from having to make the policy modification multiple times to every place the template is applied. Every vaulting policy template is defined in terms of:

“Media Vaulting Policy Hierarchy” on page 93

“Basic Vaulting Policy Concepts” on page 94

“Vaulting Templates” on page 95

“Active Vaulting Policies” on page 95

“Defining Barcode Labeling Policies” on page 98

Media Vaulting Policy Hierarchy

Default Site-Wide Vaulting Policy Whenever a new site is created, define a default vaulting policy that is used as the default policy for all new media pools that are created in that site. This policy is configured on the `Site Configuration` screen. See “Vaulting Policies” on page 50 for an example.

- You need to first create any onsite vaults or offsite vendor locations that you will use in the site-wide vaulting policy before this policy can be applied.
- If a site-wide vaulting policy is modified, you are given the option of applying this policy change to any media pools that are still using the old default policy and, if there is any media in those pools, you are also given the option of applying the new policy to those media. (By default, the policy change only applies to new media in the pools affected by this change.)
- The site-wide vaulting policy cannot be deleted.

Media Pools All pools have a vaulting policy defined that applies to all the media in those pools. This is configured on the `Edit Media Pools` screen.

- If a pool-level vaulting policy is modified, you have the option of applying this policy change to existing media for the media pool.

Backup Specifications You can define a vaulting policy that applies to a specific backup specification (and thus apply to all media used by that backup specification). This can be used to define vaulting policies for media that contain critical data (based on the backup specification used to backup that critical data) and thus require different vaulting policies to the more general pool-level policies. This can be configured via the `Edit Backup Specification` screen.

- Any policy set at this level of the policy tree overrides any pool-level policies.
- If a backup-level vaulting policy is modified, you have the option of applying this policy change to existing media used by the backup specification.
- When a backup specification uses devices in multiple sites, you are prevented from setting a backup-level policy for that backup specification.

Systems You can define a vaulting policy that applies to a system (and thus apply to all media used by the backup specifications that reference that system). This can be configured on the `Edit Systems` screen.

- Any policy set at this level of the policy hierarchy overrides any backup-level and pool-level policies.
- If a system-level vaulting policy is modified, you have the option of applying this policy change to media associated with that system.

Single Pieces of Medium On the `Edit Media` screen, you have the option of overriding the vaulting policy set by the hierarchy. While that override is in place, the media are protected from any policy changes at higher levels.

Vaulting Policies for Copy Media For any media that belong to Backup Managers that support copy operations (such as Data Protector 5.1 and 5.5), you can define different vaulting policies (at the site, pool, backup specification, and system levels of the policy hierarchy) that apply to copy media.

For example, in pool `AB_PROD`, you can set `Policy1` as the primary policy for that pool and `Policy2` as the policy for copy media for that pool. Therefore, any media used for backups in that pool will have `Policy1` applied to them and any media that are copies will have `Policy2` applied to them. If you have applied a policy to an object in the hierarchy, but you have no copy policy defined, all media for that object, including copies, will have that objects primary policy applied to them.

Basic Vaulting Policy Concepts

Vaulting policies are comprised of a series of vaulting cycles. Each vaulting cycle describes which day, after the media were used, to move the media and where to move them. Vaulting cycles then combine to provide a time-based scheme for the media's progress through their scheduled vaulting locations.

Typical vaulting locations include a vault in the media's home site, a vault in another site on the same server, or an offsite vendor location. The type of location required depends on how secure or protected against disaster the media should be and how quickly you want to be able to retrieve them.

Vaulting Templates

Media Operations uses templates as a framework for creating active vaulting policies in each site. The templates define one or more vaulting cycles, but the specific locations inside each cycle are not final because these are site specific. For example, a vaulting cycle in a template that defines the media to be moved to an offsite vendor will not have the offsite vendor and account defined because these are different for each site.

Six vaulting templates are predefined in the Data Protector Server. These templates provide a starting point for vaulting policies for non-expert administrators. These modifiable templates provide a starting point for vaulting policies.

The default templates are as follows (see “Vaulting Policies” on page 50 for details):

- No Vaulting, Low Media Security
- Onsite Vaulting, Low Media Security
- Onsite Vaulting, Medium Media Security
- Fast Recovery Access, Low Media Security
- Medium Recovery Access, Medium Media Security
- Slow Recovery Access, High Media Security

These default templates are modifiable and deletable by the top-level administrators, who can also add their own vaulting templates. The templates are accessed through `Global Objects > Vaulting Templates`.

Active Vaulting Policies

To apply a policy to an object, the policy must exist in your site. So, the first step in applying an active policy is adding it to your site. You can add active vaulting policies through `Add/Edit Pools`, `Add/Edit Backup Specs`, and `Add/Edit Systems` screens. You can also add policies under the `Vaulting Policies` tab on the `Site Configuration` screen.

Adding Vaulting Policies The first steps are to choose a name and a template for the policy. Choosing a template constructs the framework of the vaulting cycles. Next, edit the vaulting cycles to complete their configuration, which normally represents finalizing the destination options for each vaulting cycle in the policy.

1. If the vaulting policy destination is an offsite vendor, choose the offsite vendor and which of your site's offsite vendor accounts to use.
2. If the vaulting policy destination is a vault, you can leave it at the default destination or specify another site on your Media Operations Server to store the media.
3. You might want to alter the `Day Number` value, which represents the number of days after the vaulting policy started before you move it to the destination in this vaulting cycle.
4. If the `No Later Than` day number is set to zero, but your backup jobs straddle two days, the vaulting job service level agreements (SLAs) may not be achievable. (For example, the media are only available from the backup after the shipment for the offsite vendor has left.) In this case, you can set the day number to two days and use `No Later Than` to keep in compliance with the SLA.

This option puts some flexibility into the SLA. For example, if the media are not available in time for the first day's shipment to the destination vault, the media can be manually checked into the onsite vault (by clicking `Manual Vaulting`), and when the next day's vaulting job is created, it automatically requests that you move the media from the onsite vault to the destination.

The `Optional` tab on the Vaulting Job Confirmation screen lists all the media that have not yet been sent to their destination but are within their `No Later Than` window.

5. If the `Vault When Full` day number is set to zero, but your backup job is configured to append the current day's incremental backups to the previous day's incremental media still in the device, the appending scheme will not work, because the media will be vaulted immediately after they are used for backups. In this case, you can set `Vault When Full`, which will vault the media when they have reached their vaulting day, if the media contains a full backup or the media are physically full (for example, no more backups can be appended to those media). For example, if you set the `Day Number` to

five and enable `Vault When Full`, this will retain incremental media in the device until they have been filled up or are more than five days old.

The `Optional` tab on the `Vaulting Job Confirmation` screen lists all the media that have not yet been sent to their destination but have a policy with the `Vault When Full` enabled and have become full since the vaulting job was created.

6. Use `Container Storage` to define whether to enforce container-based media movements when moving media to and from offsite locations. For example, if your offsite vendor requires you to send media in locked containers, you can support this. You can create container objects using the global or site-level `Media Containers` list by clicking `Add`. You can also create containers in your media movement jobs (specifically, vaulting, scratch bin, and checkout request jobs).
7. Use `Vaulting Days` to define which days you can ship media to their destination location. Some vendors put restrictions on which days media can be shipped to them.

Selecting Vaulting Policies Once you have added the policy, select the vault policy from the `Vaulting Policy` list for the object to which you are applying the policy.

If the application of the new policy changes the object from a previous policy, the change is implemented only when you save your changes by clicking `OK`. If there were media associated with the old vaulting policy on that object, you would be prompted to apply the policy to existing media, as well as new media, or apply the policy just to the new media.

Configuring Media Operations

Defining Policies

Viewing Active Policies Many of the backup objects list which vaulting policies are currently configured for those objects. However, if you want to find all the objects that are using a policy, you can edit the policy and look at information listed under the Pools, Systems, Backup Specs, and Media tabs. You can edit the active vaulting policies through the Edit Pools, Edit Backup Specs, and Edit Systems screens. You can also edit the policies under the Vaulting Policies tab on the Site Configuration screen, which shows a list of all the vaulting policies used in that site.

Defining Barcode Labeling Policies

If you are printing your own barcode labels, there is an option to define barcode labeling policies to provide better identification of a piece of medium from different media pools. Edit Media Pools > Barcode Policies allows you to define a barcode labeling scheme for a specific media pool.

Barcode Labeling allows you to set a prefix code and a number range for a barcode string from 6-9 characters (default is a 6 character barcode). You can set a character prefix (up to “barcode length -1” characters) and a number range (barcode length minus prefix length). The choice of how many prefix characters depends on how many pieces of medium you expect to label in the selected media pool (or group of pools). The number range can be defined as:

- Barcode Labeling
- Mixed Numeric/Characters
- Extended Numeric

Example 3-1

Barcode Number Sequence

You can set a 6-character barcode policy for media pool DATABASE to have a DB prefix and be numbered as Number Only from 0000-9999.

Printing Barcodes If you have a supported barcode printer attached to the Media Operations Manager system, you can print a range of barcodes from the Barcode Policies screen and also reprint a single barcode for a piece of medium from the Edit Media screen. Additionally, you can save the list of barcodes to a file (from the Barcode Policy screen) for easy export to third-party barcode label printing software.

When any new barcode labels are printed for a specific media pool or free pool group, they comply with the barcode labeling policy for that media

pool and start new labels from the next available number.

Configuring Scratch Media Policies

As well as providing policies to vault media from devices to onsite or offsite vaults, you have the ability to manage scratch media policies that load new scratch media into devices to use for future backup jobs. The scratch media policies are based around premount jobs, which calculate how much scratch media are required in a device and when to meet the needs of a specified list of backup jobs.

You can define a single default premount job that tells the media operators how much of all the different scratch media types is needed in every device for all the backup jobs in a site, or you can define multiple custom premount jobs to split your scratch media operations across multiple sets of backup jobs. The premount jobs to load scratch media into devices are used to dismount media from those devices for vaulting.

Configuring Premount Jobs

Every premount job defined in the Media Operations Server is specific to a single site and has a set of backup specifications and copy specifications from the site assigned to it. Every automatic backup specification and copy specification in a site is assigned to a premount job in the same site, and you cannot assign a backup specification or copy specification to multiple premount jobs in the same site.

You can edit or add premount job schedules from the `Global Objects > Premount Schedules` or from `Premount Schedules` at the site level; you can assign backup specifications to premount jobs from the `Edit Backup Specifications` screen and you can assign copy specifications to premount jobs from the `Edit Copy Specifications` screen. You also have the option of bulk assigning multiple backup specifications to a specific premount schedule by clicking `Assign to Premount` on the `Backup Specifications` screen, and you can bulk assign multiple copy specifications to a specific premount schedule by clicking `Assign to Premount` on the `Copy Specifications` screen.

NOTE

Media Operations does not currently support manually created backup specifications in premount jobs. You can either mark manual media as used or scratched through the `Edit Media` screen, or you can use reactive mount jobs.

Configuring Media Operations

Defining Policies

The premount job manages the scratch premount processes for every backup and copy specification assigned to it. The premount processes are arranged around backup/copy specification objects (rather than devices), because a backup/copy job can use multiple tape libraries or standalone drives that all need to have the appropriate scratch media loaded before the job starts. Otherwise, the job will not run.

Each site has a default premount job that cannot be deleted. By default, all backup/copy specifications in the site are assigned to this job. Create additional premount jobs if you want to segment the scratch media load across data centers or times of day.

Each premount job has a schedule that applies to all backup/copy specifications assigned to that job. The schedule specifies what days to run mount and dismount operations, and the start, warning, and due times. You can configure a premount job to dismount media to be vaulted from devices even if there are no mount operations on that day.

Tuning Scratch Media Levels

Media Operations automatically calculates required scratch media levels for each premount job based on backup specification schedules, historical backup sizes, and the media compressions defined for the pools in the backup specification. If the Backup Manager does not provide history, you can set the schedule manually and you can set the average backup sizes. These values are overwritten if the Backup Server begins to provide historical average size data.

You can optimize the scratch media levels by editing the backup specifications and, under the `Drives` tab, configuring the percentage allocation of scratch media for each drive in the specification. Normally, scratch media are distributed equally across all the drives (for example, if there are two drives, each gets 50 percent). However, if your backup jobs consistently require more media than the premount job is providing (for example, if the rate of data growth outstrips the historical data), you can adjust the allocation numbers to compensate. You can also adjust the balance across multiple libraries within the same backup specification.

Understanding Reactive Mount Requests

An ad hoc mount request is triggered by a Media Operations utility (using a command line program). These jobs react to an unforeseen demand for backup media by loading scratch media into a specified drive.

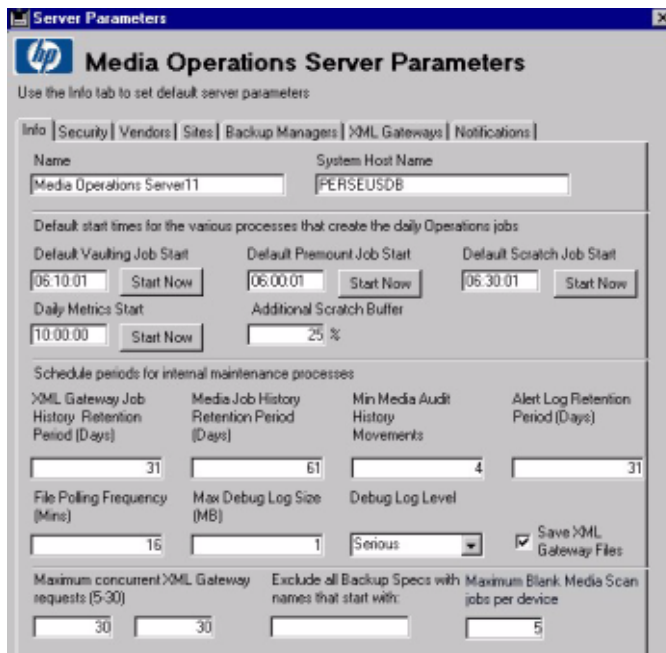
See “External Interfaces” on page B-199 for details.

Server Parameters

The `Server Parameters` screen allows you to tune the start times of the daily media movement jobs, define how much audit history is retained in your database, and define the maximum numbers of scheduled Backup Manager synchronization jobs.

Figure 3-2

Server Parameters — Info Screen



You can adjust the vaulting, scratch, and premount processing start times under the `Info` tab on the `Server Parameters` screen.

- `Default Vaulting Job Start` — This is the time of day that the process to create the days vaulting job is performed.
- `Default Premount Job Start` — This is the time of day that the process to create the days premount job is performed. (Note) this is not the time that the premons start running, but is the time that the contents of the days premons is calculated.
- `Default Scratch Job Start` — This is the time of day that the process to create the days scratch job is performed.
- `Daily Metrics Start` — This is the time of day that the process to

Configuring Media Operations

Defining Policies

create the days activity metrics is performed.

- **Additional Scratch Buffer** — The additional scratch buffer percentage defines a global adjustment to all premount job calculations.
- **XML Gateway Job History Retention Period (Days)** — Defines how long entries in the XML Gateway job history log are retained, from 1-180 days.
- **Media Job History Retention Period (Days)** — Defines how long entries in the media transit job history log are retained, from 1 to 730 days.
- **Min Media Audit History Movements** — Defines the minimum number of media movements to be retained in the media audit history for any piece of medium.
- **Alert Log Retention Period (Days)** — Defines how long entries in the alert history log are retained, from 1- 180 days.
- **File Polling Frequency (Mins)** — Defines how often to check for new files (in minutes).
- **Max Debug Log Size (MB)** — The level of message that will be entered into the debug log.
- **Debug Log Level** — Select **All** for all messages, **Warning** for all except normal messages, **Serious** for serious and critical messages, and **Critical** for *only* critical messages.
- **Maximum Concurrent XML Gateway Requests (5-30)** — (First box) Maximum number of XMLGW report jobs (such as config info, media info, and so on) that can be running at one time. (Second box) Maximum number of XMLGW Device jobs (such as device scans) that can be running at one time.
- **Exclude all Backup Specs with Names that Start with** — This field provides a method of filtering backup specifications.
- **Consolidate Scratch Bin Jobs** — Determines whether scratch bin media jobs consolidate all sources of scratch media to be returned to a site into a single job (option checked) or whether each source of scratch media to be returned to a site has its own scratch bin job.
- **Maximum Blank Media Scan jobs per device** — The maximum number of blank media scan jobs that can be running at one time.

Vaulting Jobs

The vaulting job start time defines when the vaulting jobs are created across all the sites in the Media Operations Server. The job creation time is also the start time, so the service level agreement (SLA) measurements are based on this time.

Scratch Bin Maintenance

Scratch bin start time defines when the scratch bin and scratch initialization jobs are created across all the sites in the Media Operations Server. The job creation time is also the start time, so the SLA measurements are based on this time.

Premount Jobs

The premount start time defines when the premount jobs are processed and created across all the sites in the Media Operations Server. The job creation time is not the start time; the SLA measurements are based on the defined start time for each premount job schedule.

There are a few caveats with scheduling and optimizing premount jobs:

- ✓ Make sure that the start times in the premount schedule are after the premount processing start time.
- ✓ Make sure that the device scan, if any, scheduled to run prior to premount runs prior to the premount processing start time (so that the scan happens before the premount needs are calculated).

Audit History

You can adjust the settings for how much audit history is retained in the database.

- defines how long entries in the XML Gateway job history log are retained, from 1 to 180 days
- defines how long entries in the media transit job history log are retained, from 1 to 730 days
- defines the minimum number of media movements to be retained in the media audit history for any piece of medium
- defines how long entries in the alert history log are retained, from 1 to 180 days

Configuring Media Operations
Defining Policies

4**Performing Daily Media
Operations**

Overview

All day-to-day Media Operations required to meet vaulting and scratch media policies are managed via the Daily Operations section. All daily operations are site-specific, so you must have access to a site to be able to perform that site's daily Media Operations.

This chapter describes the following:

- “Job Status Indicators” on page 107
- “Premount Jobs” on page 108
- “Vaulting Jobs” on page 115
- “Scratch Media” on page 124
- “Checkout Request (COR)” on page 137
- “Exception” on page 143
- “Mount Request” on page 144
- “Manual Vaulting Jobs” on page 146
- “Viewing Job History” on page 147
- “Web Interface” on page 149

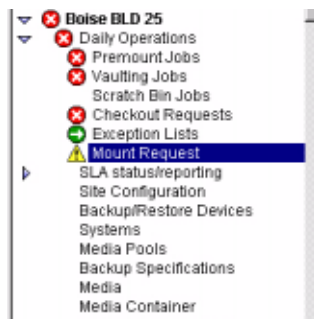
Job Status Indicators

There are three levels of job status indicators. The status indicator shows whether the vaulting policies defined in the vaulting policy hierarchy for that site are being met.

- red = overdue job — critical status job is now recorded as an SLA violation
- yellow = warning — approaching overdue time
- green = active jobs that need processing or, on an exception list, it indicates media in exception status that need to be found

Figure 4-1

Job Status Indicators



The indicator shows the overall vaulting status for that site (green for OK, yellow for warning, red for critical) and the status for each job category. The job category status is based on the SLA status settings for each active job in that category. For example, if all of the jobs in a category are green (active), except for one that is red (critical), the whole category is deemed red (critical).

Figure 4-2

Global SLA Status

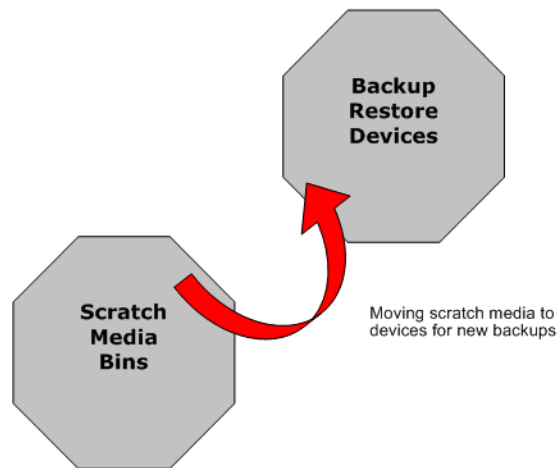
SLA ID	Start Date
2718	12/12/02
2767	12/17/02

Premount Jobs

Premount jobs preload sufficient scratch media into the backup devices to minimize the amount of scratch media used in devices and prevent mount requests with scheduled backup jobs. The premount process involves retrieving sufficient scratch media from the scratch bin, confirming that the media are scratch and of good quality, and loading the media into the assigned devices. It also takes the opportunity to dismount media from the devices needed for that day's vaulting jobs. The mount and dismount listings are ordered in the defined data center grid key for the device. This enables you to make a single pass per job without having to search for devices in the data center or on the mount/dismount lists.

Figure 4-3

Scratch Media Movement



Premount Job Listing

To view the list of active premount jobs, double-click Premount Jobs on the site's Daily Operations menu on the shortcut bar.

Figure 4-4 Premount Jobs Screen

SLA	Job ID	Schedule Name	Start Date	Start Time	Site	Due Date	Due Time
✗	1140	West Datacenter	01/11/03	07:00:00	Boise BLD 25	01/11/03	11:00:00
✗	1145	East Library	01/11/03	08:00:00	Boise BLD 25	01/11/03	12:00:00
✗	1142	Default	01/11/03	08:00:00	Boise BLD 25	01/11/03	12:00:00
✗	1141	East Datacenter	01/11/03	08:00:00	Boise BLD 25	01/11/03	12:00:00
⊕	1153	MPE - Swing	01/11/03	13:00:00	Boise BLD 25	01/11/03	17:00:00

Double-click a job or click Edit. The Premount Job - Scratch Listing screen appears.

Scratch Listing

The scratch listing displays the total number of media required from each scratch bin to complete the mount process.

Figure 4-5 Premount Job — Scratch Listing Screen

Job ID	Start Date	Start Time	Due Date	Due Time
44	01/12/03	07:00:00	01/12/03	15:00:00

Media Pool	Number of Media
AB_LTO1_SCRATCH	187
AL_LTO1	9
GB_DLT8	23
HB_DLT8_SCRATCH	62
KB_DLT8_SCRATCH	104
LB_DLT7	18
MX_LTO1	8
RB_LTO1	4
WB_DLT4	18
XB_DLT8	2
ZS_DLT8	7

Click Print Scratch Listing to print a hardcopy of the scratch listing.

Confirmation

Click the Confirmation tab to go to the Premount Job - Confirmation screen. This screen allows you to assign each piece of scratch medium to the specified device in the grid ordering for the data center. The process also confirms that the media entered are scratch and of good quality. The cataloging system that controls the media determines the quality of the media

Figure 4-6

Premount Job — Confirmation Screen

Description	Media Barcode	Library/Drive
WB0773	WB0773	BOI_HPCC538_DLT4_1
WB0595	WB0595	BOI_HPCC547_DLT4_2
WB0641	WB0641	BOI_HPCC547_DLT4_2
WB0647	WB0647	BOI_HPCC547_DLT4_1
WB0661	WB0661	BOI_HPCC547_DLT4_1
LB_DLT7	SKIP	BOI_HPCC546_DLT7_1
LB0373	LB0373	BOI_HPCC546_DLT7_1
LB2629	LB2629	BOI_HPCC878_DLT7_1
LB2786	LB2786	BOI_HPCC878_DLT7_1

Click Print Mount Listing to print a hard copy of the Premount Job - Confirmation screen. Either barcode scan or type a description of the medium and click Verify to verify the medium, or click Skip to skip the piece of scratch medium.

Confirm (by clicking Verify or Skip) all required scratch media prior to clicking Mark As Complete or you will see the following alert telling you to confirm the media.

Figure 4-7

Alert — Confirm Scratch Media



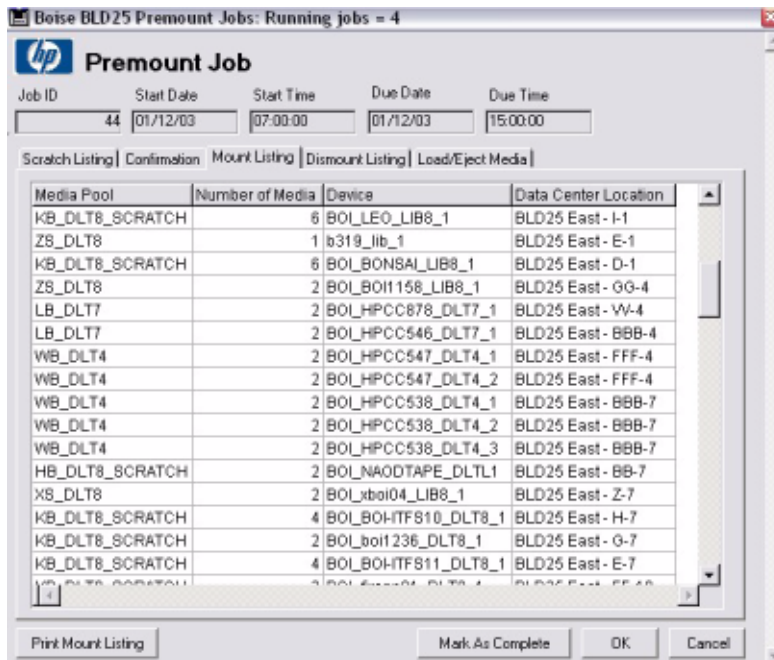
NOTE

If you click on Print Unknown Media, a list of all unknown, foreign and blank media will be printed.

Mount Listing

Check the Mount Listing tab to go to the Premount Job - Mount Listing screen. This screen displays the devices requiring media, type of media, and quantity.

Figure 4-8 Premount Job — Mount Listing Screen

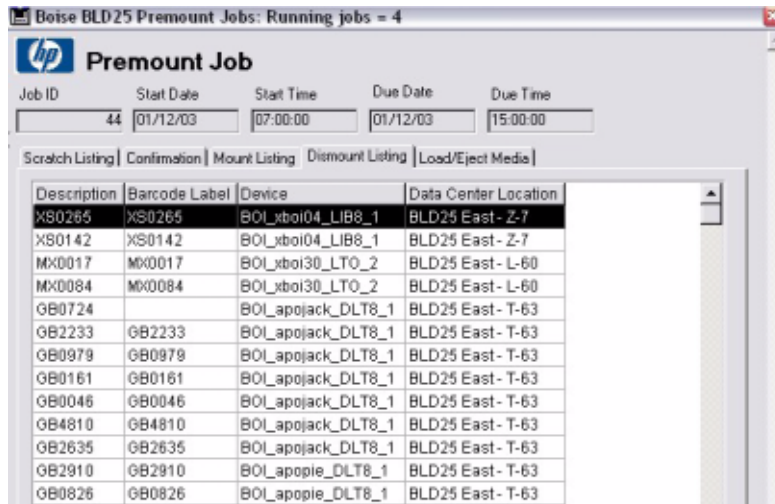


Click Print Mount Listing to print a hardcopy of the mount listing.

Dismount Listing

Click the Dismount Listing tab to go to the Premount Job - Dismount Listing screen. This screen displays all the media in the devices that you need to remove and place into the holding bin for manual check in, or that current days vaulting jobs.

Figure 4-9 Premount Job — Dismount Listing Screen



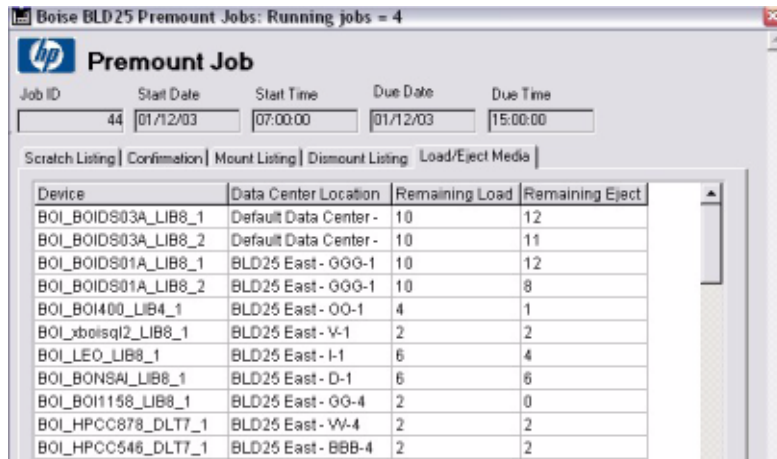
Click **Print Dismount Listing** to print a hardcopy of the dismount listing.

Load/Eject Media

Click the **Load/Eject Media** tab to go to the Premount Job - Load/Eject Media screen. This screen enables you to have media moved into and out of the cartridge access port (CAP) for the library devices in the mount/dismount lists.

The first time you click **Run Mount Cycle**, only a dismount cycle is performed (which loads the CAP up with as much media allowed that is listed on the Premount Job - Dismount Listing screen) and this dismount cycle will unload from all libraries listed on the Premount Job - Load/Eject Media screen. After verification of the dismount, the removed media are marked off. The second and subsequent cycles involve selecting the libraries from the list that have had their CAPs replaced with scratch media. The cycle then loads the contents of the CAP, verifies the media loaded, and ejects any additional dismount media until the CAP is either full or all the dismount media have been removed.

Figure 4-10 Premount Job — Load/Eject Media Screen



Click Run Mount Cycle to run the mount cycle.

NOTE

When performing load/eject operations for all silo-type library devices (such as ACSLS or DAS), there are several key differences compared to non-silo libraries:

- Configure the ID of the CAP that will be used for all Media Operations load/unload actions (for example, a CAP ID of “0,0,0” would be the CAP ID for an ACSLS library 0 CAP 0). You can configure the CAP ID by editing the silo library device and clicking the Library tab. Only one CAP ID can be used even if there are multiple CAPs in the library.
- When you click Run Mount Cycle for the first time, any silo libraries will eject *all* media listed on the Premount Job - Dismount Listing screen during this first cycle. (On non-silo libraries, it only ejects one CAPs worth of media.) This means, when you are ejecting media from a silo library, the recommended process is:
 1. Wait for the CAP to be filled and unlocked. Open the CAP. Remove all the media from the CAP.
 2. Close the CAP. (Note) on some silo libraries, you must totally empty the CAP before closing it, otherwise the library will not register that the CAP has been emptied and will not proceed to the next action.
 3. If there are more media to be ejected from this library, this

Premount Jobs

sequence is repeated until all the media have been ejected from that library.

- You cannot put the scratch media into the silo CAP until *after* you have clicked `Run Mount Cycle` for the second and any subsequent times. So, after performing the initial eject cycle by clicking `Run Mount Cycle` for the first time, the recommended process for a full load/eject cycle is:
 1. Select the silo library from the list on the `Premount Job - Load/Eject Media` screen. Click `Run Mount Cycle`.
 2. Go to the silo library and wait for the CAP to unlock. Then open the CAP and load the required scratch media into the CAP.
 3. Close the CAP. (The load will start immediately.)
 4. After all media in the CAP are loaded, any media still to be dismounted are automatically unloaded into the CAP. (This will occur only if there has been a problem in the first mount cycle.)
 5. Wait for the unload to complete and the CAP to unlock. Then open the CAP and remove media from the CAP.
 6. Close the CAP. (This will complete the load/eject cycle.)
-

Free/Scratch Pool Handling

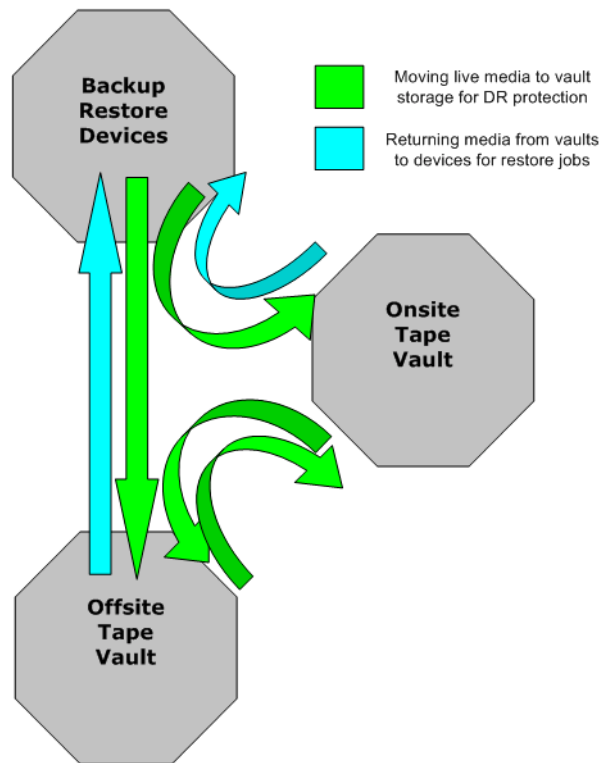
Throughout the premount job, if any of the required media pools are able to use scratch media from a dedicated free/scratch pool, then, whenever that required pool is displayed in the premount job, its free/scratch pool is also displayed as an alternative to the required pool. This means, when you are confirming the scratch media for such a pool, you can confirm scratch media from the required or free/scratch pool. A free/scratch pool is defined as an auxiliary source of media for use when there are no scratch media available in the regular pool.

Vaulting Jobs

Vaulting jobs consist of:

- vaulting job listing
- confirming a vaulting job

Figure 4-11 Vaulting Jobs Media Movement



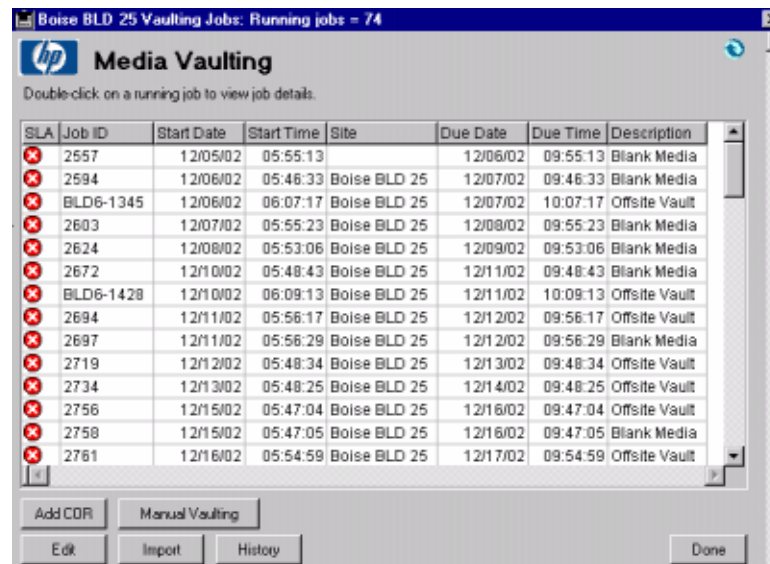
Vaulting Job Listings

Vaulting jobs are listings that display live/protected media that you need to vault or transport to a new location. These jobs are automatically created by Media Operations and are based upon the vaulting cycles defined and in use by the media.

To view the list of active vaulting jobs, double-click `Vaulting Jobs` on the site's `Daily Operations` menu on the shortcut bar.

Figure 4-12

Vaulting Job Listing



The screenshot shows the HP Media Vaulting application window titled "Boise BLD 25 Vaulting Jobs: Running jobs = 74". The window contains a table with the following columns: SLA, Job ID, Start Date, Start Time, Site, Due Date, Due Time, and Description. Each row in the table has a red 'X' icon in the SLA column. Below the table are buttons for "Add COR", "Manual Vaulting", "Edit", "Import", "History", and "Done".

SLA	Job ID	Start Date	Start Time	Site	Due Date	Due Time	Description
X	2557	12/05/02	05:55:13		12/06/02	09:55:13	Blank Media
X	2594	12/06/02	05:46:33	Boise BLD 25	12/07/02	09:46:33	Blank Media
X	BLD6-1345	12/06/02	06:07:17	Boise BLD 25	12/07/02	10:07:17	Offsite Vault
X	2603	12/07/02	05:55:23	Boise BLD 25	12/08/02	09:55:23	Blank Media
X	2624	12/08/02	05:53:06	Boise BLD 25	12/09/02	09:53:06	Blank Media
X	2672	12/10/02	05:48:43	Boise BLD 25	12/11/02	09:48:43	Blank Media
X	BLD6-1428	12/10/02	06:09:13	Boise BLD 25	12/11/02	10:09:13	Offsite Vault
X	2694	12/11/02	05:56:17	Boise BLD 25	12/12/02	09:56:17	Offsite Vault
X	2697	12/11/02	05:56:29	Boise BLD 25	12/12/02	09:56:29	Blank Media
X	2719	12/12/02	05:48:34	Boise BLD 25	12/13/02	09:48:34	Offsite Vault
X	2734	12/13/02	05:48:25	Boise BLD 25	12/14/02	09:48:25	Offsite Vault
X	2756	12/15/02	05:47:04	Boise BLD 25	12/16/02	09:47:04	Offsite Vault
X	2758	12/15/02	05:47:05	Boise BLD 25	12/16/02	09:47:05	Blank Media
X	2761	12/16/02	05:54:59	Boise BLD 25	12/17/02	09:54:59	Offsite Vault

You have several options from this screen. You can edit a job to view the `Premount Job - Confirmation` screen. You can create a checkout request, manually move media into and out of the vault, import a vaulting job, and review a history of completed jobs.

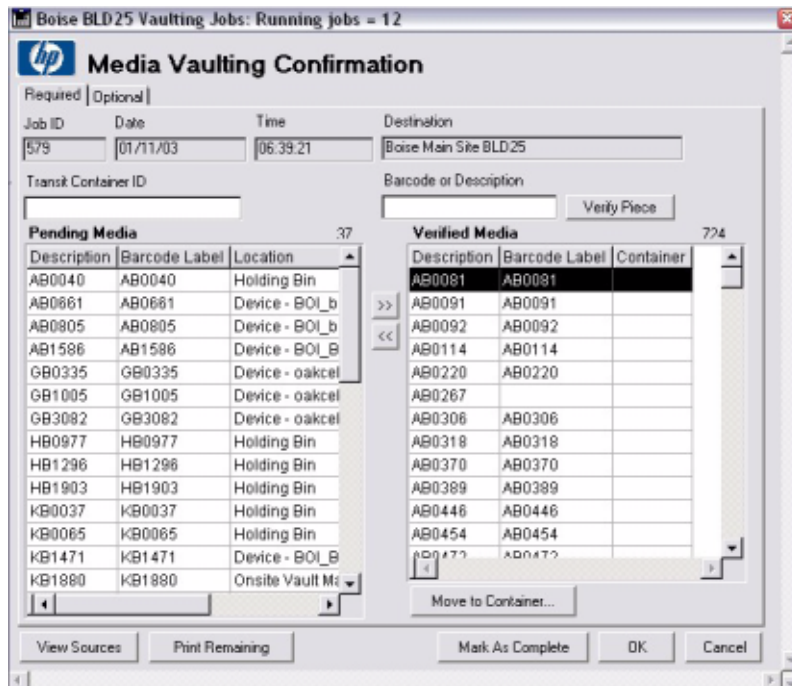
- **Edit** — Click to view the `Media Vaulting Confirmation` screen (where you can view details of the job and process the requested media movements), click `Edit` or double-click the job.
- **Add COR** — Click to create checkout requests to remove media for restores, `DRP` sessions, special projects, and so on. See “`Checkout Request (COR)`” on page 137 for additional information.

- **Manual Vaulting** — Click to submit a manual vaulting job. See “Manual Vaulting Jobs” on page 146 for additional information.
- **Import** — Click to import vaulting job request from the remote accounts. This is used to create jobs that were not automatically created on the system due to a communication error or access issue.
- **History** — Click to view completed checkout request jobs for audit reviews or to resend any completed checkout request job to an offsite vendor. You can reprint the media destination details for a completed vaulting job (for example, the destination vault name and vault slot for each piece of medium). See “Viewing Job History” on page 147 for additional information.

Vaulting Job Confirmation

Select a job and click **Edit**, or double-click a job to edit. You will see the following screen.

Figure 4-13 Media Vaulting Confirmation — Required Screen



Performing Daily Media Operations

Vaulting Jobs

The steps for confirming a vaulting job are:

1. Retrieve required media. The media in the Pending Media list are the media required for this job. Retrieve the media from their current locations. You can see the media's location on the Pending Media list.
 - However, the media could be coming from multiple source locations. So to view you required media on a source-by-source basis, you can click View Sources. From here, you can print a list of the required media from any of the sources and see the status of the media movement from each source location. When you are done printing the current source locations of the required media, click Done to return to the Premount Job - Confirmation screen.
 - If media in the Pending Media list are highlighted in red, they were marked as exceptions at the source site. This only occurs if there is an electronic link to the source site. (For example, if the source site is another Media Operations Server or it is an offsite vendor with the electronic status reporting enabled.)
 - At any time, you can click Print Remaining to print only the media still pending. This allows you to print a sublist of only the missing media.
2. Verify the requested media were found. After the media are retrieved from their current locations, either barcode scan each piece of medium, type the number and click Verify Piece; or select the medium in the Pending Media list and click >>. If the medium is prematurely verified, select it in the Verified Media list and click << to return it to pending.
3. Perform interim vault loading. If your vaulting job destination is a vault (as opposed to offsite vendor), you have the option of loading the currently verified medium into the vault without having to mark the whole job as complete. This is accomplished by clicking Vault Confirm. It allocates vaults and vault slots to that individual operator's unallocated verified media. The vault destination details are then printed.
4. Mark the job as complete. After all media are accounted for, or to move the missing media to exceptions, click Mark as Complete. You are asked if you want to exception any missing media. If you say no, the confirmation will be cancelled and you are returned to verify the

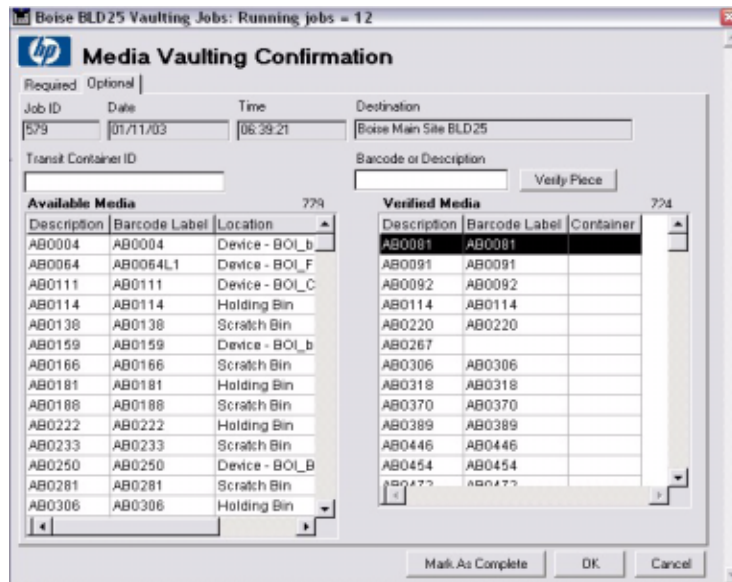
remaining media.

5. **Print out media destinations.** When you have successfully marked the job as complete, you see a print dialog. On accepting the print dialog, you get printouts detailing the destination locations for all of the media you have verified for this job (for example, the destination vault name and vault slot for each piece of medium). If for any reason the destination print out fails (for example, the printer runs out of paper), you can reprint this destination information by clicking **History** on the job list.
6. **Wait for offsite completion.** For vaulting jobs sending media to an offsite vendor that has an electronic status link (for example, if the offsite vendor is another Media Operations Server or it is an offsite vendor with the electronic status reporting enabled), then, when you mark the job as complete, the job will remain visible on the job list, because it is waiting for the job to complete at the offsite vendor. You can still view the vaulting job, but you cannot make any changes to the job. The vaulting job is automatically closed when notification is received from the offsite vendor that the job is completed; however, you can click **Mark as Complete at Destination** on the **Premount Job - Confirmation** screen if you want to manually close the job.

For offsite vaulting jobs, click the **Optional** tab to add media to the job from the data center or holding bin that are within their “move by” vaulting period as defined in the vaulting policies. The qualified media are listed on the **Media Vaulting Confirmation - Optional** screen. The process of confirming the optional media is the same as required media from the main screen.

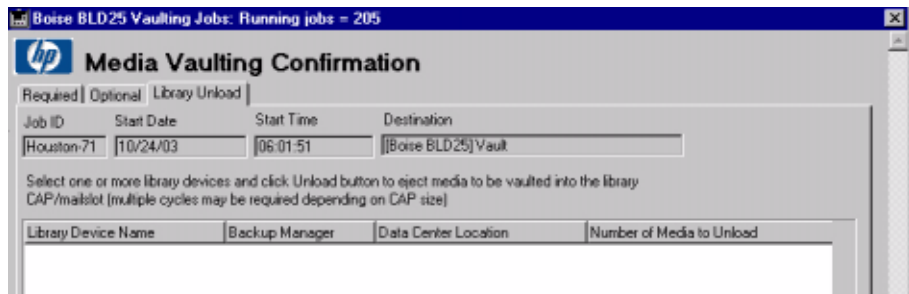
For remote account media, the media scanned are vaulted in the order scanned in the appropriate vaults. You have the option to vault tapes scanned from the beginning or since the last vaulting (vault sub lists as you go) without marking as complete. This allows you to hand the scanned media to another operator to place into the vault without having to complete the entire job first.

Figure 4-14 Media Vaulting Confirmation — Optional Screen



The Media Vaulting Confirmation - Library Unload screen lists all libraries that contain media required for this vaulting job. It lets you eject the media directly from the vaulting job.

Figure 4-15 Media Vaulting Confirmation — Library Unload Screen



Select one or more library devices and click Unload to eject media to be vaulted into the library CAP/mail slot. (Multiple cycles may be required depending on the CAP size.)

After the media are ejected, you can verify the ejected media under the Required and Optional tabs.

- Verify Piece — Click to verify the piece of medium entered using

the Media Name field.

- >> — Click to verify media highlighted in the Pending Media list and move them to the Verified Media list.
- << — Click to remove media highlighted in the Verified Media list and return them to the Pending Media list.
- View Source — Click to print media from each source location. It also allows you to re-notify a source location at another site.
- Print Remaining — Click to print all the media listed in the Pending Media list.
- OK — Click to save the job in the current state for later processing.
- Cancel — Click to cancel any actions completed since opening the job for processing.
- Mark As Complete — Click to close the job and mark any remaining pending media as vaulting exceptions.
- Move To Container — Click to move any highlighted media in the Verified Media list to another specified container.

Containers

There are two types of containers that can be used in vaulting jobs:

- **Lockable Containers:** If your vaulting job is moving media to an offsite vendor and the vaulting policy for these media specifies a lockable container must be used when sending media to this offsite vendor, the media must be assigned to a lockable container. There are rules for assigning media to lockable containers (where all the media in the lockable container must have the same vaulting policy). It is highly recommended that all of the media in the lockable container have the same protection expiry date (such as when the media becomes scratch). While verifying media that belongs in a lockable container, and there is already a lockable container in use by this job, the media are assigned to this container if appropriate, with the option for the operator to mark the container as full. If there was no appropriate container or the container was full, the operator is prompted to select a different container. If you want to reassign media to a different lockable container, select media in the Verified Media list and click Move To Container.

- **Transit Containers:** If your vaulting job is moving media to another location that does not require a lockable container, the operator has the option of selecting a transit container for transporting the media. You can assign media to a transport container by typing the container ID into the `Container ID` field before verifying a piece of medium. If you want to manually assign or reassign verified media to a container, select media in the `Verified Media` list and click `Move To Container`.

NOTE

The container columns on the pending and verified lists identify the container that the media are in (either being shipped to your site or from your site).

Multiple Users

Media Operations supports the ability for multiple operators to work on the same job confirmation at the same time. The first user to open the `Premount Job - Confirmation` screen for a job (on the Windows GUI) will be the primary owner of the job; therefore, they will be the only user to have access to `Mark as Complete`. Any subsequent operators that open the `Premount Job - Confirmation` screen for the same job receive a warning that they are only able to assist the primary owner of the job. This allows multiple users to retrieve and verify media for a job. (Each user only sees the media that they have verified.)

NOTE

If media are deleted from the Backup Manager, Media Operations automatically creates blank media vaulting jobs that retrieve the media from their current locations and return them for reuse.

Multiple Sites

If you have multiple sites configured on your Media Operations Server, depending on your vaulting policy, it is possible for a vaulting job to appear in the job list for multiple sites. The behavior for the vaulting job depends on the type of site.

- **Home Site:** The home site is defined as the originating site of the media. (The site that owns the media.) If your home site is not the destination for the media and there are media currently located in the home site that need to be moved to the destination site, home site acts as the source site. Otherwise, the home site acts as a destination site allowing you to monitor the progress of the job at the destination site

and override it if needed.

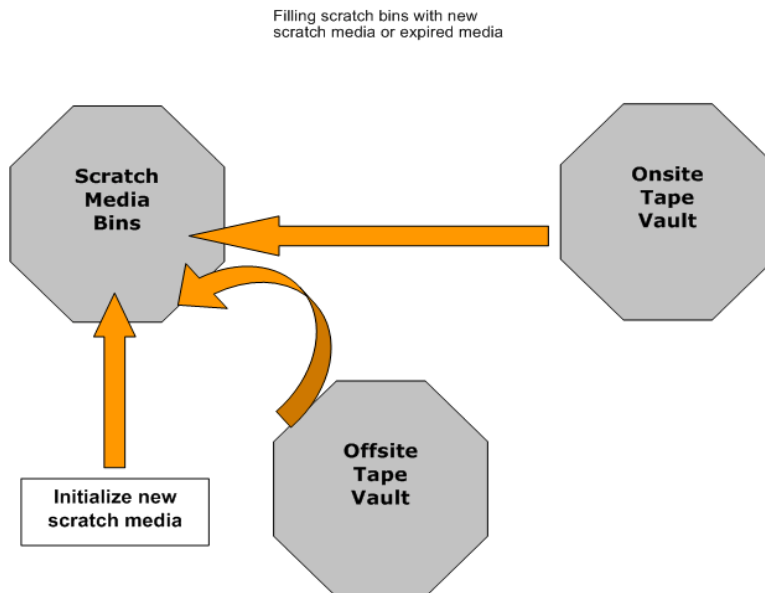
- **Source Site:** If the site is not the job destination and there are media currently located in the site that need to be moved to the destination site, then, when you verify media on the site and mark as complete, the media on the source site have been sent to the destination. This does not affect the `Pending` and `Verified` lists on the destination site.
- **Destination Site:** If the site is the job destination, then, when you verify media on the site and mark as complete, the media are now stored in their final destination and the job is closed.

Scratch Media

There are three types of scratch media jobs:

- **Scratch Bin Jobs:** This job type moves any scratch media from onsite or offsite vendors back to the scratch bins for that media type. For example, a piece of medium stored in a vault turns from protected medium to scratch medium, because its protection date has expired, thereby requiring it to be returned to the scratch bin for reuse.
- **Scratch Initialization Jobs:** If there are not sufficient scratch media in the ID scratch bins to fulfill the premount job requirements, scratch init (initialization) jobs are created to request that new media are initialized into the scratch bins.
- **Media Order Jobs:** If the Blank Bin option is enabled in the Site Configuration screen and there are not sufficient blank media to meet the requirements of future scratch initialization jobs, media order jobs are created to request that new blank media are ordered.

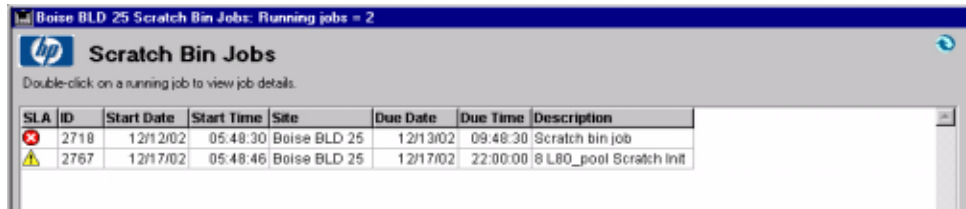
Figure 4-16 Scratch Media Movement



Scratch Jobs Listing

To view the active list of scratch jobs, double-click **Scratch Bin Jobs** on the shortcut bar under the **Daily Operations** menu for the site you are working with. The following screen appears.

Figure 4-17 Scratch Bin Jobs Screen



The screenshot shows a window titled "Boise BLD 25 Scratch Bin Jobs: Running jobs = 2". Below the title bar is the HP logo and the text "Scratch Bin Jobs". A subtitle reads "Double-click on a running job to view job details." Below this is a table with the following data:

SLA	ID	Start Date	Start Time	Site	Due Date	Due Time	Description
✖	2718	12/12/02	05:48:30	Boise BLD 25	12/13/02	09:48:30	Scratch bin job
⚠	2767	12/17/02	05:48:46	Boise BLD 25	12/17/02	22:00:00	6 L80_pool Scratch Init

You have several options from this screen. You can edit a job to view the **Premount Job - Confirmation** screen. You can also create a checkout request, manually move media into and out of the vault, import a vaulting job, edit jobs, and review a history of completed jobs. (Note) the **Add Media Order** button only appears if **Blank Bin Tracking** is enabled for the site.

- **Edit** — Click to view the **Scratch Bin Confirmation** screen (where you can view the details of the job and process the requested media movements), click **Edit** or double-click the job.
- **Add COR** — Click to create a new checkout request. See “**Checkout Request (COR)**” on page 137 for additional information.
- **Manual Vaulting** — Click to move media into and out of the scratch bin in mass. You can also remove a piece of medium from a section of the scratch bin and place it into the holding bin or vault. See “**Manual Vaulting Jobs**” on page 146 for additional information.
- **Import** — Click to import scratch bin job request from the remote accounts. This is used to create jobs that were not automatically created on the system due to a communication error or access issue.
- **History** — Click to view completed checkout request jobs for audit reviews or to resend any completed checkout request job to an offsite vendor. You can reprint the media destination details for a completed scratch bin job. See “**Viewing Job History**” on page 147 for additional information.
- **Add Init** — Click to manually create a new scratch initialization

Performing Daily Media Operations

Scratch Media

job, type the number of media to initialize, and select the pool to initialize the media into on the following screen.

Job ID
4183

Date Entered	Time Entered	Due Date	Due Time
09/10/03	14:15:14	09/10/03	14:15:14

Describe your scratch initialization job

Number of media to be initialized:
1

- Add Media Order — Click to manually create a new media order job and type the number of media to order and media type to order on the following screen.

Figure 4-18

Create Media Order Job Screen

Job ID
11476

Date Entered	Time Entered	Due Date	Due Time
02/04/04	13:11:53	02/05/04	01:11:53

Describe your media order job

Basic Media Type
[Dropdown]

Media Compression Type
[Dropdown]

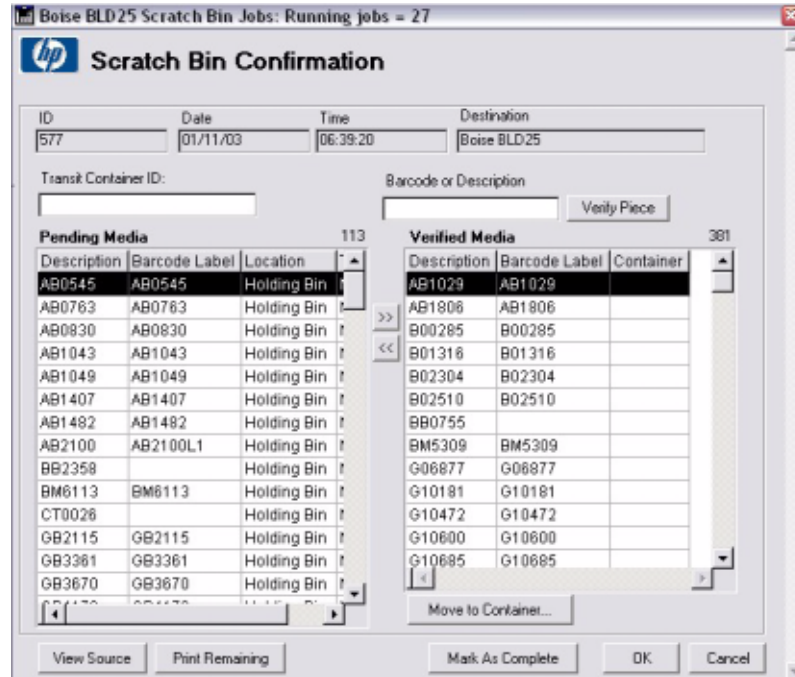
Number of media to be ordered:
1

Scratch Bin Job Confirmation

If you edited a scratch job that is a scratch bin job type, you will see the following Scratch Bin Confirmation screen.

Figure 4-19

Scratch Bin Confirmation Screen



If you are at the destination site, you will see the following Scratch Bin Confirmation screen, which has two additional tabs.

- Recycle Into Scratch Bin
- Recycle Into Library

Figure 4-20 Scratch Bin Confirmation — Recycle Into Scratch Bin Screen

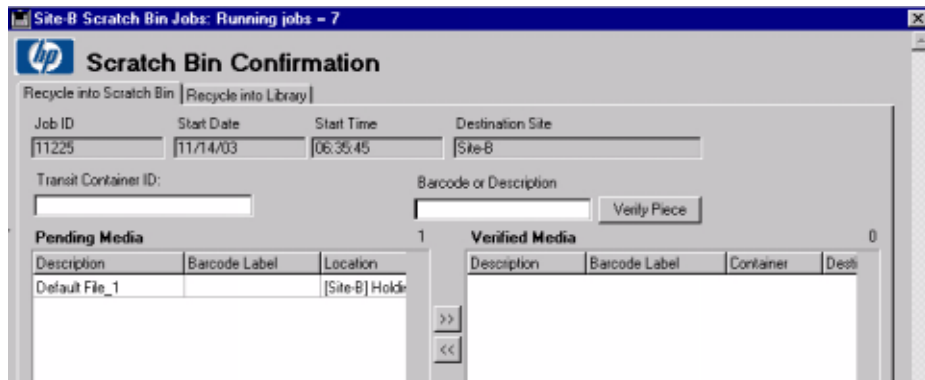
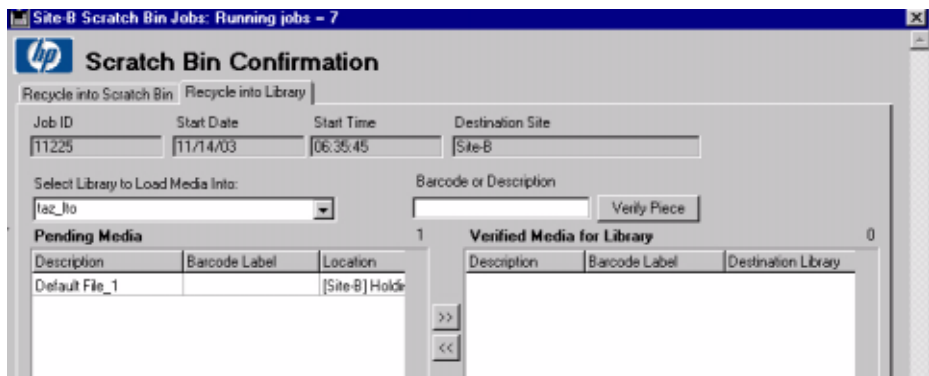


Figure 4-21 Scratch Bin Confirmation — Recycle Into Library Screen



The steps for confirming a scratch bin job are:

1. Retrieve required media. The media in the Pending Media list are the media that are required for this job. Retrieve the media from their current location. You can see the media's location on the Pending Media list.
 - However, the media could be coming from multiple source locations. So to view the required media on a source-by-source basis, you can click View Sources. From here, you can print a list of the required media from any of the sources and see the status of the media movement from each source location. When you are done printing the current source locations of the required media, click Done to return to the Premount Job - Confirmation screen.

- If media in the Pending Media list are highlighted in red, they were marked as an exception at the source site. This only occurs if there is an electronic link to the source site (for example, if the source site is another Media Operations Server or it is an offsite vendor with the electronic status reporting enabled).
 - At any time, you can click Print Remaining to print only the media still pending. This allows you to print a sublist of only the missing media.
2. Verify the requested media were found. After the media are retrieved from their current locations, either barcode scan each piece of medium, type the number and click Verify Piece, or select the medium in the Pending Media list and click >>. If the medium is prematurely verified, select it in the Verified Media list and click << to return it to pending.

If you are at the destination site, you have a choice to verify media to go to scratch bins (click Verify under the Recycle into Library tab). Any media verified under the Recycle into Library tab are loaded into the library by clicking Load Media into Libraries (multiple load cycles may be required depending on the library CAP size). Media successfully loaded into the library are marked as loaded in the Verified Media list.

3. Mark the job as complete. After all media have been accounted for, or to move the missing media to exceptions, click Mark as Complete. You will be asked if you want to exception any missing media. If you say no, the confirmation will be cancelled and you will be returned to verify the remaining media. Any media that were marked verified under the Recycle into Library tab, and were not loaded, are converted to be recycled into the scratch bin.
4. Print out media destinations. When you have successfully marked the job as complete, you will see a print dialog. On accepting the print dialog, you get printouts detailing the destination locations for all of the media you have verified for this job. If for any reason the destination print out fails (for example, the printer runs out of paper), you can reprint this destination information by clicking History on the job list.

Containers

If your scratch job is moving media to another site, the operator has the option of selecting a transit container for transporting the media. You

can assign media to a transport container by typing the container ID into the `Container ID` field before verifying a piece of medium. If you want to manually assign or reassign verified media to a container, select media in the `Verified Media` list and click `Move To Container`.

NOTE

The container columns on the pending and verified lists identify the container that the media are in (either being shipped to your site or from your site).

Multiple Users

Media Operations supports the ability for multiple operators to work on the same job confirmation at the same time. The first user to open the `Premount Job - Confirmation` screen for a job (on the Windows GUI) will be the primary owner of the job; therefore, they will be the only user to have access to `Mark as Complete`. Any subsequent operators that open the `Premount Job - Confirmation` screen for the same job receive a warning that they are only able to assist the primary owner of the job. This allows multiple users to retrieve and verify media for a job (each user only sees the media that they have verified).

Multiple Sites

If you have multiple sites configured on your Media Operations Server, depending on your vaulting policy, it is possible for a scratch job to appear in the job list for multiple sites. The behavior for the vaulting job depends on the type of site.

- **Home Site:** The home site is defined as the originating site of the media. (The site that owns the media.) If your home site is not the destination for the media and there are media currently located in the home site that need to be moved to the destination site, home site acts as the source site. Otherwise, the home site acts as a destination site allowing you to monitor the progress of the job at the destination site and override if needed.
- **Source Site:** If the site is not the job destination and there are media currently located in the site that need to be moved to the destination site, then, when you verify media on the site and mark as complete, the media on the source site have been sent to the destination. This does not affect the `Pending Media` and `Verified Media` lists on the destination site.
- **Destination Site:** If the site is the job destination, then, when you

verify media on the site and mark as complete, the media are now stored in their final destination and the job is closed.

Scratch Init

If you edited a scratch job that is a scratch init job type, you see the following Scratch Init Job Confirmation screen.

Figure 4-22

Scratch Init Job Confirmation Screen

Site-A Scratch Bin Jobs: Running jobs = 3

hp Scratch Bin Initialization

Job ID	Start Date	Start Time
4183	09/10/03	14:15:14

Description
1 Default LTO-Ultrium Scratch Init

Backup Manager	Media Pool
fedmpc02.cnd.hp.com	Default LTO-Ultrium

Number Required
1

Initialization Device
MSL5000

Initialize... Set Label Range

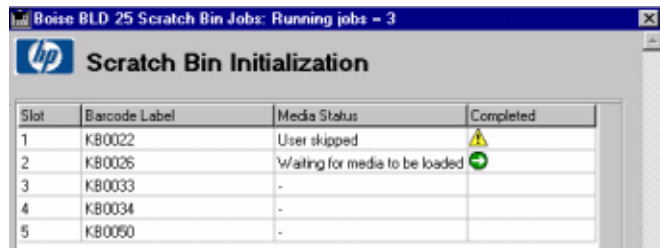
There are two ways to initialize media.

Initializing a Standalone Drive

You can select a standalone drive from a list of initialization devices. Because this is a standalone drive, you will need to define the label range of the media to be initialized.

Click **Set Label Range** to reserve a barcode label range for the number of pieces of media that you are going to initialize. After defining the barcode label range, you click **Initialize** to start the initialization process. If you do not define the label range before you click **Initialize**, you will be prompted to manually define the label for each piece of medium.

Figure 4-23 Scratch Init Standalone Drive



You are prompted to mount the first medium with the first label on the specified device. When this medium is loaded, click `Initialize` to initialize that piece of medium. `Force Initialize` needs to be enabled if you are initializing a medium that already has data on it. After the medium is initialized, you are prompted to load the second medium with the second label. This process continues until you either cancel the process or the last medium is initialized. If the media initialization fails for any reason on a piece of medium, this is shown in the status display with the red error icon and you can double-click the failed piece of medium for additional details. You can either attempt to resolve the error and click `Initialize` again to retry, or you can click `Skip` to skip to the next medium.

Initializing Using a Barcode Library

The second process for initialization uses a barcode supported library. After your media are properly labelled and loaded into the slots of the library, select the library from the device list and click `Initialize`. A barcode scan is performed on the library and a listing of blank or unknown media in the library is displayed along with their barcode labels.

Figure 4-24 Scratch Init Job Confirmation Status



Select the medium you want to initialize and click `Initialize Highlighted Media` to start the initialization process. Media Operations automatically initializes the selected medium using the barcode label for the media label. `Force Initialize` needs to be

enabled if you are initializing a medium that already has data on it. `Max Drives Used` determines how many drives inside the library can be used for the initialization process. Media Operations automatically selects only idle drives inside the library to perform the initialization process. If more media are selected for initialization than drives available, the request is queued until a drive becomes available. (This is shown as `Waiting for open drive` in the status.)

If the selected library has more than one drive block size, a drop-down list appears giving you the option of using all drives or specifying a drive block size (such as 32k or 64k), so that only drives matching the specified block size will be used for the media initialization.

If the media initialization fails for any reason, it is shown in the status display with the red error icon. You can double-click the failed medium for additional details.

After this group of media is initialized, click `Done` to return to the details screen. If there are more media required, select the next library the media are loaded in and repeat the process until the job is complete.

After all the media have been initialized, click `Mark As Complete` to close out the job.

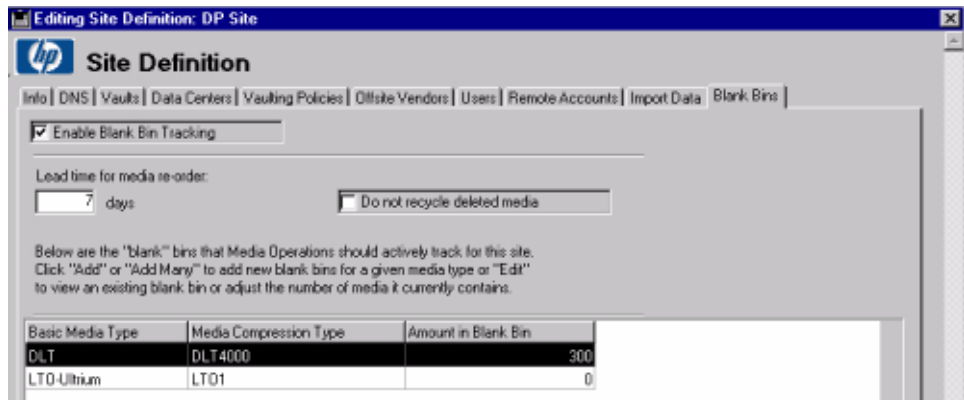
Media Reorder

If `Blank Bin` is enabled on the `Site Configuration` screen and there are not sufficient blank media to meet the requirements of future scratch initialization jobs, media order jobs are created to request that new blank media are ordered.

To activate the media reordering feature, click the `Blank Bin` tab on the `Site Definition` screen and select the `Enable Blank Bin Tracking` check box (see Figure 4-25 on page 134).

Performing Daily Media Operations Scratch Media

Figure 4-25 Site Definition — Media Reordering Screen



Basic Media Type	Media Compression Type	Amount in Blank Bin
DLT	DLT4000	300
LTO Ultrium	LTO1	0

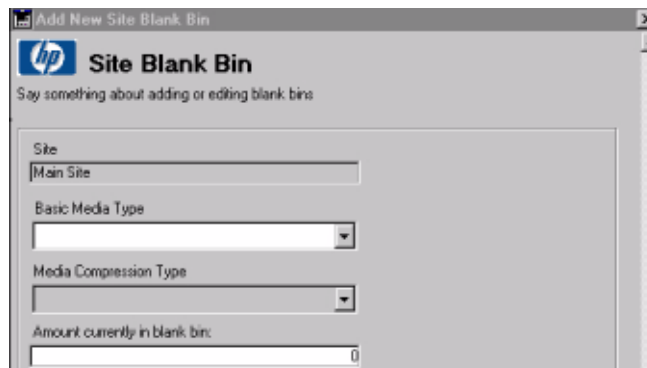
Configuring

This predicts how many media are needed for upcoming scratch initialization jobs based on criteria you set when you add a new site blank bin.

- Lead Time For Media Reorder — describes how many days before a job starts that the media need to be ordered.
- Do Not Recycle Deleted Media — Select this check box if you do not want to reuse deleted media.

Click Add or Add Many to add new blank bins for a given media type, or click Edit to view or edit an existing blank bin.

Figure 4-26 Add New Site — Blank Bin



Click OK to finish.

Confirmation

Media order jobs are created to request that new blank media are ordered. To order media, click `Scratch Bin Jobs` and then double-click the job for which you want to set up media ordering. You will see the following screen.

Figure 4-27 Media Order Screen

Media Pool	Amount Required
Default LTO-Ultrium	77
LTO_Pool Non Appendable	61

- `Job ID` — This is the identification of the job for the media being ordered.
- `Start Date` — The date the job starts for the media being ordered.
- `Start Time` — The time the job starts for the media being ordered.
- `Description` — A description of the type of media, beginning with the amount of media that are required.
- `Media Type` — The type of media being ordered.
- `Number to Order` — describes how much medium is being ordered.
- `Number Received` — The actual number of media that were received. This is an editable field.

Performing Daily Media Operations

Scratch Media

- Media Pool — describes the types of media in the pool.
- Amount Required — Describes the amount of each type of media.

When the media arrive, open the job that the media pertains to, to close the job.

Click **Mark as Complete** to finish and return to the main **Site Configuration** screen. You will now see the total number of blank media that were added.

Figure 4-28 Site Configuration — New Blank Media

Editing Site Blank bin

Site Definition

Vaulting Policies | Offsite Vendors | Users | Remote Accounts | Import Data | Blank Bins

Enable Blank Bin Tracking

Lead time for media re-order:
 days Do not recycle deleted media

Below are the "blank" bins that Media Operations should actively track for this site. Click "Add" or "Add Many" to add new blank bins for a given media type or "Edit" to view an existing blank bin or adjust the number of media it currently contains.

Basic Media Type	Media Compression Type	Amount in Blank Bin
LTO-Ultrium	LT01	138
8MM	AIT-2	0

Add Add Many Edit OK Cancel

Checkout Request (COR)

Submit a Checkout Request

Type the tracking ID from the initiator. This could be an OpenView Solutions ID, Remedy ID, or type *NONE* if it does not exist. Next, type the name of the individual who placed the request, select the priority, and type a description of the job. Optionally, select the server the media will be used on, select the destination site and location, and type the number (period) of days the media need to be removed from their vaulting cycle for this request. Type any special instructions for this job.

Figure 4-29 Checkout Request Screen

Add New Checkout Request

hp Checkout Request

Job ID
636

Date Entered: 01/11/03 Time Entered: 18:20:57 Due Date: 01/11/03 Due Time: 18:50:57

Describe your checkout request job

Request Tracking ID: Requester: Priority: High

Description: Server:

Specify the destination for the media in the checkout request.

Destination Site: Boise BLD25 Location: Holding Bin Checkout Period: 0

Instructions:

Click on "Media Selection Wizard" to assist in searching for desired media.

Enter a Media or Barcode Label: Add Media Selection Wizard

Remove Highlighted Media

Name	Barcode Label	Media Type	Current Location
------	---------------	------------	------------------

OK Cancel

Performing Daily Media Operations Checkout Request (COR)

Next, specify the medium required by either typing a number and clicking Add (if more than one match, you are prompted to select the correct medium from the displayed list), or click Media Selection Wizard to query for media meeting the criteria; media highlighted from that list are loaded into the COR. If you incorrectly include a medium, you can select it and click Remove Highlighted Media to exclude it. When you are complete, click OK to process the request. This sends notifications to each source location of the medium and will print out a COR report.

Figure 4-30 Media Selection Wizard Screen

Description	Barcode Label	Media Type	Current Location	Last Write Date
AB0629	AB0629	LTO-Ultrium	Boise Main Site	01/01/03
AB0634	AB0634	LTO-Ultrium	Boise Main Site	01/01/03
AB0639	AB0639	LTO-Ultrium	Boise Main Site	01/01/03
AB0647	AB0647	LTO-Ultrium	Boise Main Site	01/01/03
AB0649	AB0649	LTO-Ultrium	Boise Main Site	01/01/03

The Media Selection Wizard screen allows you to query for media meeting the selected filters. This allows you to quickly move a group of media into the COR without having to enter them in one at a time.

Type the desired date range and select the appropriate filters. The filters are Backup Manager, Media Pool, Backup Specification, and System. After each date or filter selection, the list of media is updated. Select the desired media and click Request Highlighted Media to move them onto the COR job.

NOTE

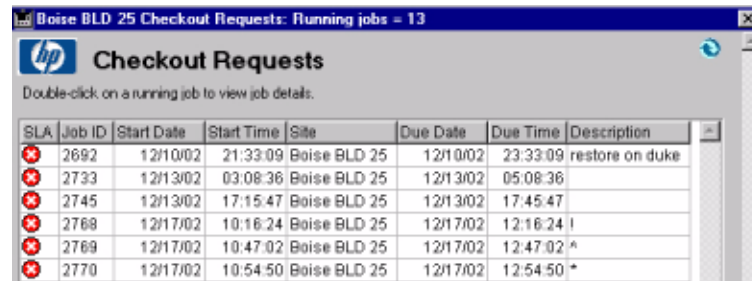
Site-level security is enforced when creating a checkout request. You are only allowed to add media that are “owned” by your site.

Checkout Request Job Listing

To view the active list of checkout requests, double-click **Checkout Requests** under **Daily Operations** on the shortcut bar for the site on which you are working. The following screen appears.

Figure 4-31

Checkout Request Job Listing



The screenshot shows a window titled "Boise BLD 25 Checkout Requests: Running jobs = 13". The window contains a table with the following data:

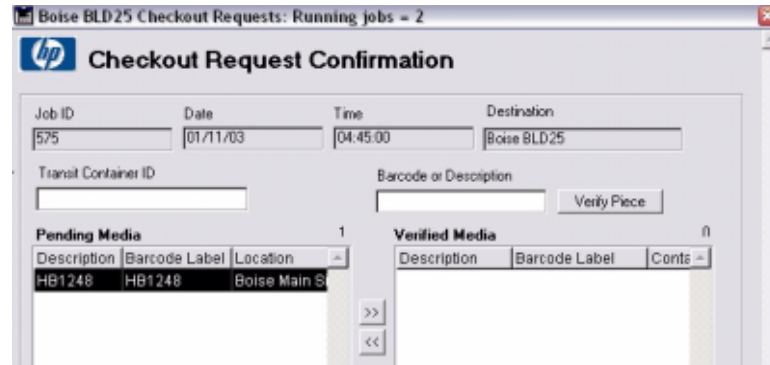
SLA	Job ID	Start Date	Start Time	Site	Due Date	Due Time	Description
✖	2692	12/10/02	21:33:09	Boise BLD 25	12/10/02	23:33:09	restore on duke
✖	2733	12/13/02	03:08:36	Boise BLD 25	12/13/02	05:08:36	
✖	2745	12/13/02	17:15:47	Boise BLD 25	12/13/02	17:45:47	
✖	2768	12/17/02	10:16:24	Boise BLD 25	12/17/02	12:16:24	
✖	2769	12/17/02	10:47:02	Boise BLD 25	12/17/02	12:47:02	*
✖	2770	12/17/02	10:54:50	Boise BLD 25	12/17/02	12:54:50	*

- **Edit** — Click to view the Checkout Request Confirmation screen (where you can view the details of the job and process the requested media movements) or double-click the job.
- **Add COR** — Click to create a new checkout request. See “Checkout Request (COR)” on page 137 for additional information.
- **Manual Vaulting** — Click to move media into and out of scratch bins in mass. You can also remove media from a section of the available medium locations and place them into the holding bin or vault. See “Manual Vaulting Jobs” on page 146 for additional information.
- **Import** — Click to import a media job from remote accounts. This is used to create jobs that were not automatically created on the system due to a communication error or access issue.
- **History** — Click to view completed checkout request jobs for audit reviews or to resend any completed checkout request job to an offsite vendor. You can reprint the media destination details for a completed checkout request job. See “Viewing Job History” on page 147 for additional information.

Checkout Request Confirmation

Figure 4-32

Checkout Request Confirmation Screen



The steps for confirming a COR job are:

1. Retrieve required media. The media in the Pending Media list are the media that are required for this job. Retrieve the media from their current location. You can see the media location on the Pending Media list.
 - However, the media could be coming from multiple source locations. So to view your required media on a source-by-source basis, you can click View Sources. From here, you can print a list of the required media from any of the sources and see the status of the media movement from each source location. When you are done printing the current source locations of the required media, click Done to return to the Premount Job - Confirmation screen.
 - If media in the Pending Media list are highlighted in red, they were marked as exceptions at the source site. This only occurs if there is an electronic link to the source site. For example, if the source site is another Media Operations Server or it is an offsite vendor with the electronic status reporting enabled.
 - At any time, you can click Print Remaining to print only the media still pending. This allows you to print a sublist of only the missing media.
2. Verify the requested media were found. After the media are retrieved from their current location, either barcode scan each piece of medium, type the number and click Verify Piece, or select the medium in

the Pending Media list and click >>. If the medium is prematurely verified, select it in the Verified Media list and click << to return it to pending.

3. Mark the job as complete. After all media have been accounted for, or to move the missing media to exceptions, click Mark as Complete. You will be asked if you want to exception any missing media. If you say no, the confirmation will be cancelled and you will be returned to verify the remaining media.
4. Print out media destinations. When you have successfully marked the job as complete, you will see a print dialog. On accepting the print dialog, you will get printouts detailing the destination locations for all of the media you have verified for this job. If for any reason the destination print out fails (for example, the printer runs out of paper), you can reprint this destination information by clicking History on the job list.

Containers

If your scratch job is moving media to another site, the operator has the option of selecting a transit container for transporting the media. You can assign media to a transport container by typing the container ID into the Container ID field before verifying a piece of medium. If you want to manually assign or reassign verified media to a container, select media in the Verified Media list and click Move To Container.

NOTE

The container columns on the pending and verified lists identify the container that the media are in (either being shipped to your site or from your site).

Multiple Users

Media Operations supports the ability for multiple operators to work on the same job confirmation at the same time. The first user to open the Premount Job - Confirmation screen for a job (on the Windows GUI) will be the primary owner of the job; therefore, they will be the only user to have access to Mark as Complete. Any subsequent operators that open the Premount Job - Confirmation screen for the same job receive a warning that they are only able to assist the primary owner of the job. This allows multiple users to retrieve and verify media for a job. (Each user only sees the media that they have verified.)

Multiple Sites

If you have multiple sites configured on your Media Operations Server, then, depending on your vaulting policy, it is possible for a vaulting job to appear in the job list for multiple sites. The behavior for the checkout request job depends on the type of site.

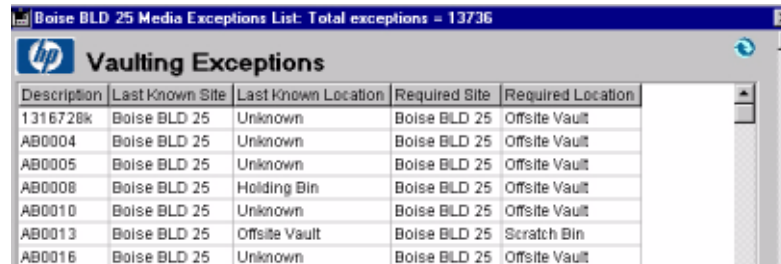
- **Home Site:** The home site is defined as the originating site of the media. (The site that owns the media.) If your home site is not the destination for the media and there are media currently located in the home site that need to be moved to the destination site, home site acts as the source site. Otherwise, the home site acts as a destination site, allowing you to monitor the progress of the job at the destination site and override if needed.
- **Source Site:** If the site is not the job destination and there are media currently located in the site that need to be moved to the destination site, then, when you verify media on the site and mark as complete, the media on the source site have been sent to the destination. This does not affect the Pending Media and Verified Media lists on the destination site.
- **Destination Site:** If the site is the job destination, then, when you verify media on the site and mark as complete, the media are now stored in their final destination and the job is closed.

Exception

This displays the list of media that were placed into vaulting exception status. A piece of medium is in an exception status when the piece that was required in the vaulting, scratch bin, or checkout request job could not be located (for example, the medium is lost). Whenever you verify a piece of medium in any medium movement and mark the job as complete, if that medium was in the exceptions list, it is removed from exception status as it was successfully verified (for example, it is no longer lost). To manually clear a piece of medium from the exceptions list, select the medium and either manually add the medium under the **Optional** tab in an offsite vaulting job or click **Manual Vaulting** to submit a manual vaulting job that moves the medium into the local vault or holding bin.

Figure 4-33

Vaulting Exception Screen



The screenshot shows a window titled "Boise BLD 25 Media Exceptions List: Total exceptions = 13736". The window contains an HP logo and the text "Vaulting Exceptions". Below this is a table with the following data:

Description	Last Known Site	Last Known Location	Required Site	Required Location
1316728k	Boise BLD 25	Unknown	Boise BLD 25	Offsite Vault
AB0004	Boise BLD 25	Unknown	Boise BLD 25	Offsite Vault
AB0005	Boise BLD 25	Unknown	Boise BLD 25	Offsite Vault
AB0008	Boise BLD 25	Holding Bin	Boise BLD 25	Offsite Vault
AB0010	Boise BLD 25	Unknown	Boise BLD 25	Offsite Vault
AB0013	Boise BLD 25	Offsite Vault	Boise BLD 25	Scratch Bin
AB0016	Boise BLD 25	Unknown	Boise BLD 25	Offsite Vault

Mount Request

An asynchronous mount request is an Interactive Mount Request screen that mounts one piece of medium at a time.

Media Operations comes with a Java-based command line utility that allows you to submit reactive mount requests from any client system into the Media Operations Server. A reactive mount request is an ad hoc mount request that reacts to an unforeseen demand for backup media by loading scratch media into a specified drive.

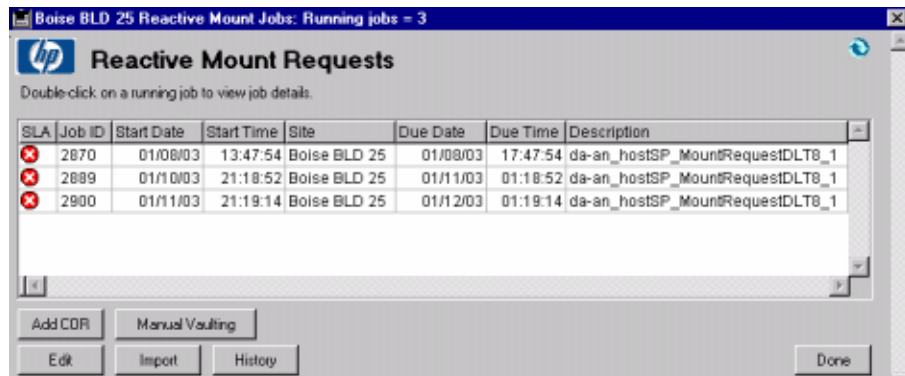
See “Reactive Mount Request Utility” on page B-206 for additional information.

Mount Request Listing

To view the active list of mount requests, double-click Mount Requests under Daily Operations for the site you are working with. The following screen appears.

Figure 4-34

Reactive Mount Requests Screen



- **Edit** — Click to view the Mount Request screen (where you can view the details of the job and process the requested media movements) or double-click the job.
- **Add COR** — Click to create a new checkout request. See “Checkout Request (COR)” on page 137 for additional information.

- **Manual Vaulting** — Click to move media into and out of scratch bins in mass. You can also remove media from a section of the available media locations and place them into the holding bin or vault. See “Manual Vaulting Jobs” on page 146 for additional information.
- **Import** — Click to import a media job from remote accounts. This is used to create jobs that were not automatically created on the system due to a communication error or access issue.
- **History** — Click to view completed mount request jobs for audit reviews or to resend any completed checkout request job to an offsite vendor. See “Viewing Job History” on page 147 for additional information.

Mount Request Job Confirmation

Figure 4-35

Interactive Mount Request Screen

The screenshot shows a window titled "Boise BLD 25 Reactive Mount Jobs: Running jobs - 2" with the HP logo and "Interactive Mount Request" header. The "Media to be Mounted" section contains a "Barcode or Description" field with a "Verify Piece" button, a "Media Pool" dropdown set to "L80_pool", and an "Available scratch media" list with items: "[C00013] Default DLT_42", "L80_pool_3", "[C00022] DP00022", and "L80_pool_5". The "Destination Device Location" section has "Library Name" set to "L80", "Datacenter" set to "BLD 25 East", and "Datacenter Location" set to "A-53". At the bottom are buttons for "Mark As Exception", "Mark As Complete", and "Cancel".

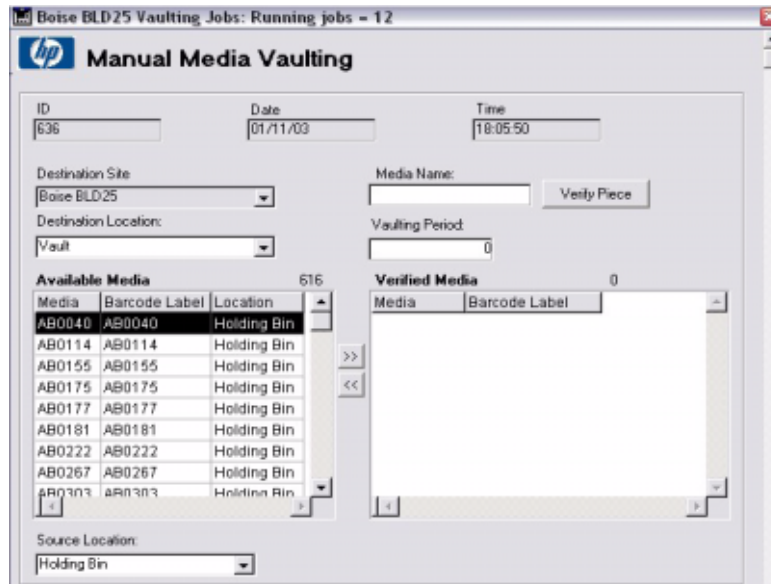
Select a scratch medium from the Available scratch media: list or scan/type a medium into the verify field. Once the medium is pulled from the scratch bin and verified, click Mark as Complete to verify the mount request. If no scratch media are available, cancel the request until scratch media are available. If you cannot locate any of the listed pieces of available scratch media, select one and mark the request as an exception to remove it. (This will add the piece of lost scratch medium to the exceptions list.)

Manual Vaulting Jobs

Manual vaulting allows you to move media into and out of the vault in mass. You can also place media from the dismount lists that were not on a regular vaulting job. This allows you to slot media from the holding bin into the vault. You can remove media from a section of the vault and place them into the holding bin or scratch bin. This allows special projects to be performed on the vault.

Figure 4-36

Manual Media Vaulting



Select the destination site and location. The available media are filtered to the source location pull down. Select media from the Available Media list and click >> to include them into this movement job. You can type the medium number and click Verify Piece or barcode scan it to include in on the job. Barcode scanned or typed media are queried from all locations not just the source location. If you miss-scan or miss-type a piece of medium, select it in the Verified Media list and click << to remove it. After all media are entered, click OK to assign them to the new location. A vaulting sheet will be printed listing the media in the order scanned, which is also the order they are assigned to vault slots.

Viewing Job History

History

The Media Vaulting - History screen allows you to view a completed job for audit reviews or to resend a job to an offsite vendor. Type a date range and click Update to view the list of completed vaulting jobs in that date range.

Figure 4-37 Media Vaulting — History Screen



The screenshot shows a web application window titled "Boise BLD25 Vaulting Job History: Number of jobs = 4". The application has the HP logo and the title "Media Vaulting". Below the logo, there is a prompt: "Enter a date range to view and click update to view the range." There are two input fields for "Starting Date" and "Ending Date", both containing "01/11/03", and an "Update" button. Below this is the instruction "Double-click on a job to view job details." A table displays the job history with the following data:

SLA	Job ID	Start Date	Start Time	Site	Due Date	Due Time	Description
	608	01/11/03	09:19:51	Boise BLD25	00/00/00	00:00:00	
	607	01/11/03	09:14:20	Boise BLD25	00/00/00	00:00:00	
	606	01/11/03	09:07:13	Boise BLD25	00/00/00	00:00:00	
	579	01/11/03	06:39:21	Boise BLD25	01/11/03	10:39:21	Offsite Vault

Double-click any of the jobs in the list on the Media Vaulting - History screen (or click View) to view the job details. The following screen is displayed for vaulting, scratch bin, checkout request, manual vaulting, and mount request job types. It includes the list of media that were due to be moved by that job, where they were moving from, and their destination. Any pieces of medium that were marked as exceptions in this job are shown in the status column. Also, the user that marked the job as complete and the date/time of completion is shown along with details of which user verified each piece of medium.

Figure 4-38 Standard Job Details

The screenshot shows a window titled "Vaulting Job Info: Job = 2829". The main heading is "Vaulting Job Information" with the HP logo. The form contains the following fields:

Job ID	Start Date	Start Time	Due Date	Due Time
2829	01/03/03	05:46:09	01/04/03	09:46:09

Description: Scratch bin job

From Location: [Empty] To Location: Stephens Site Scratch Bin

Total number of media: 21 Number of errors: 0

Date Completed: 01/11/03 Time Completed: 16:08:04 Sign off user name: Stephen Gold

Description	Barcode Label	Moved From Location	Status	User Name
AB1503	AB1503	Boise Main Site - Container: mycontainer	✓	Stephen Gold
AB1751	AB1751	Boise Main Site - Container: mycontainer	✓	Stephen Gold
InitTest		Holding Bin	✓	Stephen Gold
KB0978	KB0978	Boise Main Site - Container: mycontainer	✓	Stephen Gold
KB0988	KB0988	Boise Main Site - Container: mycontainer	✓	Stephen Gold
KB1094	KB1094	Boise Main Site - Container: mycontainer	✓	Stephen Gold
KB2397	KB2397	Boise Main Site - Container: mycontainer	✓	Stephen Gold

If the job was a scratch list job, the following screen of job details is displayed.

Figure 4-39 Scratch Init — History Screen

The screenshot shows a window titled "Vaulting Job Info: Job = 2729". The main heading is "Scratch Init Job Information" with the HP logo. The form contains the following fields:

Job ID	Start Date	Start Time	Due Date	Due Time
2729	12/12/02	05:48:49	12/12/02	22:00:00

Description: 3 CT_LTO Scratch Init

Backup Manager: bobcsbum01a.boise.itc.hp.com Media Pool: CT_LTO

Number Of Media: 3

Date Completed: 00/00/00 Time Completed: 00:00:00 Approved By: [Empty]

Web Interface

The Media Operations web GUI provides an alternate interface to perform daily operations.

The web interface is precisely the same as the Media Operations Manager daily operations with one exception, it only allows you to view 250 jobs at a time. To view the next set of 250, click **Next**. When printing out a listing, you will only be able to print the current view of 250 jobs. Also, it provides media information and SLA reporting to assist in running daily operations.

Figure 4-40 Web Interface

The screenshot shows the HP Media Operations web interface. At the top, it displays the user name 'Welcome, Stephen Gold', a 'Log out' link, a 'Help' link, and the location 'UNITED STATES'. Below this is the HP logo and the text 'Boise BLD 25' and 'Media Operations'. A sub-header indicates 'Boise BLD 25 Currently Active Jobs' with a count of '0-74 of 74'. On the left, there is a navigation menu with 'Change Site' and sections for 'Daily Operations' (including Premount Jobs, Vaulting Jobs, Checkout Requests, Scratch Bin Jobs, Mount Requests, Exception List, and Media Listing) and 'Site Reporting' (including SLA Status and Scratch Media Report). The main content area is a table of active jobs.

SLA	ID	Date	Time	Due Date	Due Time	Description
×	2557	12/5/2002	05:55:13	12/6/2002	09:55:13	Blank Media
×	2594	12/6/2002	05:46:33	12/7/2002	09:46:33	Blank Media
×	BLD6-1345	12/6/2002	06:07:17	12/7/2002	10:07:17	Offsite Vault
×	2603	12/7/2002	05:55:23	12/8/2002	09:55:23	Blank Media
×	2624	12/8/2002	05:53:06	12/9/2002	09:53:06	Blank Media
×	2672	12/10/2002	05:48:43	12/11/2002	09:48:43	Blank Media
×	BLD6-1428	12/10/2002	06:09:13	12/11/2002	10:09:13	Offsite Vault
×	2692	12/10/2002	21:33:09	12/10/2002	23:33:09	restore on duke
×	2694	12/11/2002	05:56:17	12/12/2002	09:56:17	Offsite Vault
×	2697	12/11/2002	05:56:29	12/12/2002	09:56:29	Blank Media
×	2719	12/12/2002	05:48:34	12/13/2002	09:48:34	Offsite Vault
×	2734	12/13/2002	05:48:25	12/14/2002	09:48:25	Offsite Vault
×	2733	12/13/2002	03:08:36	12/13/2002	05:08:36	
×	2745	12/13/2002	17:15:47	12/13/2002	17:45:47	

Performing Daily Media Operations
Web Interface

5**Status and Reporting Interfaces**

Overview

Media Operations is based around service level agreements (SLAs) for the media lifecycle (set by your vaulting policies and scratch policies), and you can use the SLA Status/Reporting options to check whether your SLAs are being met. You can monitor whether any configuration errors have occurred that required your intervention and generate reports. You can view SLA status, view alerts, and run reports at both the global level and the site level. You can configure automatic notification by e-mail or to OpenView Operations (OVO) for key events, such as alerts, job creation, SLA warnings, and metrics.

This chapter comprises the following topics:

“Viewing Current SLA Status” on page 153

“SLA Status Configuration” on page 158

“Viewing Alerts” on page 161

“Reports” on page 163

“Additional Reports” on page 165

“Notifications” on page 166

“Location Audits” on page 179

Viewing Current SLA Status

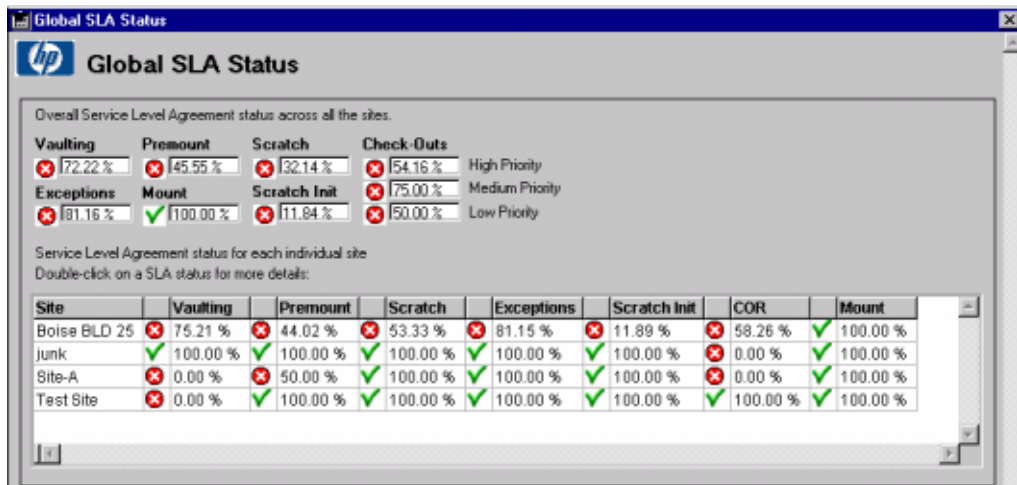
There are two levels of SLA status: global and site. There are SLA status settings for:

- **Vaulting Jobs** — move media around onsite and offsite vault locations.
- **Premount Jobs** — are scheduled jobs to load scratch media into drives/libraries to meet predicted backup needs.
- **Mount Request Jobs** — are asynchronous requests to load a scratch media into a drive.
- **Scratch Jobs** — move expired media back to scratch bins.
- **Scratch Init Jobs** — request new scratch media to be initialized.
- **Checkout Requests** — request media to be retrieved from their current location (such as for a data restore).

You can have two different priorities of checkout request job exceptions:

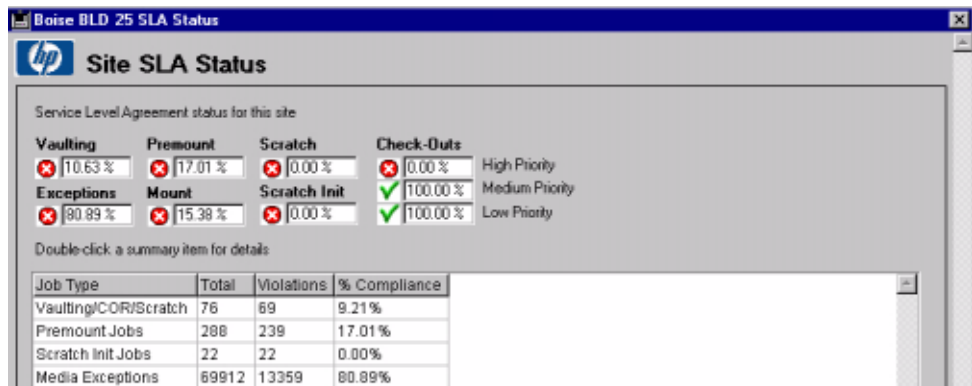
- SLA measurements for these SLA indicators are based on the SLA configuration.
- If you click `SLA Status For All Sites` on the Global SLA Status/Reporting menu on the shortcut bar, the following Global SLA Status screen shows the overall SLA status settings measured across all sites, plus the site-level SLA status indicators for each site.

Figure 5-1 Global SLA Status Screen



If you click one of the sites on the Global SLA Status screen or go into site SLA Status from the site level, there is a screen showing the nine SLA status indicators for just that site. On the Site SLA Status screen, you see an option to view details of the overdue jobs that caused these SLA status settings.

Figure 5-2 Site SLA Status Screen



The summary list shows how many jobs were overdue in the main job types.

- Vaulting/Check-Outs/Scratch — represents all the vaulting, scratch, COR, and mount request jobs that have run on that site.

- Premount — represents the premount jobs run on that site.
- Scratch Init — represents the scratch init jobs run on that site.
- Exceptions — represents the numbers of media owned by that site that are “lost” (in the exceptions list).

On the Site SLA Status screen, if you click Vaulting/COR/Scratch, you see a list of all the overdue jobs in this category. You can view any of the jobs from this historical record to see the details of the job, what media was moved by the job (and which user verified each media movement), plus details of when the job was completed and who marked it as complete.

Figure 5-3 Vaulting Job Information Screen

Vaulting Job Information

Job ID: 2810 Start Date: 01/01/03 Start Time: 05:48:26 Due Date: 01/02/03 Due Time: 09:48:26

Description: Offsite Vault

From Location: Boise BLD 25 To Location: Boise Main Site

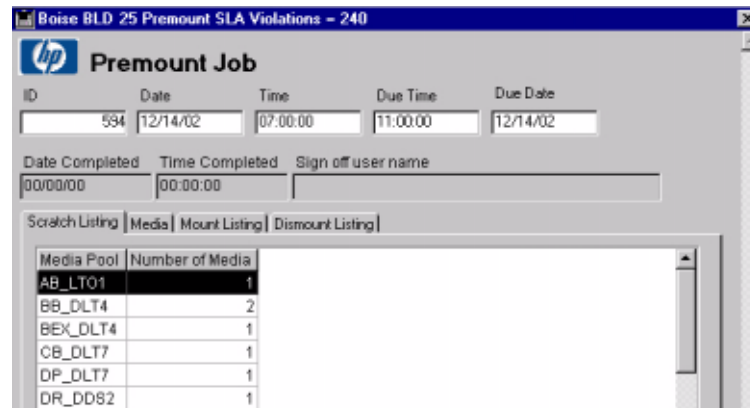
Total number of media: 20 Number of errors: 0

Date Completed: 00/00/00 Time Completed: 00:00:00 Sign off user name:

Description	Barcode Label	Moved From Site	Status	User Name
AB1751	AB1751	Boise Main Site - Container: mycontainer	✓	
KB0978	KB0978	Boise Main Site - Container: mycontainer	✓	
KB0988	KB0988	Boise Main Site - Container: mycontainer	✓	
KB1094	KB1094	Boise Main Site - Container: mycontainer	✓	
KB2397	KB2397	Boise Main Site - Container: mycontainer	✓	
KB3876	KB3876	Scratch Bin	✓	
KB7988	KB7988	Unknown	✓	

On the Site SLA Status screen, if you click Premount Jobs, you will see a list of all the overdue jobs in this category. You can view any of the jobs from this historical record to see the details of the job, what scratch media was meant to be loaded into devices, and what media was meant to be dismounted, plus details of when the job was completed and who marked it as complete.

Figure 5-4 Premount Job Screen



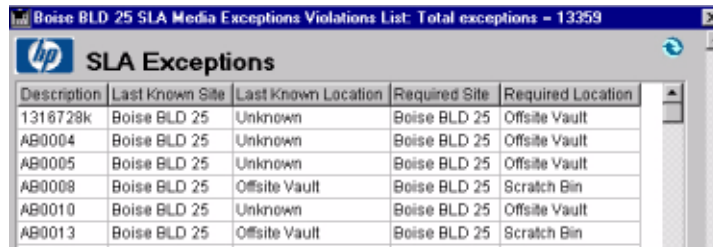
On the Site SLA Status screen, if you click Scratch Init Jobs, you see a list of all the overdue jobs in this category. You can view any of the jobs from this historical record to see the details of the job, how many scratch media were meant to be initialized into which pool, and which media were meant to be dismounted, plus details of when the job was completed and who marked it as complete.

Figure 5-5 Scratch Init Job Information Screen



On the Site SLA Status screen, if you click Exceptions, this takes you to the SLA Exceptions screen for the site. (This is the same as clicking Exceptions on the shortcut bar.)

Figure 5-6 SLA Exceptions



The screenshot shows a web browser window titled "Boise BLD 25 SLA Media Exceptions Violations List: Total exceptions - 13359". The page header includes the HP logo and the text "SLA Exceptions". Below the header is a table with the following data:

Description	Last Known Site	Last Known Location	Required Site	Required Location
1318728k	Boise BLD 25	Unknown	Boise BLD 25	Offsite Vault
AB0004	Boise BLD 25	Unknown	Boise BLD 25	Offsite Vault
AB0005	Boise BLD 25	Unknown	Boise BLD 25	Offsite Vault
AB0008	Boise BLD 25	Offsite Vault	Boise BLD 25	Scratch Bin
AB0010	Boise BLD 25	Unknown	Boise BLD 25	Offsite Vault
AB0013	Boise BLD 25	Offsite Vault	Boise BLD 25	Scratch Bin

SLA Status Configuration

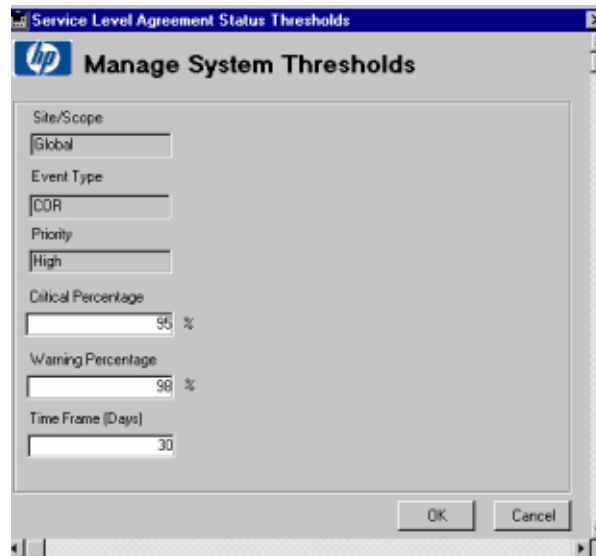
Use Global Configuration Options > SLA Configuration to set the SLA status thresholds for all sites. It allows you to change thresholds that determine how SLAs are measured against the media activity in the Media Operations product.

The System tab shows the current settings for the eight SLA status indicators representing the various job types.

System tab settings are all based on what percentage of each job type was completed successfully (within due time) over the defined time period. (For example, if the warning is set to 99% and timeframe is 30, this means that, if the percentage of successful jobs over the last 30 days falls below 99%, that SLA indicator is at warning status.) You can edit these settings by clicking Edit or double-click the measurement item.

Figure 5-7

Manage System Threshold Screen

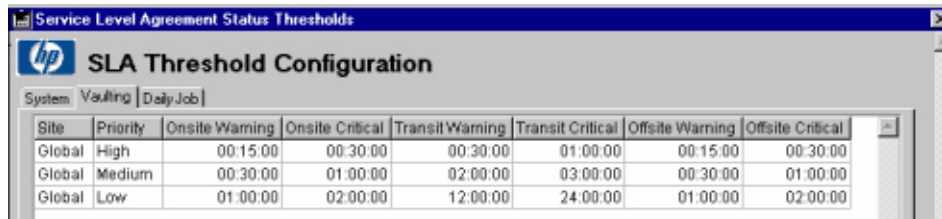


Vaulting tab settings define the warning and overdue times for vaulting, scratch, and checkout request jobs. These will show up as the warning and critical icons for the jobs in the daily operations. The status icons for the job types and the site in the shortcut bar are based on these measures. Each phase of the media movement has its own

warning/critical status (moving media within the site, performing the transit from your site to the destination offsite location, and then moving the media within that offsite location).

The total overdue time for any job will depend on whether the job includes moving media offsite or not. If the job is only moving media onsite, just the onsite times count. The due time would be the “onsite critical” time after the job starts. If moving media offsite, only the due time would be the sum of the critical times. All automatic vaulting and scratch jobs are always considered low priority, and checkout request jobs have their priority set when they are submitted.

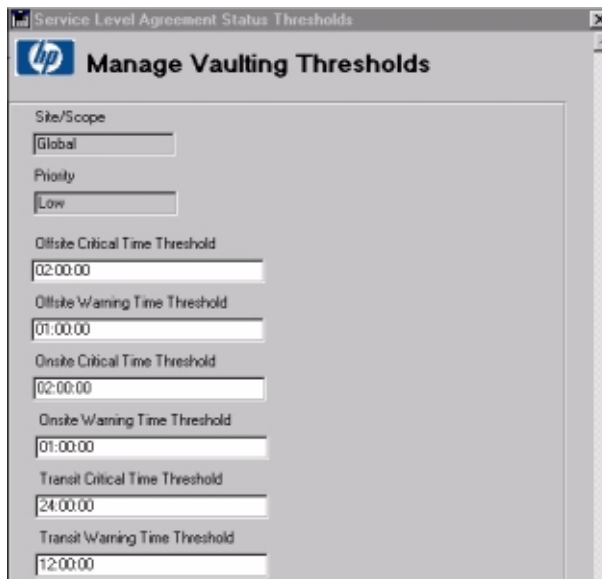
Figure 5-8 SLA Threshold Configuration — Vaulting Screen



Site	Priority	Onsite Warning	Onsite Critical	Transit Warning	Transit Critical	Offsite Warning	Offsite Critical
Global	High	00:15:00	00:30:00	00:30:00	01:00:00	00:15:00	00:30:00
Global	Medium	00:30:00	01:00:00	02:00:00	03:00:00	00:30:00	01:00:00
Global	Low	01:00:00	02:00:00	12:00:00	24:00:00	01:00:00	02:00:00

You can edit the settings for any priority (double-click or click `Edit`).

Figure 5-9 Manage Vaulting Threshold — Edit Screen



Site/Scope: Global

Priority: Low

Offsite Critical Time Threshold: 02:00:00

Offsite Warning Time Threshold: 01:00:00

Onsite Critical Time Threshold: 02:00:00

Onsite Warning Time Threshold: 01:00:00

Transit Critical Time Threshold: 24:00:00

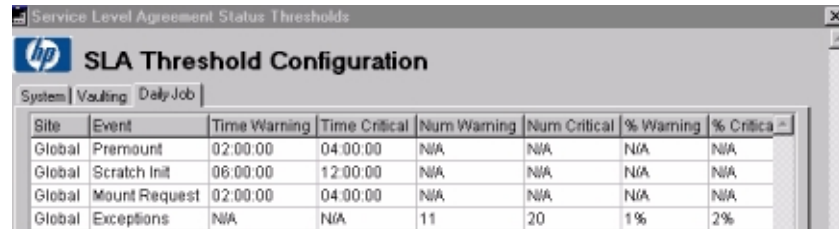
Transit Warning Time Threshold: 12:00:00

Status and Reporting Interfaces

SLA Status Configuration

Daily Job tab settings define the warning and critical times for all other job types: premount jobs, mount request jobs, and scratch init jobs. The time warning and time critical settings for each of these jobs represent how long after the job started before the job goes into the warning or critical (overdue) status. Double-click a job to edit or view.

Figure 5-10 SLA Threshold — Daily



Site	Event	Time Warning	Time Critical	Num Warning	Num Critical	% Warning	% Critical
Global	Premount	02:00:00	04:00:00	N/A	N/A	N/A	N/A
Global	Scratch Init	06:00:00	12:00:00	N/A	N/A	N/A	N/A
Global	Mount Request	02:00:00	04:00:00	N/A	N/A	N/A	N/A
Global	Exceptions	N/A	N/A	11	20	1%	2%

The Daily Job tab also include the SLA status threshold settings for exceptions. These are measured in terms of the number of media in the exception list (for example, lost media) that can be defined in terms of the total number of media exceptions and in terms of the percentage of media exceptions compared to the amount of managed media in the site (for site-level exception SLA status) or total managed media (for global exception SLA status). The settings for the total numbers of exception media take precedence of the percentages. (So, if the total number of exceptions setting is more than the amount of media represented by the percentage setting, the number setting is used for the exception SLA status.)

Figure 5-11 Manage Daily Thresholds Screen



Service Level Agreement Status Thresholds

Manage Daily Thresholds

Site/Scope: Global

Event Type: Exceptions

Job Critical Threshold: 20

Job Warning Threshold: 11

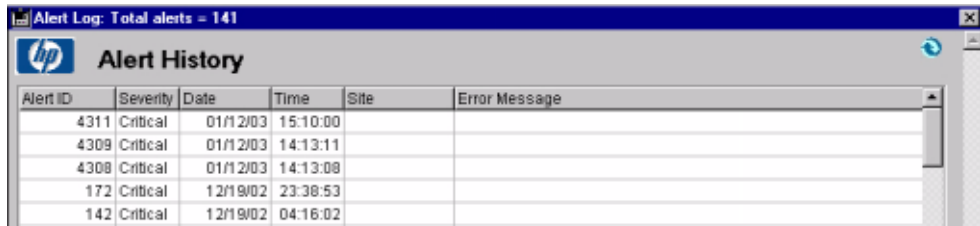
Job Critical Percentage Threshold: 2 %

Job Warning Percentage Threshold: 1 %

Viewing Alerts

Alerts are used to show configuration problems and any problems running requests via the XML Gateways to Backup Managers, and so on. Alerts are viewed either at the site level or the global level. The site-level alerts only show alerts that are site specific. The global-level alerts show alerts for all sites. From the SLA Status/Reporting screen, double-click Alert History for All Sites, or from the SLA Status/Reporting screen for a specific site, click Alert History.

Figure 5-12 Alert History — Global

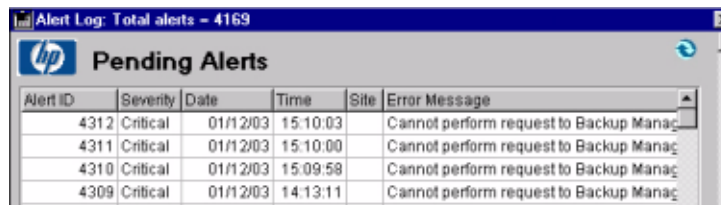


The screenshot shows a window titled "Alert Log: Total alerts = 141" with the HP logo and "Alert History" header. Below the header is a table with the following data:

Alert ID	Severity	Date	Time	Site	Error Message
4311	Critical	01/12/03	15:10:00		
4309	Critical	01/12/03	14:13:11		
4308	Critical	01/12/03	14:13:08		
172	Critical	12/19/02	23:38:53		
142	Critical	12/19/02	04:16:02		

To view a list of pending alerts for all sites, click the Current Alerts for All Sites tab on the SLA Status/Reporting screen.

Figure 5-13 Pending Alerts Screen

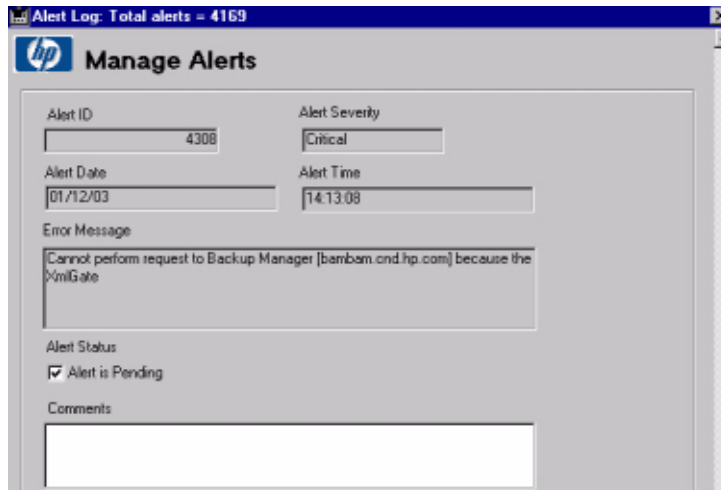


The screenshot shows a window titled "Alert Log: Total alerts = 4169" with the HP logo and "Pending Alerts" header. Below the header is a table with the following data:

Alert ID	Severity	Date	Time	Site	Error Message
4312	Critical	01/12/03	15:10:03		Cannot perform request to Backup Manag
4311	Critical	01/12/03	15:10:00		Cannot perform request to Backup Manag
4310	Critical	01/12/03	15:09:58		Cannot perform request to Backup Manag
4309	Critical	01/12/03	14:13:11		Cannot perform request to Backup Manag

You can either double-click an alert, or select an alert from the list and click View to view/manage an alert. Clicking Resolve Highlighted allows you to select multiple alerts and resolve them all at once, and then they are moved from the Pending Alerts screen to the Alert History screen.

Figure 5-14 **Manage Alerts Screen**



You can acknowledge/resolve an alert (so it switches from the current alerts list to the historical alerts list) by clicking to clear the Alert is Pending check box. This returns you to the Pending Alerts screen and, if you click Refresh (top right), the list will be redrawn without the acknowledged alert.

Reports

Use the `Reports` screen to generate reports to assist in monitoring activity on the Media Operations Server. There are four types of reports:

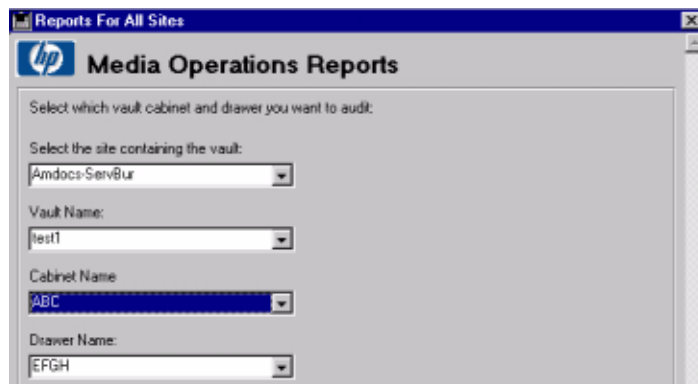
- **Vault Audit**—a list of media currently located in a cabinet or drawer of a specified onsite vault, which can be used to physically audit the media in the onsite vault.
- **Scratch Media**—the current levels of scratch media across all sites, including scratch media usage information and recommended scratch media levels.
- **Media Movement**—details of all media movements within the last 24 hours.
- **Unknown Media**—details of all unknown, blank and foreign media.

Vault Audit

The vault audit report prints the media contents of a specified vault cabinet. It is available at global and site level. You will need to select the site containing the vault, the vault name, the cabinet name, and the drawer name as shown on the following screen. Click `Print Audit Report` to print the media contents of the selected drawer.

Figure 5-15

Vault Audit Report



Scratch Media

The scratch media report shows the last 24 hours of activity in all of the scratch media bins in a specific site. (When this report is selected via the global SLA Status/Reporting, select the site to report on.) This includes current scratch bin levels, what optimal scratch bin levels should be, whether you have too many or not enough scratch media in each pool (so then you can decide whether to initialize new media for a specific pool, or remove existing media), and how much scratch media were used by backups in the prior 24 hours. The scratch media report is also available from the Media Operations web site.

Media Movement

The media movement report shows the last 24 hours of activity for all media movements due to vaulting policies, scratch bin maintenance, and checkout requests on a specific site. Example media movements include:

- moving media from a device to an onsite vault,
- moving media from a device to an offsite vault,
- moving media from an onsite vault to an offsite vault,
- moving media from an offsite vault to another offsite vault (advanced vaulting policy),
- moving media from an onsite or offsite vault back to a device (advanced vaulting policy or checkout request),
- moving media from onsite/offsite vaults to scratch bins, and so on.

For each media movement, the report details whether it was overdue or not.

Additional Reports

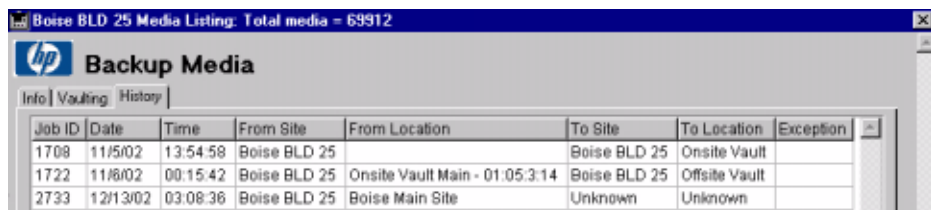
You can also use the `Feature` tabs in objects to get additional media information reports, such as:

- **Pool Media List:** (`Media` tab on media pools detail form) A pool media list, lists the media in that pool.
- **Backup Specifications Media List:** (`Media` tab on backup specs detail form)
A backup specification media list, lists the media used by that backup spec (different from current manual as there are no caveats — applies to all backup specs).
- **Systems Media List:** (`Media` tab on system detail form) A systems media list, lists the media used for backups of a specific system (different from current manual as there are no caveats — applies to all backup specs).
- **Device Media List:** (`Library` tab on devices detail form for library devices)
A device media list shows the media contents of a library device.
- **Container Media List:** (`Media` tab on container detail form) A container media list shows what media are currently in the container.

Backup Media History

If you view details on any piece of medium, the `Backup Media - History` screen lists all the movements that piece of medium has gone through.

Figure 5-16 Backup Media — History Screen



The screenshot shows a window titled "Boise BLD 25 Media Listing. Total media = 69912". Below the title bar is the HP logo and the text "Backup Media". There are three tabs: "Info", "Vaulting", and "History", with "History" selected. A table displays the following data:

Job ID	Date	Time	From Site	From Location	To Site	To Location	Exception
1708	11/5/02	13:54:58	Boise BLD 25		Boise BLD 25	Onsite Vault	
1722	11/8/02	00:15:42	Boise BLD 25	Onsite Vault Main - 01:05:3:14	Boise BLD 25	Offsite Vault	
2733	12/13/02	03:08:36	Boise BLD 25	Boise Main Site	Unknown	Unknown	

Notifications

You can configure automatic notification by e-mail or to OpenView Operations (OVO) for key events, such as alerts, job creation, SLA warnings, and metrics.

Configuring Notification Interfaces

Before you can configure any notification triggers, configure the notification interface first. The notification interfaces are configured on the `Server Parameters - Notification` screen as show below.

Figure 5-17 Server Parameters — Notifications Screen

The screenshot shows the 'Server Parameters' window for 'Media Operations Server Parameters'. The 'Notifications' tab is active. The interface includes the following elements:

- OVO opcmag.exe location:** A text input field with a 'Browse...' button.
- OVO Default Application:** A text input field.
- OVO Default Message Group:** A text input field.
- OVO Message Prefix String:** A text input field.
- Email "From" address:** A text input field containing 'perseusdb@hp.com'.
- Email "Reply To" address:** A text input field containing 'stephen.gold@hp.com'.
- Email SMTP gateways:** A list box containing 'smtp-americas.hp.com'.
- Buttons:** 'Add' and 'Edit' buttons at the bottom.

There are two types of notification interfaces

- Email
- OpenView Operations (OVO)

Email Interface Configuration

You have to configure the following e-mail interface options to enable e-mail notification.

- Email "From" Address — The e-mail address shown in the From field in all emails messages sent by the notification system.
- Email "Reply To" Address — The e-mail address used if anyone replies to an e-mail sent by the notification system.
- Email SMTP Gateways — The list of one or more SMTP Gateway Servers with their fully qualified network addresses. At least one gateway is required, because it forwards emails from Media Operations to defined users. If you define several gateways, the software will try to connect to the gateways in the list in order, until there is a response or no more gateways available.

OVO Interface Configuration

Configure the following OVO interface options to enable OVO notification.

- OVO opcmmsg.exe Location — To use OVO notification, you must have already configured your Media Operations Server to be managed by OVO. In this case, there should be a utility called opcmmsg.exe on the Media Operations Server. This utility is used to send notifications to OVO, so type the path to this utility to enable OVO notification. You can click Browse to browse your directory tree to locate the directory containing the opcmmsg.exe utility.
- OVO Default Application — Type an application name (such as MediaOps) that will be displayed in OVO for any notifications sent from this Media Operations Server.
- OVO Default Message Group — Type a message group name that will be displayed in OVO for any notifications sent from this Media Operations Server. (Note) you can override this default message group when defining each OVO notification trigger.
- OVO Message Prefix String — Type a prefix string that will be prefixed to the beginning of every OVO notification sent from this Media Operations Server.

Configuring Notification Triggers

You can configure the notification triggers at the global or site level by double-clicking **Notification** under **SLA Status/Reporting**. (At the site level, you can only add or edit notification triggers specific to that site.)

There are four possible notification triggers that can be configured:

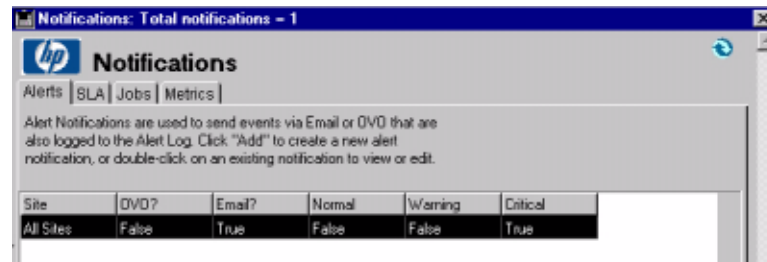
- **Alerts** — send a notification when an alert occurs.
- **SLA** — send a notification when an SLA measure is warning or critical.
- **Jobs** — send a notification when any job is created.
- **Metrics** — send an e-mail report of metrics.

Alerts

Alert notifications are used to send events via e-mail or OVO that are also logged to the alert log. Click **Add** to add a new alert notification, or double-click an existing notification to view or edit.

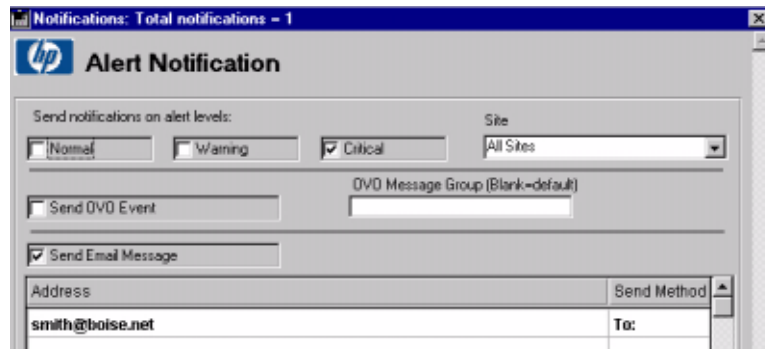
Figure 5-18

Notifications — Alerts Screen



Select the **Normal**, **Warning**, or **Critical** check box to define the level of alert for which the notification is to be sent. Click the **Site** arrow and select the site from the drop-down list. Select the **OVO Event** and/or **Send Email Message** check box and configure the list of e-mail addresses (by clicking **Add** and/or **Edit**) that will receive the notification. When configuring the e-mail address list, for each address you can set whether the e-mail will be **To:** or **CC:** or **Bcc:**. Click **OK** to finish.

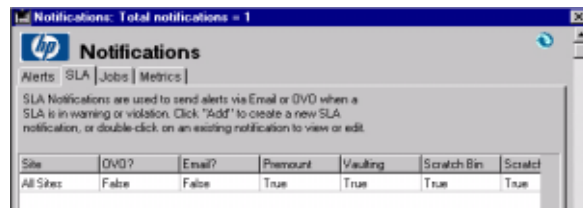
Figure 5-19 Alert Notification — Add/Edit Screen



SLA

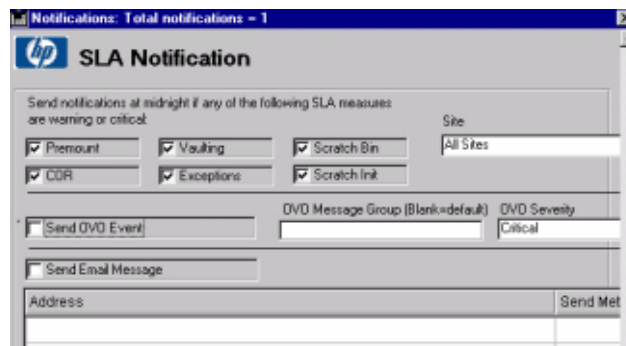
SLA notifications are used to send alerts via e-mail or OVO when an SLA is in warning or violation. Click **Add** to add a new SLA, or double-click an existing notification to view or edit.

Figure 5-20 Notifications — SLA Screen



Choose which types of SLA measure for the notification that is sent and select the site (or select **All Sites** for global SLAs). Select the **OVO Event** and/or **Send Email Message** check box and configure the list of e-mail addresses (by clicking **Add** and/or **Edit**) to receive the notification. When configuring the e-mail address list, for each address you can set whether the e-mail will be **To:** or **CC:** or **Bcc:**. Click **OK** to finish.

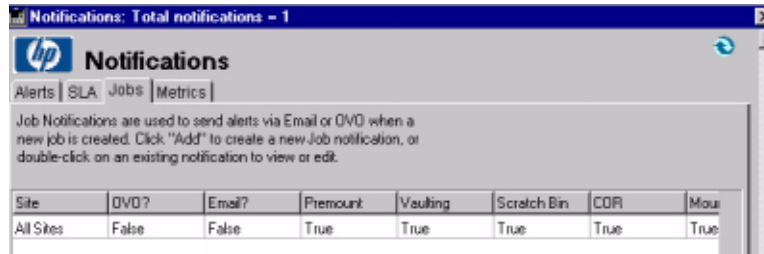
Figure 5-21 SLA Notifications — Add/Edit Screen



Jobs

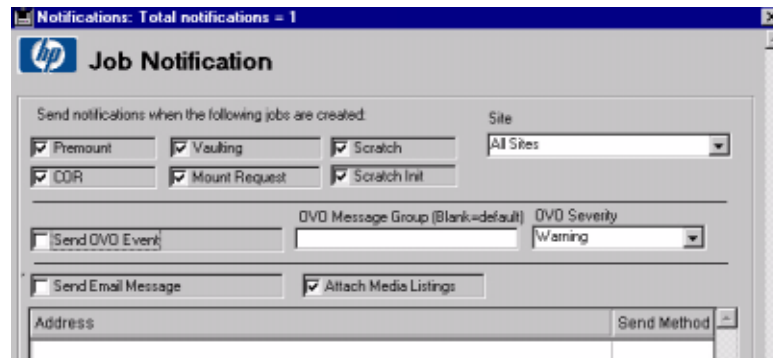
Job notifications are used to send alerts via e-mail or OVO when a new job is created. Click **Add** to create a new job notification, or double-click an existing notification to view or edit.

Figure 5-22 Notifications — Jobs Screen



Choose which types of jobs for the notification that is sent and select the site of the jobs for which to notify. You can also select the **Attach Media Listings** check box, which will include document attachments (in HTML format) on the job emails notifications that detail the required media for that job. Select the **OVO Event** and/or **Send Email Message** check box and configure the list of e-mail addresses (by clicking **Add** and/or **Edit**) that will receive the notification. When configuring the e-mail address list, for each address you can set whether the e-mail will be **To:** or **CC:** or **Bcc:**. Click **OK** to finish.

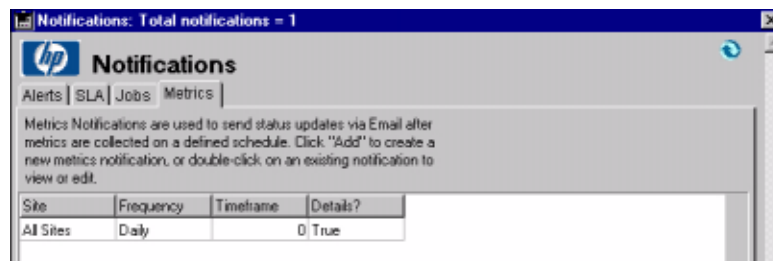
Figure 5-23 Job Notification — Add/Edit Screen



Metrics

Metrics notifications are used to send status updates via e-mail after metrics are collected on a defined schedule. Click **Add** to create a new metrics notification, or double-click an existing notification to view or edit.

Figure 5-24 Notifications — Metrics Screen



Select what period of time this metric notification will cover. (You can define multiple notification triggers for different metric periods, such as a notification generating metric reports covering the last week of activity and a different notification generating metric reports covering the last day of activity.)

The frequency options are:

- **Daily** — Metrics are sent every day after they are collected. The default collection time is 10:00 am.
- **Weekly** — This shows a new pull down for the day of week. The metrics are sent summarized for a 7-day period.

Status and Reporting Interfaces

Notifications

- **Monthly** — Metrics for the prior month are sent on the first of each month.

Timeframe This determines the number of units that are sent. If this is 0 or 1, just one unit is sent (one day, one week, one month). If you type 12, you get a report with the last 12 days, weeks, or months. If the number is 0 or 1, you get a media pool detail report. >1 gives you the totals only for all pools.

The options on the day-of-week drop-down list:

Everyday
Sunday
Monday
:
Saturday

This drop-down list determines the day of the week that the weekly report will be sent. The everyday option will send the metrics every day using the day prior to the day of sending as the ending day for the week. So, a report send on Tuesday uses Tuesday to Monday as the timeframe. A report send on Monday uses Monday to Sunday, and so on.

Figure 5-25

Metrics Notification — Add/Edit

Address	Send Method
loveland@hp.com	To:

Metric Report Description

The durations you will see are:

- Daily Detail (one day with media pool breakdown)
- Daily Summary (multiple days totals only)
- Weekly Detail
- Weekly Summary
- Monthly Detail
- Monthly Summary

Figure 5-26

Media Location Summary (Daily Average)

Week	Scratch bin	Holding bin	Devices	Onsite Vault	Offsite Vault	Other
9/18/2003 - 9/24/2003	9,346.85	2,416.28	1,676.00	841.28	63,904.00	6,308.14
9/11/2003 - 9/17/2003	7,949.85	2,539.71	1,592.00	731.14	69,454.42	6,607.28
9/4/2003 - 9/10/2003	7,596.57	3,308.28	1,731.42	707.42	68,525.71	6,686.28
8/28/2003 - 9/3/2003	7,339.14	2,671.14	1,544.28	766.85	69,080.28	6,662.57

The Media Location Summary is the total on a daily report and the average for the number of metric days for the weekly and monthly reports. The number of metric days is the number of days that have metrics collected and reported for the timeframe being reported. For example, if the monthly report does not include the first 14 days of the month due to the system being installed on the 15th, the number of metric days would be the 15th to the end of the month.

When viewing this report, you want to see the holding bin and other columns as low as possible. Other comprises of the COR, unknown and in transit location media.

Figure 5-27

Media Summary (Daily Average)

Week	Total # Tapes	Total # Expired	Scratch Bin	Num Expired
9/18/2003 - 9/24/2003	89,492.57	2,567.85	9,346.85	

Job Status

The Job Status only shown on daily detail. Listing of the jobs is closed from midnight to midnight. Jobs closed in violation of the SLA are highlighted in red.

Figure 5-28 **Open Job Summary**

Job ID	Type	Site	Entered Date/Time	Due Date/Time
9537	Vault		9/10/2003 06:31:43	9/11/2003 10:31:43
7613	Scratch		7/23/2003 06:41:33	7/24/2003 10:41:33
7614	Scratch		7/23/2003 06:41:34	7/24/2003 10:41:34
7700	Scratch		7/26/2003 06:39:54	7/27/2003 10:39:54
7725	Scratch		7/27/2003 06:30:22	7/28/2003 10:30:22

Job Metrics

Figure 5-29 **Job Summary (Daily Average)**

Site	Vaulting - Automatic	Vaulting - Manual	Scratch Bin	Scratch Init	COR	Premount	Reactive Mount
Boise BLD25	4.42	9.14	4.57	10.28	7.00	4.00	0.00

The Job Summary lists the average number of each type of job that you have during the period.

Figure 5-30 **Job Period Totals**

Week	Total # Vaulting - Automatic	Total # Vaulting - Manual	Total # Scratch Bin	Total # Scratch Init	Total # COR	Total # Premount	Total # Reactive Mount
9/23/2003 - 9/29/2003	31	64	32	72	49	28	0

The Job Period Totals lists the total number of each type of job that you have during that period.

Pool Health Metrics

Figure 5-31 Media Pool Health Summary (Daily Average)

Media Pool	Total # Tapes	Num On Exceptions	Num New Exceptions	Num Poor Scratch	Num Poor Media
[boi2-tapes.boi.hp.com]	19.00	1.00	0.00	0.00	0.00
[boi2-ccc.boi.hp.com]	1.00	0.00	0.00	0.00	0.00
[boi120.boi.hp.com] 1798 ARC DLT	2.00	0.00	0.00	0.00	0.00
[boi2-ccc.boi.hp.com].A	26.00	0.00	0.00	0.00	0.00
[boimn02.boise.itc.hp.com] AB_256K_BLOCK	5.00	2.14	0.42	0.00	0.00
[boimn02.boise.itc.hp.com] AB_LTO1_SCRATCH	7,308.00	651.42	52.71	25.71	592.28

The Media Pool Health Summary lists the average of how many tapes you have in a media pool for the period. This table shows the number on exception as well as the number of new exceptions.

Figure 5-32 New Vaulting Exceptions Period Totals

Week	Total # New Exceptions
9/23/2003 - 9/29/2003	1,888

The New Vaulting Exceptions Period Totals lists the total new vaulting exceptions for the period.

Premount Metrics

Figure 5-33 Media Premount Summary (Daily Average)

Site	Num Standalone Devices	Num Libraries	Num Media Required	Num Media Mounted
Boise.BLD25	379.71	92.71	623.28	487.57

The Media Premount Summary lists the average number of standalone devices, libraries, media required, and media that are mounted. The difference between media mounted and media required is that it indicates that media are being mounted without verifying them in the premount job. (Note) if a site requires that scratch media be verified in the premount jobs, as this is indicating, your media may or may not be mounted before the backup starts.

Figure 5-34 Media Premount Period Totals

Week	Total # Standalone Device Mounts	Total # Library Device Mounts	Total # Media Required	Total # Media Mounted
9/23/2003 - 9/29/2003	2,658	649	4,363	3,413

The Media Premount Period Totals lists the total number of standalone device mounts, library device mounts, media required, and media mounted.

Vaulting Metrics

Figure 5-35 Protected Media Summary (Daily Average)

Media Pool	Total # Tapes	Num Written	Num Vaulted
[boi2-tapes.boi.hp.com]	19.00	0.00	0.00
[boi2-ccc.boi.hp.com]	1.00	0.00	0.00
[boi120.boi.hp.com] 1798 ARC DLT	2.00	0.00	0.00
[boi2-ccc.boi.hp.com] A	26.00	0.00	0.00
[boimm02.boise.itc.hp.com] AB_256K_BLOCK	5.00	0.57	0.85
[boimm02.boise.itc.hp.com] AB_LTO1_SCRATCH	7,308.00	171.85	226.57
[boimm02.boise.itc.hp.com] adhoc	3.00	0.00	0.00

The Protected Media Summary lists the average number of tapes, number that are written, and number that are vaulted.

Figure 5-36 Protected Media Period Totals

Week	Total # Written	Total # Vaulted
9/23/2003 - 9/29/2003	8,767	11,602

The Protected Media Period Totals lists the total number written and the total number vaulted.

Scratch Metrics

Figure 5-37 Expired Media Summary (Daily Average)

Media Pool	Total # Tapes	Total # Expired	Scratch Bin	Num Expired
[bot2-tapes.boi.hp.com]	19.00	1.42	2.00	0.00
[bot2-ccc.boi.hp.com]	1.00	0.28	0.00	0.00
[bot120.boi.hp.com] 1798 ARC DLT	2.00	0.28	0.00	0.00
[bot2-ccc.boi.hp.com] A	26.00	7.42	0.00	0.00
[botmm02.boise.tc.hp.com] AB_256K_BLOCK	5.00	0.28	0.00	0.00

The Expired Media Summary lists the average number of tapes, average number of expired, average number in the scratch bin, and average number expired. Note the Total # Expired and the Num Expired are not correct for the dates prior to Media Operations 3.01.03 being installed.

Figure 5-38 Expired Media Period Totals

Week	Total # Expired
9/24/2003 - 9/30/2003	2,212

Remote Metrics

Figure 5-39 Remote Account Summary (Daily Average)

Account	Site	Num Media
BLD6	Boise BLD25	572.00
Houston	Boise BLD25	312.00

The Remote Account Summary lists the average number of media currently vaulted.

Vendor Metrics

Figure 5-40 Vendor Account Summary (Daily Average)

Vendor	Account	Site	Num Media
Boise Main Site	BLD25	Boise BLD25	49,444.00
Iron Mountain ML	10001	Boise BLD25	0.00
	1234	Boise BLD25	0.00
Iron Mountain CS	10002	Boise BLD25	4,385.00

Status and Reporting Interfaces
Notifications

The Vendor Account Summary lists the average number at the vendor site.

Vault Metrics

Figure 5-41 Media Vault Summary (Daily Average)

Vault	Site	Num Media
Main	Boise BLD25	1,435.00

The Media Vault Summary lists the average number of media in a vault at a specific site.

NOTE

The remote account metrics, vendor metrics, and vault metrics are not available for dates prior to Media Operations 3.01.03 being installed.

Location Metrics

Figure 5-42 Media Location Summary (Daily Average)

Media Pool	Scratch bin	Holding bin	Devices	Onsite Vault	Offsite Vault	Other
[boi2-tapes.boi.hp.com]	2.00	0.00	0.00	0.00	0.00	17.00
[boi2-ccc.boi.hp.com]	0.00	0.00	0.00	0.00	0.00	1.00
[boi120.boi.hp.com] 1798 ARC DLT	0.00	1.00	0.00	0.00	0.00	1.00
[boi2-ccc.boi.hp.com] A	0.00	0.00	0.00	0.00	0.00	26.00

The Media Location Summary lists the average number of media in the scratch bin, holding bin, devices, onsite, and offsite vaults. This is a media pool example (see Figure 5-26 on page 173).

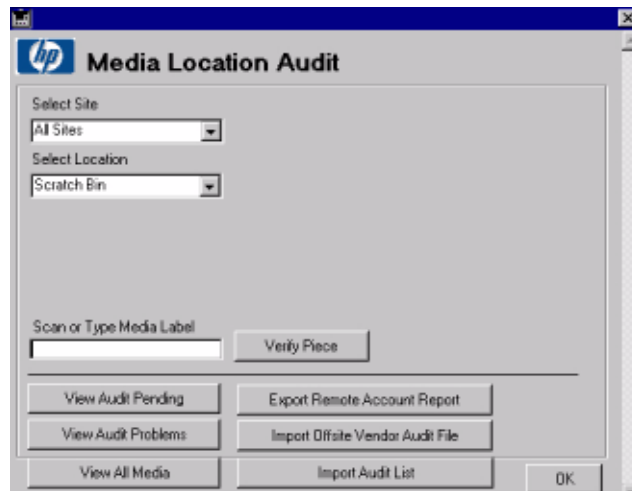
Location Audits

Location audits verify that the media are in the exact location Media Operations thinks they are in. This is beneficial in two ways:

- you can account for each piece of medium
- you are able to clear exceptions

To begin your location audit, go to `Utilities > Location Audit`.

Figure 5-43 Media Location Audit Screen



From here, you are able to audit your media. (Note) top-level administrators are the only ones that will see the bottom six buttons. If you are not a top-level administrator, the screen will have those buttons removed.

Select Site

You first need to select the site that you want to audit where the media are located. Then you will select a location.

Select Location

There are five locations that you can select:

Location Audits

- Scratch Bin
- COR Holding Area
- Device
- Vault
- Holding Bin

Scratch Bin

When selecting scratch bin as the media's location, you will see the following screen. You can scan the medium or type the media label. Click *Verify Piece* to verify the piece of medium.

Figure 5-44

Media Location Audit — Scratch Bin Screen



COR Holding Area

When selecting COR as the media's location, you will see the following screen. You can scan the medium or type the media label. Click *Verify Piece* to verify the piece of medium.

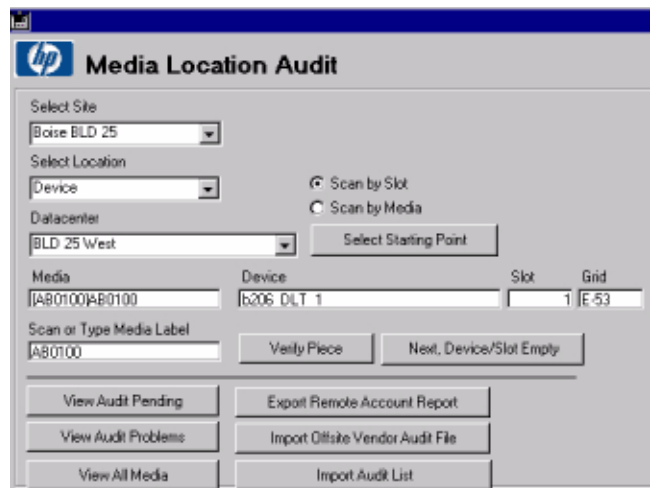
Figure 5-45 Media Location Audit — COR Screen



Device/Vault

When selecting device or vault as the media's location, you will see the following screen.

Figure 5-46 Media Location Audit — Device/Vault Screen



You will now need to select either:

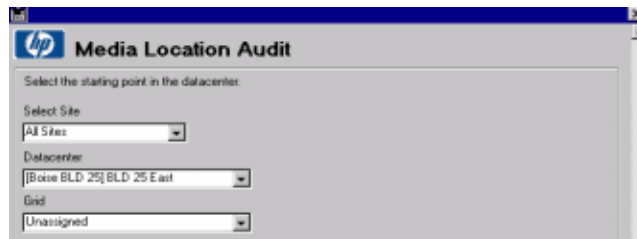
Location Audits

- Scan by Slot — This verifies the exact location of the media using the walk-through order of the vault or data center.
- Scan by Media — The general location is verified not the exact location in the vault/data center.

Next, select a data center and click `Select Starting Point`.

Figure 5-47

Media Location Audit — Select Starting Point Screen

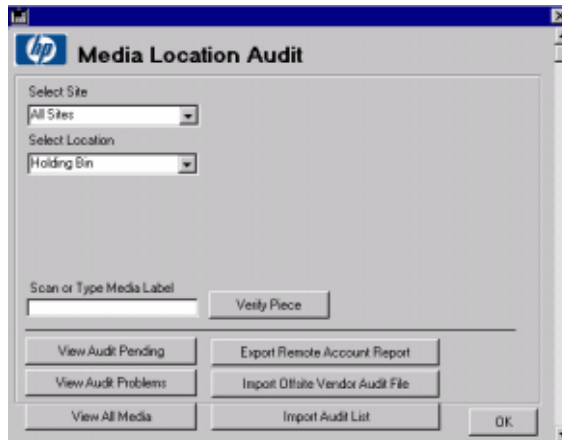


If you choose the starting point in the data center of `Unassigned`, the first medium meeting the set criteria will be displayed. If there is a medium available to audit, you will see the media label, device name, slot, and grid ID. To verify the piece of medium, either scan or type the media label and click `Verify Piece`. If the device/slot is empty, click `Next Device/Slot Empty`.

Holding Bin

When selecting the holding bin as the media's location, you will see the following screen. You can scan the medium or type the media label. Click `Verify Piece` to verify the piece of medium.

Figure 5-48 Media Location Audit — Holding Bin Screen



View

As previously mentioned, this section is only accessible by top-level administrators. You are able to view:

- Audit Pending
- Audit Problems
- All Media

When you click any of these buttons, you will see the following screen.

Figure 5-49 Media Location Audit — View Screen

Description	Barcode Label	Media Pool	Backup Manager	Last Write Date	Protection	Location	Quality	Audit Status	Audit Date/Time	Audit Location	Audited By
KB8314	KB8314	KB_DLT8_FR	bobcsbum01a.boi	12/17/02	Permanent	Transit					
	AB0682	AB_LT01_FR	bobcsbum01a.boi	11/16/02	12/31/02	Boise BLD					
Default DLT	C00008	Default DLT	raz.cnd.hp.com	05/24/03	Permanent	JAmdocs-Sea					
202711	202711	Z	boi2.boi.hp.com	11/16/02	12/31/02	Boise Main S					
B80825		Default DLT	boi319.boise.itc.hp	11/09/02	12/24/02	Boise Main S					
NK1553		Default DLT7	boi227.boi.hp.com	11/09/02	12/24/02	Boise Main S					

Here you see a detail of the media for the selected sites. You have the ability to query, print, reset audit flags, or audit specific media.

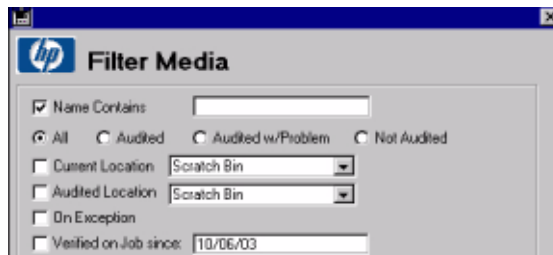
Query

This is used to reload the media list using the following filters:

- Name Contains — Query the media records for any barcode label or media label containing the string specified. Blank selects all:
- All, Audited, Audit w/Problem, Not Audited — Narrows the selection to just any audit flag, audited, audit with problem, or not audited.
- Current Location — Filters the list to the general location selected.
- Audited Location — Filters the list to the general location that the media were audited in.
- On Exception — Filters the list to media currently on a vaulting exception.
- Verified on Job since: — Filters the list to media that was successfully verified on a vaulting job (manual/scratch/offsite/and so on) since on or after the date specified — jobs closed in that timeframe only. If the job is in a pending state for offsite or confirmation, it is excluded.

If you want all the media that are not audited but were vaulted since 10/6/03, leave the Name Contains field blank, select the Not Audited radio button, select the Verified on Job since: check box, and type 10/6/2003 in the Verified on Job since: field.

Figure 5-50 Filter Media Screen



Print

When you click Print, you will receive an audit report of every piece of medium, including:

- medium number
- current location
- current status (Good, Problem, or Blank if medium has not been audited)
- time stamp
- location
- who audited

Reset Audit Flags

Before you can do a location audit, you need to purge the old audit data. Click `Reset Audit` to clean the slate.

Audit Highlighted

This allows you to audit selected media. This is useful to mark media as audited that was verified using a paper listing. Select the media you want to mark off and click `Audit Highlighted`.

Import Export

To use the device (by slot) scanning, you need a computer on the network to go through the data center or you need to write down everything in each device. For the import (from file), create a text file with each tape on a single line. For example:

```
AB0100  
BC0123  
AB1285  
:
```

To do this, type in the number, scan to notepad, and so on.

The export/import for the remote accounts/OSVs require a special XML file and is currently used only for Media Operations-to-Media Operations accounts.

Export Remote Account Report

This is used to produce an XML file for the remote account managed by the Media Operations Server. It is useful for transferring the audit results to the sending system. Only the media in the vault for this

remote account is used.

1. Select the remote account from which to generate the file.
2. Type the name of the file to save.
3. Copy the file to the sending server.

Import Offsite Vendor File

This is used to import the file on the home system that was generated using `Export Remote Account Report`. If the remote account information from the offsite system does not match the account name and password for an offsite vendor account record, the file is not imported. The current locations will not be changed to offsite, to do this, click `Request Audit` from the vendor's account entry.

Review the exceptions file to see the media that either did not match with media in the Home Server or, for which there was more than one matched, did not match with media in the Home Server or for which there was more than one match.

1. Select the file to import.
2. Type the name of a file to save the exceptions.

Import Audit List

Select the location from which the media are being audited. (Note) this will not change the current location of the media. All media imported will be marked as audited at this location.

1. Select the file to import.
2. Type the name of a file to save the exceptions.
3. Review the exceptions file to see the media that either did not match with media in the Home Server or for which there was more than one match.

A **Installing and Licensing**

Installing the Media Operations Server

This chapter provides an overview of the installation procedure and introduces the installation concept. Installation consists of installing the:

- Media Operations Server
- XML Gateway
- Media Operations Manager (optional)

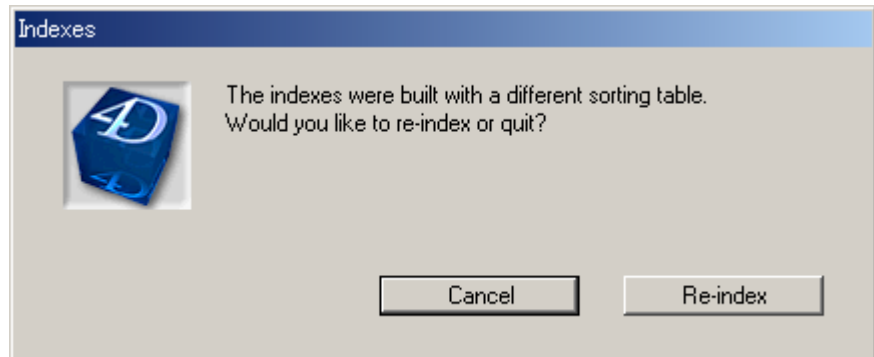
Installation Overview

The Media Operations installation package is installed manually from the CD-ROM.

- The minimum requirements for the Media Operations Server is a 500 MHz Pentium III CPU (or above), 256 MB RAM, and 500 MB free disk capacity. (A dual processor machine is highly recommended.) The installation process checks that sufficient disk space is available to install the Media Operations Server components.
- The unlicensed version of the product is a fully functional demo version (see “Licensing Media Operations” on page A-197). The administrator installs license keys after the product is installed.
- It is recommended to install the Media Operations Server onto a system that is a client of a tape backup solution as it provides a tape backup mechanism of the Media Operations Server data.
- The Media Operations Server installation includes a built-in web server that provides the web-based Media Operations GUI. The Media Operations Server installation package detects the presence of any existing web server on the system that the Media Operations Server is being installed on, and warns the installer that another port (3612) will be used for the Media Operations Web Server so that it can co-exist with the existing web server.
- To successfully install the Media Operations Server, there must be a local printer installed. If you do not have a local printer connected to your system, you can still install if you configure a local printer in your operating system, even if the printer is not attached.
- Media Operations Clients and Servers in languages that use Western

European character sets (such as ISO extended ASCII) can communicate with one another with no issues. Media Operations Clients and Servers in languages that use double-byte character sets (for Media Operations 3.0, only SJIS and EUC-KR are supported) can communicate successfully only with another Media Operations installation using that character set. This means Japanese clients must link to Japanese servers, Korean to Korean, and so on. See “Supported Languages” on page 13.

- When installing Media Operations in a double-byte language environment, you receive the following screen that gives you an option to Cancel or Re-index. Click `Re-index` to continue. Click `Re-index` within 30 seconds to avoid timing out. Do not click `Cancel`.



Installing Media Operations

Follow the procedure below to install Media Operations on your server. You are prompted through several screens during the installation process.

1. Insert the installation CD-ROM and run `setup.exe` from the server directory.
2. Click `Next` on the `Installation Wizard` screen to continue with the installation.
3. The next screen displays the licensing agreement, please read carefully and click `Yes` to accept the agreement and continue the install process. Accept this agreement to continue the installation.
4. At this point, you can choose the destination where the files are installed. The default location is

C:\Hewlett-Packard\DataMgt\MediaOps. To install to this location, click **Next**. To install to a different location, click **Browse** and select location.

NOTE

The Media Operations Server Database files are located in the same destination directory as the Media Operations Server. Because the database files can grow to a large size, you should select a destination location for the Media Operations Server that can accommodate this growth.

5. You are next prompted to choose where you want to install the data management communication service files. The communications service is a common component that is used by other Data Management applications that you install on your system. To install to the default folder, click **Next**. To install to a different folder, click **Browse** and select the folder.
6. Type an initial top-level administrator username and password. (You cannot continue the installation unless this information is entered.) Note the top-level administrator's login and password, because they will be the only way to log in until you create additional users.
7. At this point, you have the option to go back and review your settings or proceed with the installation. To review your settings, click **Back**. To proceed, click **Next**.
8. You have the option of reading the Read Me file. Click **Finish** to exit the installation wizard.
9. The installation is now complete. You should see the server console window for the Media Operations Server.

Installing Media Operations Manager Overview (Optional)

You have the option of installing the Media Operations Manager onto supported client systems. This provides the graphical user interface to Media Operations. This is useful when you want to provide Media Operations on a local site even when Media Operations Server is located in another site.

(Note) a copy of the Media Operations Manager is included with the Media Operations Server, so you will not need to install the Media Operations Manager onto the Server System.

This processes an installation package that is manually installed from the Media Operations CD-ROM.

Installing the Media Operations Manager

Follow the procedure below to install Media Operations Manager on your client system. You are prompted through several screens during the installation process.

1. Insert the installation CD-ROM and run `setup.exe` from the `client` directory on the CD-ROM.
2. Click `Next` on the `Installation Wizard` screen to continue with the installation process.
3. The next screen displays the licensing agreement. Please read carefully and click `Yes` to accept the agreement and continue the install process. Accept this agreement to continue the installation.
4. At this point, you can choose the destination where the files are installed. The default location is `C:\Hewlett-Packard\DataMgt\MediaOps`. To install to this location, click `Next`. To install to a different location, click `Browse` and select location.
5. At this point, you have the option to go back and review your settings or proceed with the installation. To review your settings, click `Back`. To proceed, click `Next`.

Installing Media Operations Manager Overview (Optional)

6. You have the option of reading the Read Me file. Click `Finish` to exit the installation wizard.
7. The installation is now complete. You should see the `Media Operations Manager` icon on the desktop, and there should be a `Media Operations` option in your `Start` menu.

Installing XML Gateway Overview

There are stand-alone installation packages that support installation of the XML Gateway onto Microsoft Windows, HP/UX, and Solaris platforms. The currently supported Backup Managers that the XML Gateway integrates with are:

- HP OpenView Storage Data Protector v 5.5, 5.1 and 5.0
- HP OpenView Omniback II v 4.1
- VERITAS NetBackup Business Server 4.5*
- VERITAS NetBackup Data Center 4.5*

* Feature Pack 3 or higher is necessary for VERITAS NetBackup support.

You can install the XML Gateway onto the same system as your Backup Manager (such as on your HP Data Protector Cell Manager), on another system with the same firewall zone as the Backup Manager, or on the Media Operations Server System. (This must be a dual processor system for this configuration.)

Installing XML Gateway on Windows

Follow the procedure below to install the XML Gateway on your server. You are prompted through several screens during the installation process.

1. Insert the installation CD-ROM and run `setup.exe`, from the `xmlgw windows` directory on the CD-ROM.
2. Click **Next** on the `Installation Wizard` screen to continue with the installation process.
3. The next screen displays the licensing agreement. Please read carefully and click **Yes** to accept the agreement and continue the install process. Accept this agreement to continue the installation.
4. At this point, you can choose the destination where the files are installed. The default location is `C:\Hewlett-Packard\DataMgt\DPXMLGW`. To install to this location, click **Next**. To install a different location, click **Browse** and select location.

Installing and Licensing

Installing XML Gateway Overview

5. Next, you are prompted to choose where you want to install the data management communication service files. The communications service is a common component that can be used by other data management applications that you install on your system. To install to the default folder, click **Next**. To install to a different folder, click **Browse** and select the folder. If you have already installed the Media Operations Server, this step is skipped.
6. At this point, you have the option to go back and review your settings or proceed with the installation. To review your settings, click **Back**. To proceed, click **Next**.
7. You have the option of reading the Read Me file. Click **Finish** to exit the installation wizard.
8. The installation is now complete.

Installing DP XML Gateway on HP-UX

Follow the procedure below to install the XML Gateway product on an HP-UX system.

Prerequisites

To install onto HP-UX, you will need either root access or an account with root capabilities.

An HP-UX system that will become your future XML Gateway host must have:

- ✓ supported HP-UX version installed
- ✓ sufficient disk space for the XML Gateway software
- ✓ port numbers 25555 and 25556 free
- ✓ TCP/IP protocol installed and running (must be able to resolve hostnames)

Installation

1. Insert the Media Operations CD-ROM and mount it.
2. Using the standard swinstall procedure, type the path.

For example:

```
swinstall -s taz:/cdrom/xmlgw/hpux/  
HPMedOps.depot HPMedOps
```

3. Check that the `max_thread_proc` parameter of the HP-UX kernel is set to at least 512. (This is the maximum number of threads allowed per process.) For more details, see “Kernel Tuning for XML Gateway on HP-UX” on page C-223.

See HP-UX documentation for additional information on `swinstall`.

Uninstall

To remove the XML Gateway software from an HP-UX system, type:

```
swremove HPMedOps
```

Installing XML Gateway onto Sun/Solaris

Prerequisites

To install onto Solaris system, you will need either root access or an account with root capabilities.

A Solaris system that will become your future XML Gateway host must have:

- ✓ supported Solaris version installed
- ✓ sufficient disk space for the XML Gateway software
- ✓ port numbers 25555 and 25556 free
- ✓ TCP/IP protocol installed and running (must be able to resolve hostnames)

Follow the procedure below to install the HP XML Gateway on a Solaris system.

1. Mount the Media Operations CD-ROM and `cd` to the directory by typing:

```
<cdrom mount point>/xmlgw/solaris
```

2. Type:

```
pkgadd -d and press Enter,
```

```
HPMedOps.pkg and press Enter, and
```

```
HPdpxmlgw and press Enter.
```

3. You are now asked:

```
Do you want to continue with the installation of
```

Installing and Licensing
Installing XML Gateway Overview

```
<HPdxmlgw> [y,n,?]
```

4. Type **y** to continue.

Uninstall

To remove the XML Gateway software from a Sun/Solaris system, type:

```
pkgrm HPdxmlgw
```

Licensing Media Operations

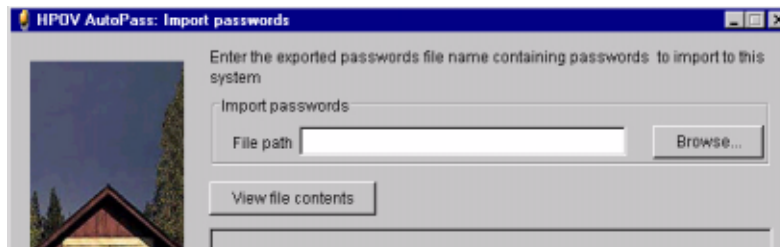
When the product is initially installed, it has no license key and is therefore acting as a demo product (with a 60-day time limit and unlimited media license). While the product is in “demo” mode, every time you log into Media Operations a message is displayed showing how many days of the demo period are remaining.

The product is still fully usable until the 60-day time limit expires. When the 60-day demo period expires, the product is switched to “expired” mode. While in “expired” mode, you cannot run any daily media movement jobs, except for checkout request jobs, and the web GUI is disabled. Every time you log in, you get an error dialog prompting you to install the appropriate number of licenses.

Even though the product cannot be used in expired mode, the server continues to run any scheduled activities, such as polling for new information from the Backup Managers or making backups of the database, and so on. Any new pieces of medium detected on the Backup Managers ARE added into the Media Operations Database even though the media license has been exceeded. This ensures the product is kept in sync with the environment, so that when the product switches to normal licensed mode, it is still up to date.

To enable full product use with no time limits, go to `Utilities > Add License`. This option is only available if you log in via the Media Operations Manager running on the Media Operations Server. The `Add License` command launches the `Auto Pass License Key` application in a separate window, and you can use this application to install new license keys.

Figure A-1 **Auto Pass License Key**



Each key represents an increment of either 2000 or 10,000 to the

Installing and Licensing

Licensing Media Operations

maximum managed media limit (the increment is encoded in the license key), or you can buy a license to manage unlimited pieces of medium.

When a new license key is entered using this option, it is first checked to ensure that it is not the same as an existing license key (if it is, the option gives an error message) and then the new key is checked to ensure it is a valid Media Operations license key.

Assuming the new key is unique and valid, the media license is extended by either 2000, 10,000, or unlimited pieces of medium depending on the license key.

Once you have installed sufficient licenses to cover your expected managed media, the product will be fully operational. However, if you did not install sufficient licenses to cover the current media or you exceed your license as the amount of managed media increases over time, the product switches to “license exception” mode. In license exception mode, you have a 60-day grace period to correct the license by installing sufficient new licenses to cover your media. During this grace period, Media Operations remains fully operational, but if you have not installed sufficient licenses by the end of 60 days, Media Operations switches into “expired” mode — which means that you cannot run daily operations, except checkout requests, and you cannot use the web GUI. You can return the product to full operation from expired mode by installing sufficient licenses to cover the amount of managed media.

Viewing Licences

On the `Utilities` menu of the Media Operations Server System, you can click `View Licences` to view your current license configuration.

Figure A-2

HPOV Utopias — Report Passwords



B External Interfaces

Overview

The Media Operations Server includes the following external interfaces:

“XML File Import Interface” on page B-201

“XML Offsite Vendor Interface” on page B-203

“Bulk Configuration File Import” on page B-213

XML File Import Interface

To support Backup Managers other than those supported by the XML Gateway, the Media Operations Server supports a file-import interface that allows an external backup application to post HTTP/XML formatted files to a directory on the Media Operations Server.

NOTE

Each file-import Backup Server should have its own unique directory assigned to it when it is added to the Media Operations configuration.

File Import

Every unique file-import directory is polled by the Media Operations software for any incoming files containing response data blocks. (Any files not from the server name defined for that file-import directory are ignored.) The polling frequency is set to once per minute by default, but you can modify this using the `File Polling Frequency` setting defined in `Global Configuration Options > Server Parameters`.

Any new devices, pools, backup specifications, or media detected in the HTTP/XML response data in valid incoming files are automatically added to the Media Operations Server (same as for new devices, pools, and so on in the XML response data from the XML Gateway).

Creating Files

You must:

- ✓ Provide scripts to convert information from your Backup Server (other than those supported by the XML Gateway) into incoming files containing Backup Manager, pool, device, backup specification, and media information.
- ✓ Ensure the files are copied into the file-import directory defined for that Backup Server.

The files you create must match the format described in “XML Import File Format” on page B-202 and must parse against the applicable Media Operations XML file format DTD. See “XML Import File Format” on page B-202 for instances of the DTDs.

Usage

There are two basic usages:

- **Configuration Update** — you provide Backup Manager, pool, device, and backup specification data, preferably imported in this order. Generate and import these files at least once a day to keep Media Operations in sync with the Backup Manager's configuration.
- **Media Update** — you provide a media information report of all media on the Backup Server at least once a day. There are two ways of providing incremental media information (preferably once an hour throughout the day):
 - If you support media usage information, provide a file that parses against the Used Media Information DTD. This enables you to set vaulting policy at system or backup specification level, and to see what media were used for the backup specification or system.
 - If you cannot support media usage information, provide a standard media information file consisting of a list of media that have changed since the last media update.

If the script that generates the XML import files has an error (for example, the Backup Manager is offline), you can log these errors in Media Operations by submitting a Backup Manager Error XML file.

XML Import File Format

The file-passing interface uses files formatted in an HTTP/XML protocol. The files contain the HTTP/XML response data blocks for:

- backup/restore device information (`LibraryDevice.dtd`)
- Backup Manager configuration data (`CellConfig.dtd`)
- media pool information (`MediaPool.dtd`)
- backup specification data (`BackupSpecs.dtd`)
- media information request (`MediaInfo.dtd`)
- media usage within a specified time period (`MediaUpdate.dtd`)
- Backup Manager errors (`ErrorReport.dtd`)
- device contents updates (`RepositoryList.dtd`)

See the DTDs found on the installation media under `docs\xml` for a guide to creating valid Media Operations XML.

XML Offsite Vendor Interface

Media Operations provides support for electronic links to offsite vendors. This electronic link allows Media Operations to send electronic verification of media being shipped to offsite storage and also provides electronic requests to return media from offsite storage back to the data center (such as for recovery jobs). This provides a much more reliable link to the offsite vendor compared to tracking media into and out of the offsite vendor via paper lists.

The Media Operations administrator has the ability to manually add their own offsite storage vendors and accounts, and then select these custom offsite locations as part of the media vaulting policies.

There are two possible offsite vendor types:

- **Media Operations:** Media Operations type is used when the offsite vendor is using Media Operations to manage its offsite media storage. The electronic link works between your Media Operations Server and the Media Operations Server at the offsite vendor.
- **Generic:** Generic type is used when the offsite vendor has its own proprietary electronic link interface. When configuring offsite accounts for such an offsite vendor, the Media Operations administrator writes scripts to take information from Media Operations and convert it to the offsite vendor's link protocol.

Usage

This section defines the scripting interface used with generic vendor types.

There are three basic types of electronic links to offsite vendors:

- media transit request
- request and receive audits
- status checking

Generic Input Parameters for All Request Types

For both types of requests, Media Operations passes the following parameters into the script that you create.

- **Parameter 1: Request type parameter**

- 1 (transit request)
- 2 (status request)
- 3 (request audit)
- 4 (send audit)

- **Parameter 2: XML parameters files**

The file name of the XML parameters file. Media Operations creates this file prior to calling the script. This parameter is delimited by quotation marks.

- **Parameter 3: results file name**

The file name passed into the script by Media Operations. Media Operations expects any results of the script to be written to this file. This parameter is delimited by quotation marks.

- **Parameter 4: proxy type**

Defines whether a Proxy Server is needed to connect to the offsite vendor and, if so, what type of Proxy Server: 0 — no proxy, 1 — http proxy, and 2 — socks proxy.

- **Parameter 5: proxy server name**

If a Proxy Server is used to connect to the offsite vendor, this parameter defines the network name of the Proxy Server.

- **Parameter 6: proxy port**

If a Proxy Server is used to connect to the offsite vendor, this parameter defines the port number used to connect to the Proxy Server.

- **Parameter 7: proxy username**

If a Proxy Server is used to connect to the offsite vendor and the Proxy Server requires a username and password, this parameter defines the proxy username.

- **Parameter 8: proxy password**

If a Proxy Server is used to connect to the offsite vendor and the

Proxy Server requires a username and password, this parameter defines the proxy password.

Media Transit Requests

Transit requests are electronic notifications of media movements to or from an offsite vendor. There are two types: outgoing and return.

- **Outgoing transit requests** let the offsite vendor know that media has been shipped to them and details the media shipped.
- **Return transit requests** let the offsite vendor know that you want the vendor to return media to you and specifies the set of media to return.

The XML parameters file will conform to the `TransitRequest.dtd` file. If the transit request is a return request (for example, transit type is `cor` or `scratch`), the XML will include a destination element with address and contact details specified.

You can either create two scripts (one for outgoing and one for return requests) or create one script that adapts its behavior based on the transit type in the XML parameters file.

On exit, your script must return one of the following result codes:

- 1 — Job/Request successful
- 3 — error while parsing xml parameters file
- 5 — bad account or password

Request and Receive Audit Requests

Request audit sends an electronic request to the offsite vendor for an audit that returns a list of all the media for your account in the offsite vendor's possession. Receive audit sends a request to the offsite vendor to verify the list of media sent in the request matches the media for your account currently in the offsite vendor's possession.

If the request type parameter is 3, then the XML parameters file will conform to the Request Audit DTD. In that case, the script must create the specified XML results file in compliance with the Audit List DTD.

If the request type parameter is 4, then the XML parameters file will conform to the Offsite List DTD.

On exit, your script must return one of the following result codes:

- 1 — Job/Request successful (for request type 4)

XML Offsite Vendor Interface

- 2 — Job/Request successful with a result file to process (for request type 3)
- 3 — error while parsing xml parameters file
- 5 — bad account or password

Status Checking Requests

Status checking request are electronic requests to the offsite vendor to monitor the progress of a previously submitted media transit.

The XML parameters file will conform to the `JobStatus.dtd` file.

If the job being monitored has completed and has results to return (for example, the offsite vendor had media exceptions while performing the job), the script must create the specified XML results file in compliance with `StatusResults.dtd`.

On exit, your script must return one of the following result codes:

- 1 — Job/Request successful
- 2 — Job/Request successful with a result file to process
- 3 — error while parsing xml parameters file
- 4 — job is still running
- 5 — bad account or password
- 6 — no transit job exists (This result causes the job to be transmitted again.)

XML Offsite Vendor File Format

See the following DTDs and examples, found on the installation media under `docs\xml`, for a guide to creating valid Media Operations XML:

- Job Status
- Status Results
- Request Audit
- Audit List
- Offsite List
- Transit Request

Reactive Mount Request Utility

Media Operations comes with a Java-based command line utility that allows you to submit reactive mount requests from any client system into the Media Operations Server. A reactive mount request is an ad hoc mount request that reacts to an unforeseen demand for backup media by

loading scratch media into a specified drive.

These requests are used when there is an asynchronous requirement for a piece of scratch media to be loaded into a drive for a backup job. For example, if not enough scratch media was loaded into a library by the scheduled premount jobs, the Backup Server needs more scratch media to be loaded when the backup runs. Reactive mount requests are also used to load scratch media for manually created backup specifications (where the backup job is outside the scope of your Backup Managers).

The command-line utility is called `reactivemount.jar` and can be found in the `MediaOps\Client` directory on the Media Operations Server and any Media Operations Manager system. If you installed with the default installation locations, this file will be at `C:\Program Files\Hewlett-Packard\DataMgt\MediaOps\Client`.

NOTE

The reactive mount request utility is Java-based, so you must have Java (v1.2 or higher) installed on the system on which you want to run the utility.

Usage

The usage for the reactive mount utility is as follows:

```
java exe> -cp <full path to reactivemount.jar file>  
com.hp.ov.dm.reactivemount.DoReactiveMount <param list...>
```

Mandatory Parameters The mandatory parameters are:

- m Media Operations Server name (server to which to send the reactive mount request)
- s or -mp Backup specification name (which specification requires media to be mounted)
Media Pool name (which media pool needs to be mounted in the specified device. This parameter is only valid if you have `-c` defined.)
- d Drive name (which drive in that backup spec to load the scratch media into)
- u UserName (a valid Media Operations username for authentication)
- p UserPassword (a valid Media Operations password for authentication)

External Interfaces

XML Offsite Vendor Interface

- c Backup Manager (the Cell Manager that has a mount request)
NOTE: If the reactive mount request is for a manually created backup specification (with no Backup Manager), this parameter should not be defined.

Optional Parameters The optional parameters for the utility are:

- r Name of requestor for tracking purposes
- ml Media label of the scratch media to load into the device
- sn Serial number of the scratch media to load into the device
- b Barcode of the scratch media to load into the device

Return Codes The return codes for the utility are:

- 0 Success
- 1 Invalid user
- 2 Bad backup specification
- 3 Invalid device
- 4 Invalid Backup Manager
- 5 Invalid media
- 6 Media not in pool
- 7 Duplicate media encountered
- 8 Media is manual and still in protected state
- 100 Unrecognized parameter
- 101 Required parameter not found
- 102 Connection failed
- 103 Connection timed out
- 4200 Multiple manual backup specifications with same name
- 4201 More than one user entry

If the mount request is for a piece of media from a pool with a strict policy, specify the required piece of media in terms of its barcode, label, or serial number or any combination of the three. If the media pool has a loose policy, you do not need to define the required piece of media, and, if no media is defined, the reactive mount job in the Media Operations Server

will allow the operator to select from a list of valid scratch media.

Example 1 The following is an example of the utility being executed on a Microsoft Windows system:

```
java.exe)  
-cp "C:\ProgramFiles\Hewlett-Packard\DataMgt\MediaOps\Client  
\reactivemount.jar")  
com.hp.ov.dm.reactivemount.DoReactiveMount)  
-m server1.xyx.com  
-c bkpmgr1.abc.com  
-s backup_spec_1  
-d tape_drive_1  
-u mediaops_login_1  
-p mediaops_login_1_password
```

When the reactive mount request is submitted to the Media Operations Server by the command-line utility, it creates a new mount request job in the Daily Operations job lists. The media operator who processes this job loads the appropriate piece of scratch media into the specified drive.

Example 2

The following example describes how to modify Omniback/Data Protector backup mount requests so they appear as mount request jobs in Media Operations. This is accomplished by modifying the Omniback/Data Protector mount scripts.

```
Example - mount.bat  
.@echo off  
set THIS=%0  
set USER=%1  
set GROUP=%2  
set HOSTNAME=%3  
set STARTPID=%4  
set DEVNAME=%5  
set DEVHOST=%6  
set DEVFILE=%7  
set DEVCLSS=%8  
set DEVCLASSNAME=%9  
shift  
shift  
shift
```

External Interfaces

XML Offsite Vendor Interface

```
shift
shift
shift
shift
shift
shift
shift
xset MEDID=%1
set MEDLABEL=%2
set MEDLOC=%3
set POOLNAME=%4
set POLICY=%5
set MEDCLASS=%6
set MEDCLASSNAME=%7
set SESSIONKEY=%8
REM Original command to e-mail the mount request
REM net send %HOSTNAME% "Mount request occurred for device
%DEVNAME%, session id %SESSIONKEY%"
REM
REM Variables to set to get the mount request across correctly
set OMNISTAT_CMD="c:\program files\omniback\bin\omnistat"
set JAVA_EXEC="D:\program
files\hewlett-packard\datamgt\dmcomms\jre\bin\java.exe"
set MOSERVER="motestserver"
set CELLSERVER="dptestserver"
set RCTMOUNT_JAR="c:\downloads\reactivemount.jar"

REM Only create a reactive mount request if the current session
is a backup session
%OMNISTAT_CMD% -session %SESSIONKEY% -status_only | find
"Backup"
if errorlevel 1 goto done

REM This session is a backup session, so create a reactive
mount request in MediaOps server % MOSERVER %

%JAVA_EXEC% -cp %RCTMOUNT_JAR%
com.hp.ov.dm.reactivemount.DoReactiveMount -m %MOSERVER% -c
%CELLSERVER% -mp %POOLNAME% -d %DEVNAME% -u s -p s

done
```

(mount.bat for windows Cell Managers and mount.sh for UNIX Cell Managers) so that it calls the reactive mount utility to submit the mount request to Media Operations.)

Example — mount.sh

```
@echo off
set THIS=%0
set USER=%1
set GROUP=%2
set HOSTNAME=%3
set STARTPID=%4
set DEVNAME=%5
set DEVHOST=%6
set DEVFILE=%7
set DEVCLASS=%8
set DEVCLASSNAME=%9
shift
shift
shift
shift
shift
shift
shift
shift
shift
shift
shift
set MEDID=%1
set MEDLABEL=%2
set MEDLOC=%3
set POOLNAME=%4
set POLICY=%5
set MEDCLASS=%6
set MEDCLASSNAME=%7
set SESSIONKEY=%8
REM Original command to e-mail the mount request
REM net send %HOSTNAME% "Mount request occurred for device
%DEVNAME%, session id %SESSIONKEY%"
REM
REM Variables to set to get the mount request across correctly
set OMNISTAT_CMD="c:\program files\omniback\bin\omnistat"
set JAVA_EXEC="D:\program
```

External Interfaces

XML Offsite Vendor Interface

```
files\hewlett-packard\datamgt\dmcomms\jre\bin\java.exe"
set MOSERVER="motestserver"
set CELLSERVER="dptestserver"
set RCTMOUNT_JAR="c:\downloads\reactivemount.jar"
REM Only create a reactive mount request if the current session
is a backup session
%OMNISTAT_CMD% -session %SESSIONKEY% -status_only | find
"Backup"
if errorlevel 1 goto done
REM This session is a backup session, so create a reactive
mount request in MediaOps server % MOSERVER %
%JAVA_EXEC% -cp %RCTMOUNT_JAR
% com.hp.ov.dm.reactivemount.DoReactiveMount -m %MOSERVER% -c
%CELLSERVER% -mp %POOLNAME% -d %DEVNAME% -u s -p s
:done
```

Bulk Configuration File Import

This utility lets you perform bulk loads of configuration data. Use the `Import` tab on the `Site Definition` screen to access this functionality. The configuration data types listed below are supported. The imported data must match the format described below.

Data Center Grids

If you want to import data center grid information, it must be contained in a comma-delimited text file and match the format described below.

The fields values are Site, Data Canter, Grid and Order Key. All values must be separated by commas and bounded by quotation marks (" "). There must be no more than one record per line.

For example:

```
"Site", "Data Center", "Grid", "Order Key"  
"London #1", "North", "B16", "25"
```

System Grid Locations

If you want to import system grid information, it must be contained in a comma-delimited text file and match the format described below.

The fields values are System, Site, Data Canter and Grid. All values must be separated by commas and bounded by quotation marks (" "). There must be no more than one record per line.

For example:

```
"System", "Site", "Data Center", "Grid"  
"xyz1036.abc.hp.com", "junk", "Brad's DataCenter", "A6"  
"xyz1037.abc.hp.com", "junk", "Brad's DataCenter", "A7"  
"xyz1038.abc.hp.com", "junk", "Brad's DataCenter", "A8"
```

Media Locations

If you want to import media location information, it must be contained in a comma-delimited text file and match the format described below.

The fields values are Media, Location (Vault or Offsite), Site, Vault, Slot, Vendor, Account and Container. Container is only needed if you are

Bulk Configuration File Import

defining a media location in an offsite vendor where the media is stored in a locked container. If the defined container does not already exist in Media Operations then it is automatically created. All values must be separated by commas and bounded by quotation marks (" "). There must be no more than one record per line.

For example:

```
"Media", "Location", "Site", "Vault", "Slot", "Vendor", "Account"  
"AB0001", "Vault", "Akron BLD 3", "closet", "1", , ,  
"AB0002", "Vault", "Akron BLD 3", "closet", "1", , ,  
"AB0003", "Offsite", "Akron BLD 3", , , "Vendor1", "10"
```

Example including container:

```
"Media", "Location", "Site", "Vault", "Slot", "Vendor", "Account", "C  
ontainer"  
"AB0003", "Offsite", "Akron BLD 3", , , "Vendor1", "10", "Container1"
```

Device Definitions

If you want to import device definition information, it must be contained in a comma-delimited text file and match the format described below.

The fields values are System, Device, Type, Media Type and Compression. All values must be separated by commas and bounded by quotation marks (" "). There must be no more than one record per line.

For example:

```
"System", "Device", "Type", "Media Type", "Compression"  
"slc1036.abc.xy.com", "L0", "Library", "LTO-Ultrium", "LTO2"  
"slc1036.abc.xy.com", "L1", "Library", "LTO-Ultrium", "LTO2"  
"slc1036.abc.xy.com", "L2", "Library", "LTO-Ultrium", "LTO2"
```

Import Manual Media

If you want import new manual media definitions (for example, media not associated with any Backup Manager, such as legacy media already stored in offsite or vault locations), it must be contained in a comma-delimited text file and match the format described below.

The fields values are MediaLabel, MediaBarcode and Pool (the name of a manually created pool in this site into which you want to import the media). All values must be separated by commas and bounded by quotation marks (" "). There must be no more than one record per line.

For example:

```
"MediaLabel", "MediaBarcode", "Pool"  
"AB001", "AB001", "DLT_Pool"  
"AB002", , "DLT_Pool"
```

NOTE

When creating manual media through this Import function, media is created as scratch media but with its last used date set to when the import was performed. This means, if the vaulting policy for the manual pool that this media is in has a minimum retention time set, the manual media will have the vaulting policies applied to it even though it is scratch media.

External Interfaces
Bulk Configuration File Import

C **Diagnostics and Tuning**

Overview

This appendix describes how to change logging levels for the various Media Operations components to facilitate diagnostics. It also discusses product tuning issues.

The sections in this appendix are:

“Media Operations Server Logs” on page C-219

“Media Operations Manager Logs” on page C-219

“XML Gateway Configuration, Logs, and Tuning” on page C-220

“Data Management Communications” on page C-224

Media Operations Server Logs

Log files for the Media Operations Server are found at:

```
<Install Location>\DBServer\log\...
```

For example:

```
C:\ProgramFiles\HP\DataMgt\MediaOps\DBServer\log\log.0.txt
```

The logging level for the Media Operations Server is adjustable under the **Log Level tab on the Server Parameters screen** under Global Configuration Options. Only a top-level administrator has access to this information.

Media Operations Manager Logs

Log files for the Media Operations Manager are found at:

```
<Install Location>\Client\log\...
```

For example:

```
C:\ProgramFiles\HP\DataMgt\MediaOps\Client\log\log.0.txt
```

The logging level for the Media Operations Server is adjustable under the **Log Level tab on the Server Parameters screen** under Global Configuration Options. Only a top-level administrator has access to this information.

XML Gateway Configuration, Logs, and Tuning

This sections discusses the configuration of the XML Gateways, the logging, and considerations for tuning the gateway.

Configuration

Based on the machine that hosts the XML Gateway, you can adjust several settings in the XML Gateway that can affect:

- performance
- logging for the XML Gateway
- logging for the Backup Managers
- cleanup of unclaimed XML reports
- the location of those reports
- timeouts that affect when locked Backup Manager jobs are terminated

XML Gateway Configuration File

```
<XmlgwConfig>
  <ResultsFilePath cleanUpMin = "15" keepFilesMin = "15">
    $ARCHIVELOCATION</ResultsFilePath>
  <Logging level = "SEVERE">
    <LogFilePath>$LOGFILEPATH</LogFilePath>
    <BkmgrLogging level = "0" socketTimeOut = "15">xmlgw1_0.log
      </BkmgrLogging>
    </Logging>
  <Threading reportThreads="5" actionsThreads="5"
    actionTimeoutMin="5" />
</XmlgwConfig>
```

Cleanup

XML reports are generated by the XML Gateway based on requests that are made from the Media Operations Server. These reports are written to disk and then removed when the Media Operations Server collects the completed reports. If the Media Operations Server fails to collect the reports, the undeleted reports are removed by the cleanup process.

If the Media Operations Server has problems retrieving the reports before they are removed, due to load, the cleanup should be adjusted.

The `cleanUpMin = "15"` attribute indicates the frequency (in minutes) at which the cleanup is run. The `keepFilesMin = "15"` attribute is the age of the file that is removed when the cleanup is run. So, if `cleanUpMin="60"` and `keepFilesMin="15"`, the cleanup will run every hour, but will remove all files that are more than 15 minutes old when the cleanup is started.

File Locations

The value between the tags `<ResultsFilePath>` and `</ResultsFilePath>` is the location to which the XML files are written.

CAUTION

Do not change the `ResultsFilePath` value without consulting support, as your Media Operations Server will no longer be able to retrieve the requested XML.

The `<LogFilePath>` tag indicates the location to which the log files are written. This can be changed, but must point to a valid location with sufficient disk space available to accommodate the log files.

Logging

The `<BkmgrLogging>` tag allows you to change the logging level, file name, and timeout used for the Backup Manager. Valid values for level are "0, or 1-X", where any value between 10-200 is valid for *x*. The text between the tags is the file name that the Backup Manager is told to use when logging requests from the gateway.

The `<socketTimeOut>` tag is used to terminate requests to the Backup Manager that appear to be hung. If your Backup Manager is very slow, this value may need to be increased, but this will increase the time it takes the XML Gateway to complete a request when there is a problem with the Backup Manager.

Threading

The XML Gateway processes multiple requests at the same time. To do this, it generates several threads per request. If the host supporting the XML Gateway can handle a large threading load, you can increase the threading level up to 15 for `reportThreads` and `actionThreads` in the configuration file.

The `actionTimeoutMin` is specifically used to timeout actions requested by the gateway. Actions include entering and ejecting media, library and drive scans, and initialization. If the Backup Manager does not respond to the request at least every several minutes, as defined by the `actionTimeoutMin`, the action is considered “locked,” the Backup Manager is told to terminate the job, and an error is reported. If any of these actions on your libraries or devices take longer than `actionTimeoutMin`, the value may be increased.

There are some side effects to increasing this value. For example, when a medium is not in the CAP, but the Backup Manager was told to load a piece of medium, some Backup Managers, such as Data Protector, will wait for you to load media. The `actionTimeoutMin` terminates this request and returns a `CapEmpty` error.

While the action is locked and waiting, that thread is not available to any other request. Once all the threads are used, all requests wait until one of the other requests is complete. If you up your `actionTimeoutMin`, it is recommended that you increase your threading level also.

Logs

Changing the logging level of the XML Gateway:

1. Open the `xmlgw_config` file on the XML Gateway host:
 - Windows:
`<xmlgw_Install_Loc>\dpxmlgw\config\xmlgw_config`
 - HP-UX and Solaris:
`/etc/opt/hpdpxmlgw/config/xmlgw_config`
2. Change the `Logging level="SEVERE"` setting in the XML configuration file.
3. Change the level and logname to which logs on the Backup Manager are written (optional). See the “Configuration” on page C-220 for more details.

Log Levels

The log level settings for the XML Gateway and their meanings are:

- SEVERE — writes only severe messages to the log file, all others are ignored.
- WARNING — writes both severe and warning messages to the log file.
- INFO — writes informational messages as well as severe and warning messages.
- ALL — writes all logging messages to the log file, including highly detailed tracing messages. It will cause large log files to be created.

Kernel Tuning for XML Gateway on HP-UX

If you installed the XML Gateway on an HP-UX system, you may need to adjust one of the HP-UX kernel tunable parameters to ensure reliable operation of the XML Gateway. Without this tuning, any requests to Backup Managers via this XML Gateway can fail with network connection errors, such as error codes -8 or -2002.

If the HP-UX system that you are installing the XML Gateway on has the kernel setting `max_thread_proc` still set to the default of 64 threads per process, set `max_thread_proc` to 512 or greater and then recompile the kernel. For further details, see http://www.hp.com/products1/unix/java/infolibrary/prog_guide/java1_3/configuration.html

Data Management Communications

This section covers logging and tuning for the Data Management Communications module (DMComms).

Service Logs

Information in this section pertains to logging level and log file location.

Changing the Logging Level

1. Open the communications configuration file on the DMComms host:
 - Windows:
`<DMComs_Install_Location>\DMComms\config\bbc_config`
 - HP-UX and Solaris:
`/etc/opt/hpdmcomms/config/bbc_config`
2. On Windows and Unix, change the `LOG_LEVEL` in the `[com.hp.ov.ipcserver]` section to the setting of your choice. Valid settings are:

```
[com.hp.ov.ipcserver]
SERVER_PORT = 25556
SECURE_COMM = SSL
SSL_PROVIDER = JSSE
SSL_CA_CERTIFICATE_filename = /opt/hpdmcomms/certs/ca.jks
SSL_CA_CERTIFICATE_FORMAT = JKS
SSL_KEYSTORE_filename = /opt/hpdmcomms/certs/server.jks
SSL_KEYSTORE_FORMAT = JKS
SSL_CLIENT_VERIFICATION_MODE = Anonymous
SSL_ENCRYPTION_LEVEL = Export
LOG_LEVEL=WARNING
```

3. On Windows, you can also change LOG_LEVEL in the [com.hp.ov.ipccclient.rpc] section to the setting of your choice. Valid settings are:

```
[com.hp.ov.dm.ipccclient.rpc]
SECURE_COMM = SSL
SSL_PROVIDER = JSSE
SSL_CA_CERTIFICATE_filename = REPLACE_WITH_CA.JKS
SSL_CA_CERTIFICATE_FORMAT = JKS
SSL_ENCRYPTION_LEVEL = Export
LOG_LEVEL=SEVERE
SERVER_PORT=25556
HTTP_PIPELINE=false
DISABLE_EXPECT_100=true
CLIENT_PORT=57000-58000
REQUEST_TIMEOUT=0
RESPONSE_TIMEOUT=0
```

Log File Locations

For Windows, the log files for DMComms are found at:

<Your DMComms Installed Location>\DMComms\log\...

For example:

c:\Program Files\HP\DataMgt\DMComms\log\mv_comms.log.0

For HP-UX and Solaris, the log files for DMComms are found at two locations:

/var/opt/hpdmcomms/log/mv_comms.log.0

/var/opt/hpdmcomms/log/daemon.log

Changing Communications Port Numbers

The default port numbers used by the Media Operations communications service are ports 25555 and 25556. All communications over the network between Media Operations components use an HTTPS/XML format. If you need to change these communications port numbers for any reason (for example, you have another application using the same port numbers), use the following process:

1. Go to the directory containing the communications configuration file, which is in the config directory of DMComms.
 - For Windows, the default installation location is:
C:\Program

Diagnosics and Tuning

Data Management Communications

Files\Hewlett-Packard\DataMgt\DMComms\config

- For HP-UX and Solaris systems, the default installation location is:

/etc/opt/hpdmcomms/config

2. Edit the file `bbc_config` to change the port settings. There are two different port numbers, one for the HTTP-based RPC communications and the other for the HTTP-based data transfer communications. Each port number is set in both the Communications Client and Communications Server sections of this file:

```
[com.hp.ov.bbc.fx] section
SERVER_PORT = 25555
```

```
[com.hp.ov.dm.ipcclient.fx] section
SERVER_PORT = 25555
```

```
[com.hp.ov.ipcserver] section
SERVER_PORT = 25556
```

```
[com.hp.ov.dm.ipcclient.rpc] section
SERVER_PORT = 25556
```

3. For UNIX, if you change the port numbers, you should also reflect this change in the `/etc/services` file. By default, Media Operations adds entries in this file for its communications settings:

```
hpdmcomms 25555      # HP DMComms port number
hpdmcomms 25556      # HP DMComms port number
```

D **Application Managers**

Overview

Media Operations supports several Application Managers:

- HP OpenView Omniback v4.1 and HP OpenView Storage Data Protector v5.0, 5.1 and 5.5
- VERITAS NetBackup Business Server and Data Center v4.5

This application matrix provides a quick glance as to what is supported by the various Application Managers.

Table D-1 Application Matrix

	Scratch Init	Library/Load Eject	Copy Support	Location Update	Mixed Pools	Media Subtype	Remote Gateway
HP OpenView Omniback v4.1 and HP OpenView Storage Data Protector v5.0	Yes	Yes*	No	Yes	No	No	Yes
HP OpenView Storage Data Protector v5.1 and 5.5	Yes	Yes*	Yes	Yes	No	No	Yes
VERITAS NetBackup Business Server and Data Center v4.5 (<i>requires Feature Pack 3 or higher</i>)	Yes*	Yes*	No	Yes	Yes	No	No*

Scratch Init

Whether the Backup Manager application has the ability to initialize/format new scratch media. See “Scratch Init” on page 131.

Load Eject

Whether the Backup Manager is unable to trigger the loading of scratch media into libraries and unloading from libraries where the media are to be vaulted.

See “Load/Eject Media” on page 112 for additional information.

Copy Support

Whether automated copy jobs are detected and therefore factored into

premount calculations. Also, whether media are copies and any copy specific vaulting policies are applied to that media.

Mixed Pools

If the Backup Manager application does not have a fixed media type for its pools, it is possible to get media pools to have a media type of “mixed.” Any mixed pools are excluded from `Premount` and `Scratch Init`.

Example:

If media in a pool are DDS1 and DDS2, they are not mixed.

If media in a pool are DDS1 and LTO1, they are mixed.

Media Subtype

Whether the Backup Manager automatically configures the media compression type of pools. The media subtype is determined by what type are the majority of the subtypes. For applications that do not support automatic configuration of media subtype, you will need to manually configure the media subtype in the GUI for each pool.

Example:

DDS pools containing DDS1, DDS2, and so on. If there are five DDS1 and ten DDS2, the compression will be that of the DDS2.

Location Update

The media location change in Media Operations is automatically copied back to the Backup Manager’s media location.

Remote Gateway

Whether the gateway is able to remotely communicate over the network with the new Backup Manager. If not, it can be installed on any Backup Manager. If it cannot communicate remotely, it *must* be installed directly on to the Backup Manager.

HP OpenView Omniback/HP OpenView Storage Data Protector

When performing load/eject operations for all silo-type library devices (such as ACSLS or DAS), the cartridge access port (CAR) must be set to manual.

VERITAS NetBackup

Virtual Media

It is possible to get excess virtual media, particularly in a non-barcode library. This may happen if you move blank media or non-barcoded blank media into a barcode library.

Permissions

The file `/usr/opensv/var/authorize.txt` is used to validate users executing reports and actions. If the user/host/group combination is not in the file as specified in Media Operations, all requested actions are rejected.

The file must be changed in NetBackup. “Any” and * are not acceptable matches; combinations must consists of a real user on a real host with a real group that has permissions. An NT user is acceptable, in which case enter a *domain* for that user in place of a group.

Initialization

In libraries, NetBackup does not support initialization of media on demand. It moves media from a blank pool to a target pool. The default pool is a blank pool.

- Library — does not support on-demand initialization.
- Stand Alone — supports on-demand initialization.

Silo

When performing load/eject operations for all silo-type library devices (such as ACSLS or DAS), the cartridge access port (CAP) must be set to `Automatic`.

Gateway Configuration File

There are three specific additions for NetBackup:

- Backup application mode of the XML Gateway
- Installation location of the backup application
- Definition of blank pools (define `NetBackup/Blank`)

If the values are not set in the configuration file, they default to `*`.

If your default settings are different or you prefer not to use the NetBackup settings, you can change `Add Override` to `NONE` — multiple pools to scratch.

Application Managers
VERITAS NetBackup

Glossary

access rights The permissions to perform specific tasks. Users have the access rights of the user class to which they belong.

automatically created media

Media that are used for backups controlled by the Backup Manager.

backup device A device configured for use with a Backup Manager that can write data to storage media. This can be, for example, a DDS/DAT drive or a library.

backup generation One backup generation includes one full backup and all incremental backups until the next full backup.

backup restore devices A piece of equipment designed to store copies of files from user's machine or other servers.

backup session A process that creates a copy of data on storage media. The activities are specified in a backup specification or an interactive session. *See also* **Incremental backup session** and **Full backup session**.

backup specification A list of objects to be backed up, together with backup options and a set of devices to be used. The objects are entire disks/volumes or parts of them, such as files, directories, or even the Windows NT Registry. File selection lists, such as include-lists and exclude-lists, can be specified.

backup types *See also* **incremental backup** and **full backup**.

barlist A configuration file that contains a description (database) of backup objects and a set of backup devices. Now referred to as a **backup specification**.

blank media Media that are ready to be used.

catalog protection Defines how long information about backup data (such as backup sessions, file names, and file versions) is kept in the Backup Manager Database. *See also* **data protection**.

cell A set of systems that are under the control of a Cell Manager. It typically represents the systems on a site or an organizational entity which are connected to the same LAN.

Glossary

Central control is available to administer the backup and restore policies and tasks.

checkout request Checkout requests are the means for obtaining tapes from vaults for file restore and disaster recovery.

CMMDB — Centralized Media Management Database The result of merging the MMDBs from several cells in the MoM cell. This is a MoM functionality. It allows the sharing of devices and media across several cells. *See also MoM.*

COR — Checkout Request Checkout requests are the means for obtaining tapes from vaults for file restore and disaster recovery.

data expiry policy The time before the data on the media can be erased.

data protection Defines how long the backup data on the media remains protected, that is, how long until the backup will overwrite it. When the protection expires, the Backup Manager can reuse the media in one of the next backup sessions.

database server A computer with a large database stored on it, such as the SAP R/3 or Microsoft SQL Database. A server has a database that can be accessed by clients.

datalist A Backup Manager configuration file that contains the definition details of a backup specification.

date entered The date that you entered the request (automatically entered).

device A physical unit which contains either just a drive or a more complex unit, such as a library.

device chains Several standalone devices of the same media class can be configured as a device chain. Devices in a chain are used sequentially.

device streaming A device is streaming if it can feed enough data to the medium to keep it moving forward continuously. Otherwise, the tape has to be stopped; the device waits for more data, reverses the tape a little, resumes to write to the tape, and so on. In other words, if the data rate written to the tape is less or equal to the data rate which can be

Glossary

delivered to the device by the computer system, the device is streaming. Streaming significantly improves the performance of the device.

disaster recovery A process that helps to restore a client's main system disk to a state close to the time when a (full) backup was performed.

disk agent The Disk Agent is a process that controls reading from and writing to a disk. During a backup session, the Disk Agent reads data from a disk and sends it to the Media Agent, which then moves it to the device. During a restore session the Disk Agent receives data from the Media Agent and writes it to the disk.

disk agent concurrency The number of Disk Agents that are allowed to send data to one Media Agent concurrently. It essentially defines from how many disks the data collected and wrote to a medium.

drive A physical unit which receives data from a computer system and can write it onto a magnetic medium. It can also read the data from the medium and send it to the computer system.

drive index A number which identifies the mechanical position of a drive inside a library device. This number is used by the robotic control to access a drive.

enterprise backup environment Several cells can be grouped together and managed from a central cell. The enterprise backup environment includes ALL clients located in several cells which are managed and administered from a central cell using the Manager of Managers (MoM) concept. *See also MoM.*

enterprise cell manager

Several cells can be grouped together and managed from a central cell. The management system of the central cell is the Manager of Managers (MoM). The MoM allows you to configure and manage multiple cells from a central point. Previously, this use to be called the Advanced Backup Manager. *See also MoM.*

event logs Files where Windows NT logs all events that occur (such as start or stop of services, and log on and log off of the users).

Glossary

filesystem The organization of files on a hard disk. A filesystem is backed up so that the file attributes and the file contents are stored on the backup media.

full backup A backup in which all selected objects are backed up, whether or not they have been recently modified.

FWD SCSI Fast Wide Differential (FWD) Small Computer Systems Interface (SCSI) is a high speed differential interface with a synchronous transmission rate between 5 MHz and 10 MHz and a 16-bit data path.

HSM — hierarchical storage management A method for optimizing the use of expensive hard disk storage by migrating less frequently used data to less-expensive optical platters. When needed, the data is migrated back to the hard disk storage. This balances the need for fast retrieval from hard disk with the lower cost of optical platters.

HTTPS — HyperText Transport Protocol Secure The protocol for accessing a secure web server. Using HTTPS in the URL, instead of HTTP, directs the message to a secure port number

rather than the default web port number of 80. The session is then managed by a security protocol. *See also security protocol.*

incremental backup A backup that selects only files that have changed since a previous backup. Several levels of incremental backup are available, allowing selective backup of only files that have changed since the last incremental backup.

IP address The numeric address of a system used to identify the system on the network. The IP address consists of four groups of numbers separated by periods (full stops).

job ID The automatically generated identifier for the checkout job.

library Also called autochanger, autoloader, or exchanger. A library contains media in repository slots. Each slot holds one medium (for example, DDS/DAT). Media are moved between slots and drives by a robotic mechanism, allowing random access to the media. The library can contain multiple drives.

lights-out operation or **unattended operation.** An operation that takes place outside normal business hours, such as during the night or on the weekend. This implies that no operator personnel is present to work with, for example, the backup application or service mount requests.

log retention time The length of time the media audit logs are saved on the server.

LVM — Logical Volume Manager

A subsystem for structuring and mapping physical disk space to logical volumes. An LVM system consists of several volume groups, where each volume group has several volumes.

Manager of Managers (MoM) *See* **enterprise cell manager.**

media audit log Tracks every movement performed with each piece of medium.

media condition factors The user-assigned age threshold and overwrite threshold used to assert the condition of a medium.

media condition The quality of a medium as derived from the media condition factors. Heavy usage and age result in increased read and write errors. Media need to be replaced when the condition field indicates POOR.

media pool A set of media of the same type (such as DDS) used and tracked as a group. Media are formatted and assigned to a media pool.

media type The physical type of the media, such as DDS or DLT.

media ID A unique identifier assigned to a medium by the Backup Manager.

media label A user-defined identifier used to describe a backup medium.

medium location A user-defined physical location of the backup media, such as “building 4” or “offsite storage”.

merge How files are restored. If the file to be restored already exists at the destination, the one with the more recent modification date is kept. Files not present on the disc are always restored. *See also* **overwrite.**

MoM Server *See enterprise cell manager.*

mount request A screen prompt that tells the user to insert media into a device. Once you respond to the mount request by providing the required media, the session continues.

mountpoint The access point in a directory structure for a disk or logical volume (for example “/opt” or “d:”). On HP-UX, the mountpoints are shown with the bdf command.

multi-drive server This relates to licensing. It allows the configuration of one system with multiple devices running at the same time. A Multi-Drive Server license allows you to run an unlimited number of Media Agents on a single system. The Multi-Drive Server license is also bound to the IP address of the Cell Manager.

object

For Windows NT clients: A logical disk (such as d:).

For UNIX clients: A mounted filesystem or a mount point.

For Netware: A volume. The scope of the data can be further reduced

by selecting files or directories. Additionally, an object can be a database entity.

overwrite

As a restore option: How files are restored to the destination. All files are restored from the backup even if they are older than existing files. *See also merge.*

As a media condition factor: How many times a piece of medium can be rewritten, hence influencing when a medium becomes POOR.

parallelism The concept of reading multiple data streams from an on-line database is referred to as parallelism.

point-in-time recovery A filesystem recovery made from a specific date.

polling

(1) A communications technique that determines when a terminal is ready to send data. The computer continually interrogates its connected terminals in a round-robin sequence. If a terminal has data to send, it sends back an acknowledgement and the transmission begins. Contrast with an interrupt-driven system, in which the terminal generates a

Glossary

signal when it has data to send.
(2) A technique that continually interrogates a peripheral device to see if it has data to transfer. For example, a mouse button was pressed or data is available at a communications port. Contrast with event driven techniques, in which the operating system generates a signal and interrupts the system.

polling schedule Defines when in the day the configuration information is extracted from the Data Protector Cell Manager.

post-exec A backup option that executes a command or script after the backup of an object or after the entire session completes.

pre-exec A backup option that executes a command or script before the backup of an object or before the entire session is started.

protection *See data protection and catalog protection.*

restore session A process that copies data from the backup media to a client system.

scan A function that identifies the media in a device. This synchronizes the MMDB with the

media that are actually present at the selected locations (for example, slots in a library). It is useful to perform a scan and check the actual media in the device, for example, if someone has manually manipulated media without using the Backup Manager to eject or enter.

scratch Media that are used for new overwriting backups.

scratch media bin A holding area for new or recycled media to which new backup sessions can be written.

scratch media maintenance

Perform the daily Media Operations related to stocking the scratch bins on the site with expired media and new scratch media to meet the scratch requirements of the pre-mount jobs defined for that site.

scheduler The function that controls when and how often backups occur. By setting up a schedule, you automate the start of your backups.

security protocol A communications protocol that encrypts and decrypts a message

Glossary

for online transmission. Security protocols generally also provide authentication. The security protocols that have emerged on the web are Netscape's SSL, NCSA's SHTTP, Microsoft's PCT, and the IETF's IPsec. Web browsers and servers generally support all the popular security protocols.

session *See* **backup session** and **restore session**.

shared disks A Windows NT shared disk is a disk on another system that has been made available to other users on the network.

SLA service level agreement

SLO service level objectives

slot A slot is a mechanical position in a library. Each slot can hold a medium, such as a DLT tape. Some Backup Managers refer to each slot by a number. To read a medium, a robotic mechanism moves the medium from a slot into the drive.

sparse file A file whose virtual size is greater than its actual bit size because the file contains empty blocks. For example, a 10 megabyte sparse file may

actually contain only 5 megabytes of data. If you do not enable sparse file processing during restore, it might be impossible to restore this file.

stackers Devices with multiple slots for media storage usually with only one drive. A stacker selects media from the stack sequentially. In contrast, a library can randomly select media from its repository.

tablespace A part of a database structure. Each database is logically divided into one or more tablespaces. Each tablespace has data files or raw volumes exclusively associated with it.

time entered The time that you entered the request (automatically entered).

unattended operation *See* **lights-out operation**.

user profile *Windows NT specific term.* Configuration information retained on a user basis. This information includes desktop settings, screen colors, network connections, and so on. When the user logs on, the user profile is loaded and the Windows NT environment is set accordingly.

Glossary

user rights *See* **access rights**.

vault An onsite or offsite storage location for removable media.

vaulting job Performs the daily media operation related to moving media between onsite and offsite locations to meet the vaulting policies for that site.

vaulting policy Defines how long the media are retained in the backup/restore device that was last used, in an onsite vault, in an offsite vault, and in the vaulting cycle.

VG — volume group A unit of data storage in an LVM system. A volume group can consist of one or more physical volumes. There can be more than one volume group on the system.

volser — VOLume SERIAL number A label on the medium to identify the physical tape used in very large libraries. A volser is a naming convention specific to GRAU and STK devices.

Windows NT Registry A database repository about the computer's configuration.

WINS server A system running Windows Internet Name Service software that resolves Windows networking computer names to IP addresses.

A

- active, 95
- adding
 - backup managers, 22, 36
 - grids, 77
 - media types, 90
 - sites, 22, 73
 - vaulting policies, 96
- alerts, 161
- application managers, 227
- audits, 183
 - history, 103
 - importing, 186
 - location, 179
 - problems, 183
 - requests, 205
- auto pass license key, 197
- automatic backup, configuring, 81

B

- backup, 165
 - configuring processes, 81
 - database, 89
 - manual environment, 82
 - tuning objects, 89
- backup managers, 9, 84
 - adding, 22, 36
 - deleting objects, 68
 - editing, 63
 - home site, 66
 - integrating with, 6
- backup specifications
 - media list, 165
 - vaulting policy, 93
- barcode printer, 12
- barcode scanner, 11
- barcode scans, 6
- barcodes
 - labeling policies, 98
 - number sequence, 98
 - printing, 98
 - using for initializing, 132
- bulk configuration file imports, 213

C

- cabinets, creating, 33
- checkout requests, 137
 - job listing, 139
- communications port number, 225

- compression, refining, 90
- configuration files, bulk import, 213
- configuration report, 87
- configuring
 - automatic backup, 81
 - backup processes and objects, 81
 - email interface, 167
 - Media Operations, 71
 - media vaulting policies, 92
 - notification triggers, 168
 - OVO interface, 167
 - premount jobs, 99
 - problems, 161
 - scratch media policies, 99
 - sites, 73
 - SLA status, 158
 - XML gateway, 220
- connecting to server, 19
- container media list, 165
- containers, 121, 129
- copying media, vaulting policies, 94
- COR, 137
 - holding area, 180

D

- daily jobs, 105
- data centers, 49, 74, 77
 - importing grids, 213
- data management communications, 224
- Data Protector, 228, 230
- data retention, 4
- database backup, 89
- deleting
 - backup manager objects, 68
 - sites, 63
- device definitions, 214
- device media list, 165
- device scan, 88
- diagnostics, 217
- dismount listing, 111
- DMComms, 224
- DNS suffixes, 44
- drawers, creating, 33

E

- editing
 - backup manager, 63
 - grids, 77
 - site, 43
 - sites, 74

Index

ejecting media, 112
email interface, 167
Environmental Limitations, 11
export remote account report, 185
external interfaces, 199

F

features, 14
firewalls, 7
formats, XML offsite vendor file, 206

G

generic vendor type, 12, 27
 creating account, 56
grids, 77
groups, XML gateway, 87
GUI, 8, 9
 web, 149
 web client, 10
 Windows, 21
 Windows client, 9

H

history, 165
 alerts, 161
 backup media, 165
holding bin, 182
home site, 66

I

importing, 214
 audit list, 186
 bulk configuration files, 213
 data, 60
 data center grid, 213
 device definitions, 62, 214
 media locations, 213
 offsite vendor file, 186
 system grid locations, 213
initializing standalone drives, 131
installing
 Media Operations Manager, 191
 Media Operations server, 188
 XML gateway, 85, 193
integrating
 backup managers, 6, 81
 vis XML gateway, 6
interfaces
 external, 199

XML file import, 201
XML offsite vendor, 203
Iron Mountain, 76
Iron Mountain vendor type, 13, 27
 creating account, 55

J

jobs
 daily, 105
 manual vaulting, 146
 media order, 124, 133
 metrics, 174
 notifications, 170
 premount, 103, 108, 156
 scratch bin, 124
 scratch initialization, 124, 131, 156
 status, 173
 status indicators, 107
 vaulting, 103, 115
 viewing history, 147

L

languages supported, 13
license key, 197
licenses, viewing, 198
licensing, 197
lifecycle, media, 4
links to offsite vendors, 12
listing
 checkout request jobs, 139
 dismount, 111
 mount, 111
 mount request, 144
 premount jobs, 109
 scratch jobs, 125
 scratch media, 109
 vaulting jobs, 116
loading media, 112
location
 audits, 179
 metrics, 178
locations, refining, 89
lockable containers, 121
logging on, 20
 to Media Operations Manager, 20
 to web interface, 21
logs
 Media Operations Manager, 219
 Media Operations server, 219

service, 224
XML gateway, 220, 222

M

manual backup
 environment, 82
 implementing, 84
manual media definitions, 62, 214
manual vaulting jobs, 146
media, 165
 adding and modifying types, 90
 ejecting, 112
 importing locations, 61
 lifecycle, 4
 loading, 112
 movement report, 164
 order jobs, 124, 133
 policies, 92
 pools, 114
 vaulting policy, 93
 scans, 6
 scratch, 124
 transit requests, 205
 vaulting policies
 configuring, 92
 hierarchy, 93
media locations
 importing, 213
Media Operations
 manager systems, 8
 server, 8
Media Operations Manager, 2
 installing, 191
 logs, 219
metrics, 171
 job, 174
 location, 178
 pool health, 175
 premount, 175
 remote, 177
 report, 173
 scratch media, 177
 vault, 178
 vaulting, 176
 vendor, 177
modifying media types, 90
monitoring, 85
mount listing, 111
mount requests, 144

 reactive, 100
multiple sites, 122, 130
multiple users, 122, 130

N

NetBackup, 228, 230
notifications, 166
 metrics, 171
 SLA, 169

O

offsite storage vendors, 73
offsite vendor
 importing file, 186
offsite vendors, 12, 26, 76
Omniback, 228, 230
operator-level administrators, 80
optimizing backup objects, 89
OVO interface, 167

P

pending, 183
platform support, 11
policies, 92
polling schedule, 87
pool health metrics, 175
pool media list, 165
port number, changing, 225
premount jobs, 103, 108
 configuring, 99
 listing, 109
premount metrics, 175
printer, barcode, 12
printing
 audits, 184
 barcodes, 98
product administrators, 78

R

reactive mount requests, 100, 206
remote accounts, 80
 defining, 59
remote metrics, 177
reports, 163
 additional, 165
 backup specifications media, 165
 configuration, 87
 container media, 165
 device media, 165
 device scan, 88

Index

- export remote account, 185
- media information, 88
- media movement, 164
- metrics, 173
- pool media, 165
- scratch media, 164
- systems media, 165
- vault audit, 163

requests, reactive mount, 206

reserving slots, 75

rows, creating, 34

S

- scanner, 11
- scratch bin
 - jobs, 124
 - maintenance, 103
- scratch initialization job, 131, 156
- scratch initialization jobs, 124
- scratch jobs listing, 125
- scratch media, 124
 - levels, tuning, 100
 - listing, 109
 - metrics, 177
 - policies, configuring, 99
 - pool handling, 114
 - report, 164
- security management, 78
- server
 - connecting to, 19
 - installing, 188
 - logs, 219
 - parameters, 86, 101
 - parameters, notifications, 166
- service level agreements, 152
- service logs, 224
- site default vaulting policy, 74
- Site Definition, 43
- site management, 73
- site, editing, 43
- site-level administrators, 79
- sites
 - adding, 22, 73
 - deleting, 63
 - editing, 74
 - multiple, 122, 130
- SLA notifications, 169
- SLAs, 152
 - current status, 153
 - status configuration, 158

- threshold, 159
- slots, reserving, 75
- standalone drives, initializing, 131
- status checking requests, 206
- status indicators, 107
- super operator-level administrators, 79
- supported platforms, 11
- system grid locations, 61
 - importing, 213
- system threshold, 158
- systems
 - media list, 165
 - vaulting policy, 94

T

- TCP/IP broadcasting system, 19
- templates, vaulting, 95
- threading, 222
- top-level administrators, 78
- transit containers, 122
- tuning, 217
 - scratch media levels, 100
 - XML gateway, 220, 223
- tuning backup objects, 89

U

- user interface, web, 149
- users
 - accessing, 78
 - multiple, 122, 130
 - site definition, 57
 - types, 78

V

- vaulting
 - containers, 121
 - cycle, 25
 - job information, 155
 - jobs, 103, 115
 - manual jobs, 146
 - metrics, 176
 - offsite, 26
 - onsite, 32
 - templates, 95
 - threshold, 159
- vaulting policies, 50, 95
 - adding, 96
 - basic concepts, 94
 - creating, 23

- default, 93
 - viewing active, 98
- vaulting policy
 - default, 74
- vaults, 73, 75
 - audit report, 163
 - metrics, 178
 - priorities, 75
- vendor metrics, 177
- VERITAS NetBackup, 230
- VERITAS Netbackup, 228
- viewing licenses, 198

W

- web interface, logging on, 21
- web user interface, 149

X

- XML file import
 - directory, 88
 - format, 202
 - interface, 201
- XML Gateway, 65
- XML gateway, 6, 9, 40, 85
 - adding group, 64
 - configuration, logs and tuning, 220
 - groups, 87
 - installing, 85, 193
 - logs, 222
 - threading, 222
 - tuning, 223
- XML offsite vendor
 - file format, 206
 - interface, 203

