HP Data Protector Media Operations A.06.20

User Guide

Part Number: n/a
First edition: March 2011

Legal and notice information

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.

Contents

Figures

Tables

About this guide

This guide provides information about:

- planning and preparing for a disaster
- testing a disaster recovery procedure
- successfully performing a disaster recovery

Intended audience

This guide is intended for users of HP Data Protector Media Operations, with knowledge of:

- Data Protector concepts

Related documentation

HP Media Operations provides three guides, together with context-sensitive (F1) Help and Help Topics for Windows platforms. The guides are available printed and in PDF format. The PDF files are installed during the Media Operations setup procedure on Windows. Once installed, the manuals reside in the `Media_Operations_home\docs` directory on Windows.

You can also find these documents from the Manuals page of the HP Business Support Center website:

http://www.hp.com/support/manuals

In the Storage section, click **Storage Software** and then select your product.

There are three guides specific to Media Operations:

- *HP Data Protector Media Operations Getting Started Guide*—containing a pre-installation checklist, a ten-minute installation guide and a fifteen-minute configuration guide
- *HP Data Protector Media Operations User Guide*—this guide

- *HP Data Protector Media Operations Product Announcements, Software Notes, and References*—containing a list of resolved issues, late breaking news and other information

Document conventions and symbols

Table 1 Document conventions

Convention	**Element**
Blue text: Table 1	Cross-reference links and e-mail addresses
Blue, underlined text: http://www.hp.com	website addresses
Bold text	• Keys that are pressed • Text typed into a GUI element, such as a box • GUI elements that are clicked or selected, such as menu and list items, buttons, tabs, and check boxes
Italic text	Text emphasis
`Monospace` text	• File and directory names • System output • Code • Commands, their arguments, and argument values
`Monospace, italic` text	• Code variables • Command variables
`Monospace, bold` text	Emphasized monospace text

△ CAUTION:

Indicates that failure to follow directions could result in damage to equipment or data.

ⓘ IMPORTANT:

Provides clarifying information or specific instructions.

NOTE:

Provides additional information.

TIP:

Provides helpful hints and shortcuts.

General Information

General information about DPNE can be found at http://www.hp.com/go/dataprotector

HP technical support

For worldwide technical support information, see the HP support website:

http://www.hp.com/support

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website:

http://www.hp.com/go/e-updates

After registering, you will receive e-mail notification of product enhancements, new driver versions, firmware updates, and other product resources.

HP websites

For additional information, see the following HP websites:

- http://www.hp.com
- http://www.hp.com/go/storage
- http://www.hp.com/support/manuals
- http://www.hp.com/support/downloads

Documentation feedback

HP welcomes your feedback.

To make comments and suggestions about product documentation, please send a message to DP.DocFeedback@hp.com. All submissions become the property of HP.

1 Media Operations overview

In this chapter

This chapter describes the general principles on how Media Operations works. It is organized as follows:

- "Media Operations concepts" on page 17
- "Logging on to Media Operations" on page 21
- "Environmental requirements" on page 24

Media Operations concepts

Media Operations tracks and manages online, offline, and offsite storage media, such as magnetic tapes. The result is reliable backups, fast data recovery, improved staff efficiency, and reduced costs. Major benefits are as follows:

- **Scalable and Highly Flexible Architecture**

  Media Operations can be used in environments from a single system to thousands of systems on different sites.

- **Easy Central Administration**

  Through its easy-to-use graphical user interface (GUI), you can administer your environment from a single system. The GUI can be installed on various systems to allow multiple administrators to access Media Operations.

- **High Performance**

  You can track thousands of removable media regardless of their location, including creating daily task lists, organizing tapes for logical data center walk-throughs, and controlling tape libraries, barcode scanners, and media label printers.

- **Integration with Backup Applications**

  Media Operations integrates with leading backup applications, including HP Data Protector and Symantec NetBackup.

- **Cost-efficiency**

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

- **Automated Operation**

  Media Operations enforces data retention and media recycling policies. Through it, you can control removable backup devices for tape loads and ejects.

  Additionally, it automates data exchange with backup applications, offsite vaulting services, and removable media suppliers.

- **Monitoring, Reporting and Notification**

  Service Level Agreement (SLA) Status/Reporting functionality allows you to check whether SLAs are being met. You can monitor configuration errors and generate reports, view SLA status and alerts, and run reports at both global and site level. Additionally, you can configure automatic notification by e-mail or to Operations Manager (OM) for key events such as alerts, job creation, and SLA warnings.

Media lifecycle

Media Operations allows lifecycle management of removable media (see "Media lifecycle" on page 19), which includes:

- Moving live media from backup/restore devices (tape libraries and standalone tape drives) to onsite/offsite tape vaults for disaster protection.
- Moving scratch media from scratch bins into backup/restore devices to provide usable media for upcoming backup jobs. Scratch media are generated by moving expired media from tape vaults to scratch bins and by creating new scratch media when necessary.
- Moving live media from onsite/offsite tape vaults to backup/restore devices to meet recovery requests.

NOTE:

Media Operations does not control the data held on a medium; this is the responsibility of the Backup Manager.

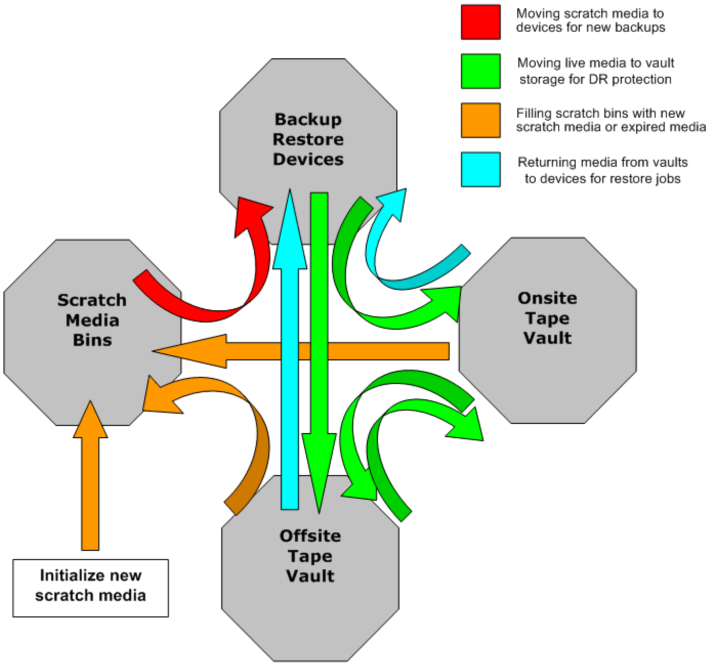

🟥 Moving scratch media to devices for new backups
🟩 Moving live media to vault storage for DR protection
🟧 Filling scratch bins with new scratch media or expired media
🟦 Returning media from vaults to devices for restore jobs
Backup Restore Devices
Scratch Media Bins
Onsite Tape Vault
Offsite Tape Vault
Initialize new scratch media

Figure 1 Media lifecycle

Components

Major Media Operations components are:

- **Media Operations Server**, containing:
    - a database of data objects (such as devices, media, media pools) and their attributes,
    - business logic to process administrator-defined vaulting and scratch policies, and lists of tape movements to be performed,
    - scheduling and SLA monitoring functions.
- **Media Operations Manager**—a graphical interface used to remotely configure, monitor, and run your media vaulting and scratch media policies. There are Windows and web-based versions. You can also attach a barcode scanner to the client system to input barcodes from large numbers of media as they are moved between locations.
- **XML Gateway**—providing integration between Media Operations and Backup Managers. For details of versions of HP Data Protector and Symantec NetBackup supported by Media Operations A.06.20, see "Installing XML Gate-

way" on page 29. The XML file import interface facilitates integration of Backup Managers not currently supported by XML Gateway.

- **Backup Manager**—such as HP Data Protector, controlling backup functions. Media Operations interacts with Backup Managers to track and provide medium use. After installing Media Operations on Media Operations Server, you can track media from a variety of Backup Managers.

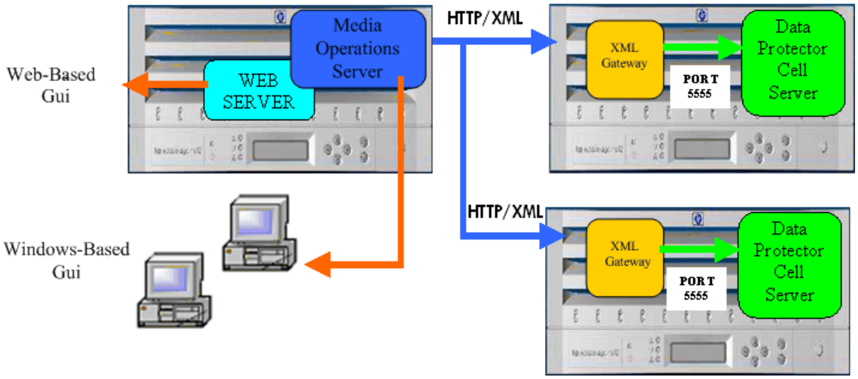


Figure 2 Components

Integration with backup manager

Media Operations integrates with the Backup Manager via:

- XML Gateway
- XML file import, allowing integration with Backup Servers not supported by XML Gateway

Media Operations uses these to extract configuration information from the Backup Manager, which autoconfigures devices, media pools, systems, and backup specifications. It also extracts current media information. XML Gateway interface allows Media Operations to trigger barcode and media scans in any of the Backup Server's tape libraries/devices. This provides up-to-date information on the contents of these devices.

For more information about supported interfaces, see "Backup managers" on page 66.

Logging on to 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. The **4D Server Connection** window appears, containing the following tabs:

- **Recent Tab**

  Lists all 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**

  Lists the names of the server databases over the network. 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**

  Assigns 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 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. However, if you know the IP address of the server whose name is not broadcast, you can type its IP address.

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

Using Media Operations graphical user interface

Media Operations provides GUIs available from the client system (Windows client) and from the internet (web client).

Windows client

Windows GUI allows you to administer the complete media lifecycle environment from a single system. It can be used from the Server or a desktop system.

You can also install the GUI on several systems, allowing multiple users to access Media Operations via locally installed consoles.

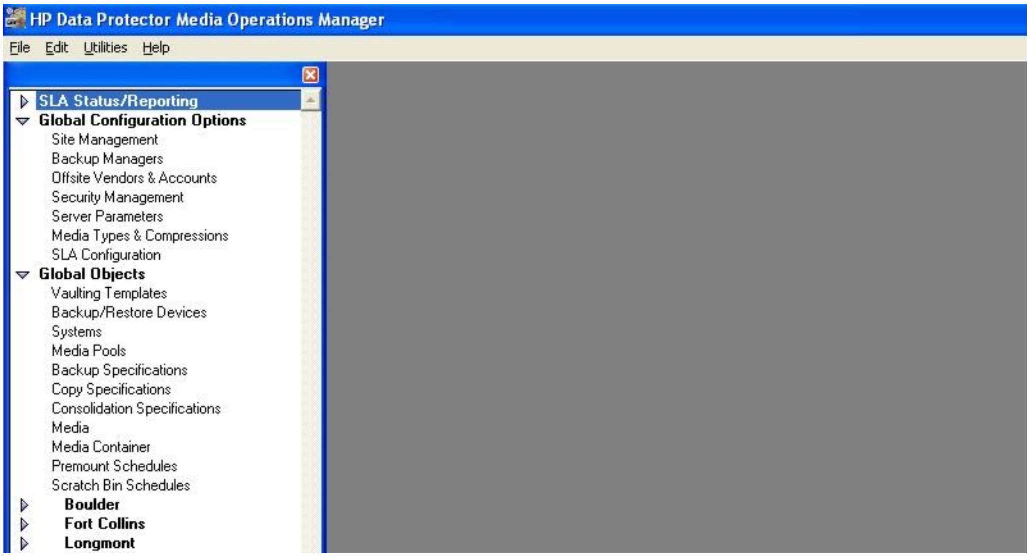


Figure 3 Media Operations GUI

To start the Media Operations GUI:

1. Click **Start** on the Windows desktop and select **Media Operations Manager**.
2. In the **4D Server Connection** window, select the server to which you want to connect from the 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**. The Media Operations GUI is started.

NOTE:

If you are running Media Operations in “demo” mode and you have media configured, an alert tells you how many days are left before the product switches to “expired” mode (see “Licensing Media Operations” on page 36).

Web client

The web-based GUI provides operator functions only. You must perform site configuration functions from the Windows client.

To log to Media Operations web GUI:

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. 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 hosts another web server, type the network name or IP address followed by “`:3612`”. For example:

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

Using the CLI

You can start Media Operations jobs through the command line interface (CLI). See “Running jobs through the CLI” on page 93 for the syntax.

Environmental requirements

Platform support

NOTE:

Combinations of Media Operations component and operating system/processor platforms are only supported where the operating system version is still supported by its vendor.

The basis for the Media Operations Server and Media Operations Manager components is a product called 4D version 6.8 from 4D, Inc. The functionality of Media Operations is limited to the features that 4D offers. Limitations apply for support for clusters and also support for 64-bit processor architectures and 64-bit versions of the Microsoft Windows operating systems. The Media Operations Server and Manager are therefore supported only on 32-bit processor architectures and 32-bit versions of Microsoft Windows operating systems.

For the most up-to-date information about platform support, see the Support Matrix for Media Operations, which lists all software and hardware requirements, at this location: https://h20230.www2.hp.com/selfsolve/manuals.

Most of the support areas require that you register as an HP Passport user and sign in. Many also require an active support contract. To find more information about support access levels, go to: http://support.openview.hp.com/access_level.jsp.

To register for an HP Passport ID, go to: http://h20229.www2.hp.com/passport-registration.html.

Barcode scanner support

Barcode scanners are supported on the Media Operations Server, Media Operations Manager Client, and the Media Operations GUI on a server running IE or Netscape, provided that the scanner behaves like a keyboard and emulates **Enter** (not carriage return) after scanning.

Barcode printer support

Media Operations Server supports any Zebra 300 dpi label printer.

These printers are also supported when attached to a supported Media Operations Manager.

Media Operations Server supports the following tape libraries for use with the barcode labels it prints:

- 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 84 for more information about barcode support.

Offsite vendor support

Media Operations supports electronic links to offsite vendors. This allows electronic verification of media being shipped to offsite storage, and provides electronic requests to return media from offsite storage to the data center (for recovery jobs).

Offsite vendor types are Media Operations, Generic, and Iron Mountain. For descriptions, see "Site management" on page 39.

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 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 2 Supported languages

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 3 Supported languages—intersite transfers

Client Locale	Server Locale
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)

2 Installing and licensing

Installing Media Operations

This chapter tells you how to install the following Media Operations components manually from the installation DVD or CD:

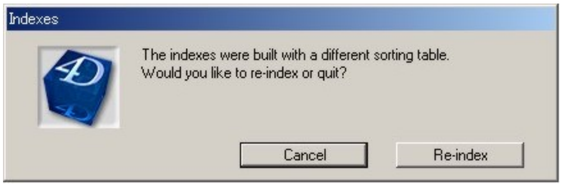
- Media Operations Server
- XML Gateway
- Media Operations Manager (optional)

Prerequisites

- Minimum requirements for the Media Operations Server: 500 MHz Pentium III CPU (or above), 256 MB RAM, and 500 MB free disk capacity. A dual processor machine is highly recommended. Installation checks that sufficient disk space is available.
- The unlicensed version of the product is a fully functional demo version (see "Licensing Media Operations" on page 36). The administrator installs license keys after the product is installed.
- It is recommended to install Media Operations Server onto a tape backup product client, as it provides a tape backup mechanism for the Media Operations Server data.
- Media Operations Server installation includes a built-in web server that provides the web-based Media Operations GUI. The server installation package detects any existing web server on the system, and warns you that another port (3612) will be used for Media Operations Web Server (so that it can co-exist with the existing web server).
- To install the Media Operations Server successfully, you need a local printer. If no local printer is connected to your system, 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 without issues. Media Operations Clients and Servers in languages that use double-byte character

sets (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 the *HP Data Protector Media Operations product announcements, software notes, and references* for more information.

- When installing Media Operations in a double-byte language environment, the following screen gives you an option to cancel or re-index. Click **Re-index** within 30 seconds to avoid timing out.



Indexes

The indexes were built with a different sorting table.
Would you like to re-index or quit?

Figure 4 Indexes

Installing Media Operations Server

NOTE:

Media Operations server is not supported in a Windows cluster environment.

If a Backup Manager is installed on a cluster environment, while adding this Backup Manager in Media Operations, you must specify the virtual name of the cluster as the Backup Manager name.

To install the Media Operations Server:

1. Insert the installation DVD or CD and run `setup.exe` from the `server` directory.
2. Click **Next**.
3. Read the license agreement and click **Yes** to accept it.
4. Enter the destination for the files. The default location is `C:\Hewlett-Packard\DataMgt\MediaOps`. To install to a different location, click **Browse** to select the location. Click **Next**.

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

5. Select the location for data management communication service files. Communications service is a common component that can be used by other Data Management applications. To install to a folder other than the default, click **Browse** to select the destination. Click **Next**.
6. Type an initial top-level administrator username and password. Make a note of the username and password; they are the only way to log in until you create additional users.

NOTE:

The password has a maximum length of 10 characters.

7. Go back to review your settings, or proceed with the installation.
8. Read the ReadMe file, or click **Finish** to exit the installation wizard.

Installation is now complete. You should see the server console window for the Media Operations Server.

Installing XML Gateway

There are standalone installation packages that support installing XML Gateway on Microsoft Windows, HP-UX, Linux, and Solaris. Media Operations A.06.20 XML Gateway integrates with the following supported Backup Managers:

- HP Data Protector A.06.20, A.06.11, A.06.10, and A.06.00
- Symantec NetBackup Server 6.0
- Symantec Enterprise Server 6.0

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

NOTE:

For NetBackup, XML Gateway *must* reside on the NetBackup Master server.

If you are installing XML Gateway in a cluster environment, it must be installed on both active and passive nodes. If you want to use the XML Gateway that is installed on a cluster configuration, specify the virtual name of the cluster as the XML Gateway name while adding the Backup Manager in Media Operations.

Installing XML Gateway on Windows

NOTE:

If you are installing the XML Gateway after installing a Media Operations server, to avoid having to restart, stop the DMComms in between the installations.

To install XML Gateway:

1. Insert the installation DVD or CD and run `setup.exe` from the `\xmlgw\windows` directory.
2. Click **Next**.
3. Read the license agreement and click **Yes** to accept it.
4. Enter the destination for the XML Gateway files. The default location is `C:\Hewlett-Packard\DataMgt\DPXMLGW`. To install to a different location, click **Browse** to select the destination. Click **Next**.
5. *If you have already installed the Media Operations Server, this step is skipped.* Select the location for the data management communication service files. Communications service is a common component that can be used by other data management applications. To install to a folder other than the default, click **Browse** to select the destination. Click **Next**.
6. Go back to review your settings, or proceed with the installation.
7. Read the ReadMe file, or click **Finish** to exit the installation wizard.

Installing XML Gateway on Unix

Prerequisites

- Make sure you have root access or an account with root capabilities.
- A Unix system that will become your future XML Gateway host must have:
  - supported Unix version installed,
  - sufficient disk space for the XML Gateway,
  - port numbers 25555 and 25556 free,
  - TCP/IP protocol installed and running (able to resolve hostnames).

To install on HP-UX:

1. Insert the installation DVD or CD 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 the `max_thread_proc` parameter of the HP-UX kernel is set to at least 512 (the maximum number of threads allowed per process). For more details, see “Kernel tuning” on page 159.

See HP-UX documentation for additional information on `swinstall`.

To install on Solaris:

1. Mount the installation DVD or CD to the directory: *<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
   <HPdpxmlgw> [y,n,?]
   ```

   Type `y` to continue.
4. Start the gateway services:

   ```
   /opt/hpdmcomms/sbin/start_hpdmcomms nl /opt/hpdpxmlgw/sbin/
   start_hpdpxmlgw
   ```

NOTE:

When upgrading from the existing XML Gateway version to A.06.20, if the directory `/opt/hpdmcomms` still remains after uninstalling the existing version, remove the directory manually (using the command `rm –f /opt/hpdmcomms`) to avoid any conflicts.

To install on Linux:

1. Insert the installation DVD or CD and mount it.
2. Execute the following command:

   ```
   rpm -ivh <rpmpath>/HPMedOps.rpm
   ```

This installs the XML Gateway on the Linux machine and also starts the Java services.

NOTE:

When upgrading from the existing XML Gateway version to A.06.20, if the directory `/opt/hpdmcomms` still remains after uninstalling the existing version, remove the directory manually to avoid any conflicts.

NOTE:

If the RPM installation fails with the error “Failed dependencies”, you need to install the dependent libraries before installing the RPM.

Stopping Gateway Services on UNIX

To stop Gateway Services on UNIX, run the following commands:

```
/opt/hpdmcomms/sbin/stop_hpdmcomms
```

```
/opt/hpdpxmlgw/sbin/stop_hpdpxmlgw
```

Uninstalling XML Gateway

To remove the XML Gateway:

HP-UX: type `swremove HPMedOps`

Solaris: type `pkgrm HPdpxmlgw`

Linux: type `rpm -e HPMedOps`

Installing Media Operations Manager (optional)

Media Operations Manager provides the GUI to Media Operations. Install it to provide Media Operations for a local site when Media Operations Server is located on another site.

NOTE:

Media Operations Manager copy is included with the Media Operations Server, so you do not need to install the Media Operations Manager on the Server System.

To install Media Operations Manager:

1. Insert the installation DVD or CD and run `setup.exe` from the `client` directory.
2. Click **Next**.
3. Read the license agreement and click **Yes** to accept it.
4. Enter the destination for the files. The default location is `C:\Hewlett-Packard\DataMgt\MediaOps`. To install to a different location, click **Browse** to select the location. Click **Next**.
5. Go back to review your settings or proceed with the installation.
6. Read the ReadMe file, or click **Finish** to exit the installation wizard.

Installation is now complete. You should see the **Media Operations Manager** icon on the desktop and a **Media Operations** option in your **Start** menu.

Upgrading to Media Operations A.06.20

The following upgrade paths are supported:

- Media Operations 6.10 to Media Operations 6.20
- Media Operations 6.11 to Media Operations 6.20

Before upgrading an existing product version to Media Operations release A.06.20, consider the following:

- Refer to the *HP Data Protector Media Operations product announcements, software notes, and references* for information about supported and discontinued platforms and versions.

- After the upgrade, the Media Operations Server and all XML Gateways must have Media Operations version A.06.20 installed.
- If you have a permanent license for Media Operations A.05.xx or A.06.xx, you can use it with Media Operations A.06.20.

  For details about licensing, see "Licensing Media Operations" on page 36.

Before you begin

Back up the existing Media Operations Server system and the Media Operations database.

NOTE:

It is mandatory to back up the Media Operations database. You can manually save the data files available in the location *<MediaOperations_install_dir>*\MediaOps\DBServer\MediaDB to a temporary location. After upgrading the Media Operations Server version, copy back the saved data files to *<MediaOperations_install_dir>*\MediaOps\DBServer\MediaDB. (This backup procedure helps in restoring data files in cases where the upgrade fails and you have to reinstall the product).

Upgrading Media Operations Server and Manager to A.06.20

Use the following procedure if Media Operations Server version A.06.10 or A.06.11 is installed on your system.

NOTE:

If the services are manually stopped before the upgrade, you must ensure that the Services window is closed before starting the upgrade, otherwise the upgrade will fail.

NOTE:

If the Media Operations Server and XML Gateway are installed on the same system, stop all Media Operations services before starting the upgrade. This avoids re-starting the system when the upgrade is complete.

1. Run `setup.exe` for the Server version A.06.20. This starts the upgrade wizard for Media Operations Server installation. The upgrade process stops all the running A.06.10 or A.06.11 server services and copies the new files onto them.
2. If XML Gateway is installed on the same system as the server, upgrade the gateway manually to the newer version.

Upgrading Media Operations XML Gateway to A.06.20

Use the following procedure if XML Gateway version A.06.10 or A.06.11 is installed on your system.

Upgrading on Windows

NOTE:

If the Media Operations Server and the XML Gateway are installed on the same system, stop all Media Operations services before starting the upgrade. This will avoid re-starting the system once the upgrade is completed.

1. Run `setup.exe` for the XML Gateway version A.06.20. This starts the upgrade wizard for the XML Gateway installation. The upgrade process stops the running XML Gateway on the system and copies the new files onto the existing ones.
2. After a successful upgrade, the XML Gateway services start up.

Upgrading on HP-UX

NOTE:

You must have root permission to perform the upgrade.

Install the new version of XML Gateway by executing the command:

```
swinstall -s <A.06.20_depot_location>/HPMedOps.depot HPMedOps
```

For more details, see “Installing XML Gateway on Unix” on page 30.

Upgrading on Solaris:

On Solaris, you need to remove the older version of the XML Gateway before installing a new version.

NOTE:

You must have root permission to perform the upgrade.

1. Remove the older version of the XML Gateway, using the command:
   ```
   pkgrm HPdpxmlgw
   ```
2. Install the new version:
   ```
   pkgadd -d <A.06.20_package_location>/HPMedOps.pkg HPdpxmlgw
   ```
   For more details, see "Installing XML Gateway on Unix" on page 30.

Upgrading on Linux

On Linux, you need to remove the older version of the XML Gateway before installing a new version.

NOTE:

You must have root permission to perform the upgrade.

Remove the previous version of the XML Gateway, using the command: rpm -e HPMedOps Install the new version: `rpm -ivh A.06.20_package_location/HPMedOps.rpm`

For more details, see "Installing XML Gateway on Unix" on page 30.

Licensing Media Operations

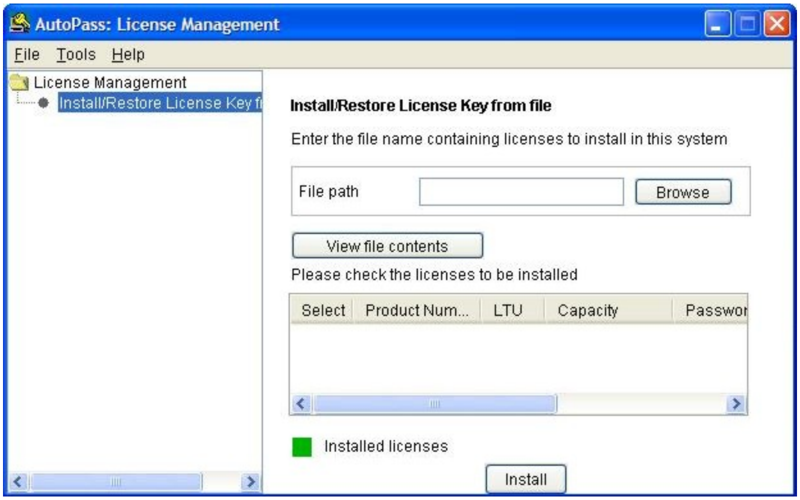
When you first install Media Operations, it has no license key and is acting as a demo product (with a 60-day time limit and unlimited media license). While the product is in "demo" mode, a message is displayed every time you log in showing how many demo days remain.

The product is fully usable until the 60 days expire. After that, the product switches to "expired" mode; you cannot run any daily media movement jobs, except checkout request jobs, and the web GUI is disabled. Every time you log in, an error dialog prompts you to install the appropriate number of licenses.

Although you cannot use the product in expired mode, the server continues to run any scheduled activities, such as polling for new information from the Backup Managers or making database backups. Any new media detected on the Backup Managers are added into the Media Operations database. This ensures the product is kept in sync with the environment—when it switches to a 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 **AutoPass License Key** application in a separate window. Use this to install new license keys.

NOTE:

The Media Operations Server system must have JRE 1.4.2 or higher version installed in order to use AutoPass for Media Operations licensing.



Install/Restore License Key from file

Enter the file name containing licenses to install in this system

Please check the licenses to be installed

Figure 5 AutoPass license key

Each key allows an increment of either 2000 or 10,000 to the maximum managed media limit (the increment is encoded in the license key). You can also buy a license to manage unlimited number of media.

When a new license key is entered using this option, it is checked to ensure that it is different from any existing license key, and that it is a valid Media Operations license key.

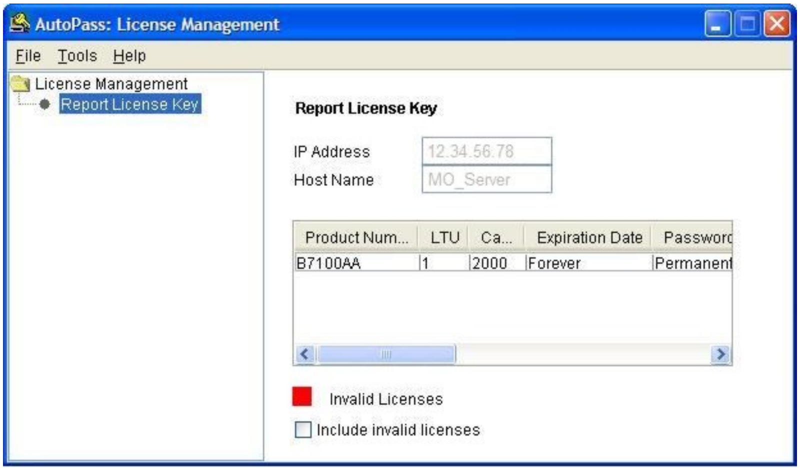
If the new key is unique and valid, the media license is extended by either 2000, 10,000, or unlimited media depending on the key.

After installing sufficient licenses to cover your expected managed media, the product becomes fully operational.

If you do 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 this mode, you have 60 days to install sufficient new licenses. During this period, Media Operations remains fully operational. If you have not installed sufficient licenses by the end of 60 days, Media Operations switches into “expired” mode; 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 licenses

On the **Utilities** menu of the Media Operations Server, click **View Licenses** to view your current license configuration.



Report License Key

IP Address: 12.34.56.78

Host Name: MO_Server

Product Num...	LTU	Ca...	Expiration Date	Passworc
B7100AA	1	2000	Forever	Permanent

🟥 Invalid Licenses

□ Include invalid licenses

Figure 6 AutoPass report licenses

3 Configuring Media Operations

In this chapter

This chapter includes information on the following:

Site management

A site is a geographic location with one or more data centers and a common set of operators. Media Operations allows you to configure and manage multiple physical sites with different service level agreements (SLAs).

Each site's configuration defines the physical layout of devices and available onsite and offsite vault locations.

A site consists of the following:

- **Vaults**

  Vaults reflect the physical layout of secure media storage in a site. They consist of cabinets, drawers, rows, and slots created in that order.

  Vaults have no capacity until you create rows and slots. When creating a row, define what media type will fit into the slots. If you add a new media type that does not fit into the defined vault slot types, you need to add a new slot-type definition, and then define the rows that accept this media type. See "Adding and modifying media types" on page 79 for more information.

  You can create vaults either manually or automatically (if your vault has a structured addressing scheme for its components).

You can edit vaults from the **Site Configuration** window provided you have permissions to edit sites. If you delete a vault, all media in the vault are moved to the holding bin for the deleted vault site.

Vaulting Policy

Vaulting policies are rules defining what happens to the medium after the backup. Every site has a default vaulting policy assigned when new media pools are created/added.

Either create your own vaulting policy, or use one of the pre-defined templates. See "Configuring media vaulting policies" on page 79 for more information.

Vault Priorities

When you configure vaulting policies, Media Operations puts the media into the most appropriate vault in the destination site. Vault selection depends on whether the vaults support the media's vault-slot type, whether there are free slots, the vault's onsite and offsite priorities, and the reserved slots configuration.

You can assign onsite and offsite priority to each vault to define which vault is the preferred recipient of the local site (online priority) or the offsite (offline priority) media.

Reserving Slots

To control media allocation, you can reserve slots for exclusive use with a specified media pool. Media from the pool can only be stored in the reserved slots. You can apply this configuration at row, drawer, or cabinet level.

To view a list of reserved slots, click the **Reserved Slots** tab on the **Onsite Vault Management** window.

- **Offsite Storage Vendors**

  Offsite vendors are secure media locations not controlled by the Media Operations Server, such as other Media Operations Servers within your own company or external vendors.

  You can manually add offsite storage vendors and accounts, and select them as part of media vaulting policies.

NOTE:

Once defined, offsite vendors can be used for any site. Each site, however, has its own unique account with the offsite vendor, identifying the owner of each medium.

Media Operations supports electronic links to offsite vendors. This enables electronic verification of media shipped to offsite storage. It also enables electronic requests to return the media from offsite storage back to the data center (for example, for data recovery). For more information about electronic link interfaces, see "External interfaces" on page 141.

Three offsite vendor types are:

- *Media Operations*

  This is used when your offsite storage location is another Media Operations Server. An electronic link between the two servers automatically creates jobs on the offsite server for outgoing and returning media, and provides status information on the offsite jobs. In addition, there are auditing options for synchronizing two Media Operations Servers if they get out of sync.

- *Generic*

  This is used when there is not another Media Operations Server at your offsite storage location. If the offsite vendor has their own proprietary electronic interface, customized scripts convert information from Media Operations into the vendor's electronic link protocol.

- *Iron Mountain*

  This is used when your offsite vendor is Iron Mountain and an Iron Mountain FTP electronic link (SecureBase) is used. If you are not using the FTP link, use the Generic vendor.

- **Data Centers**

  Data centers are collections of systems and backup devices within a site. 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 it because it is the default repository for any device or system created without a specified data center (such as automatically created devices and systems). You can change the data center assignment if you have additional data centers. See "Refining physical locations" on page 78 for details.

  Configuring data centers helps you optimize premount jobs. Premount jobs are faster and more efficient if the premount walk-through is grouped in a logical order by physical location (when the shortest/quickest path from device to device is used).

  Data Center Grids

  You can further optimize the device walk-though order by creating data center grids to be assigned to systems and devices. Each data center grid represents a physical location (such as a grid tile) and has a unique walk-through order key defining the order in which operators proceed during premount jobs.

  You can add or edit grids:

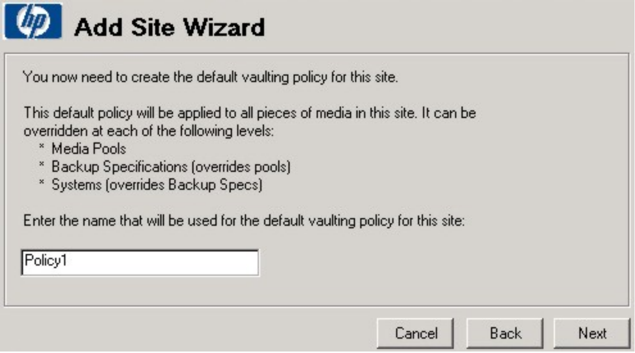
  - When adding or editing a data center

- When adding or editing a site definition (see "Bulk configuration file import" on page 152)

Adding a new site

You can add sites from **Global Configuration Options -> Site Management** provided you have top-level administrator permissions. If you have no sites configured, you are automatically taken to **Add Site Wizard** when you log in:

1. Type a site name, site address, and primary contact. Click **Next** to proceed.
2. Enter a name for the default vaulting policy to be applied to all media in the site.



Add Site Wizard

You now need to create the default vaulting policy for this site.

This default policy will be applied to all pieces of media in this site. It can be overridden at each of the following levels:
 * Media Pools
 * Backup Specifications (overrides pools)
 * Systems (overrides Backup Specs)

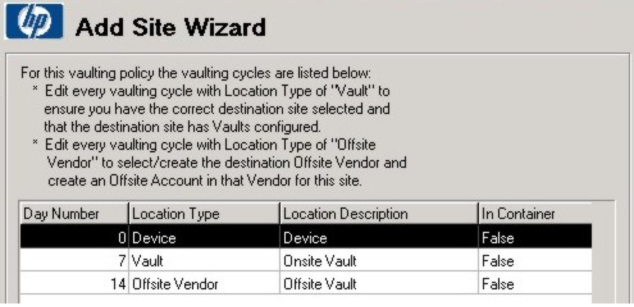
Enter the name that will be used for the default vaulting policy for this site:

Policy1

Figure 7 Creating default vaulting policy

3. Specify a vaulting policy for the new site. Select a policy template from the drop-down list or click **Add Template** to define your own policy.

4. Edit the vaulting cycles as instructed to ensure you have the correct destination site selected and the destination site has vaults configured.



Add Site Wizard

For this vaulting policy the vaulting cycles are listed below:
* Edit every vaulting cycle with Location Type of "Vault" to ensure you have the correct destination site selected and that the destination site has Vaults configured.
* Edit every vaulting cycle with Location Type of "Offsite Vendor" to select/create the destination Offsite Vendor and create an Offsite Account in that Vendor for this site.

Day Number	Location Type	Location Description	In Container
0	Device	Device	False
7	Vault	Onsite Vault	False
14	Offsite Vendor	Offsite Vault	False

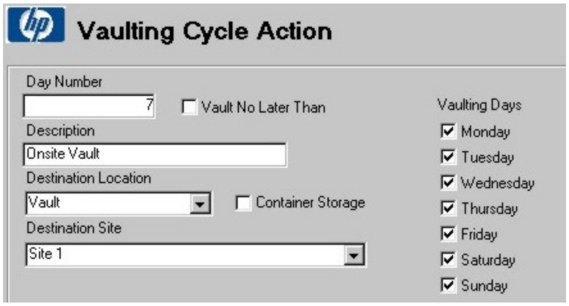
Figure 8 Vaulting cycle

To edit the location type and location destination, double-click **Location Type** or **Location Destination**, or click **Edit**.

NOTE:

Clicking **Next** without editing vaulting cycles produces an alert message. To proceed, edit the vaulting cycle referred to in the alert by either double-clicking the cycle, or selecting it and clicking **Edit**.

5. Type the day number. Select the destination location and the destination site. To select the days for the cycle to occur, select the appropriate **Vaulting Days** check boxes.



Vaulting Cycle Action

Day Number: 7

□ Vault No Later Than

Description: Onsite Vault

Destination Location: Vault

□ Container Storage

Destination Site: Site 1

Vaulting Days
- ☑ Monday
- ☑ Tuesday
- ☑ Wednesday
- ☑ Thursday
- ☑ Friday
- ☑ Saturday
- ☑ Sunday

Figure 9 Vaulting cycle action

6. If the vaulting cycle has an offline vendor destination, select an offsite vendor and an offsite vendor account. As you are adding a new site, there are no offsite vendors defined. Click **Add Offsite Vendor**.

7. In the **Offsite Storage Vendor Definition** page, specify the vendor name and type, and enter the vendor description. See "Site management" on page 39 for information about vendor types.

   Click **Add** to create accounts in the new offsite vendor. You are taken to **Vendor Account Definition**.

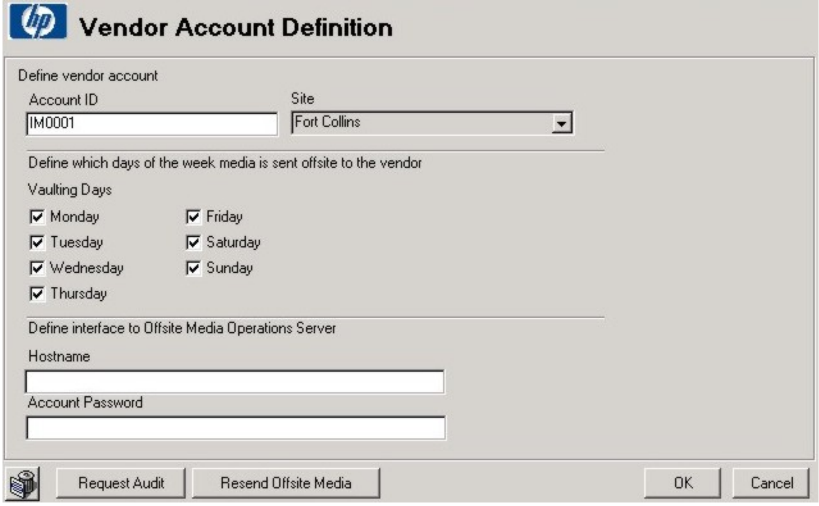
8. Which **Vendor Account Definition** window is displayed depends on the offsite vendor type you have selected:

- **Media Operations Vendor**

  Enter:

  - Unique vendor account ID
  - Hostname of the system on which the offsite Media Operations system resides
  - Password

  Account ID and password must match a remote account on the offsite Media Operations Server.



Vendor Account Definition

Define vendor account

Account ID: IM0001

Site: Fort Collins

Define which days of the week media is sent offsite to the vendor

Vaulting Days

☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday
☑ Sunday

Define interface to Offsite Media Operations Server

Hostname:

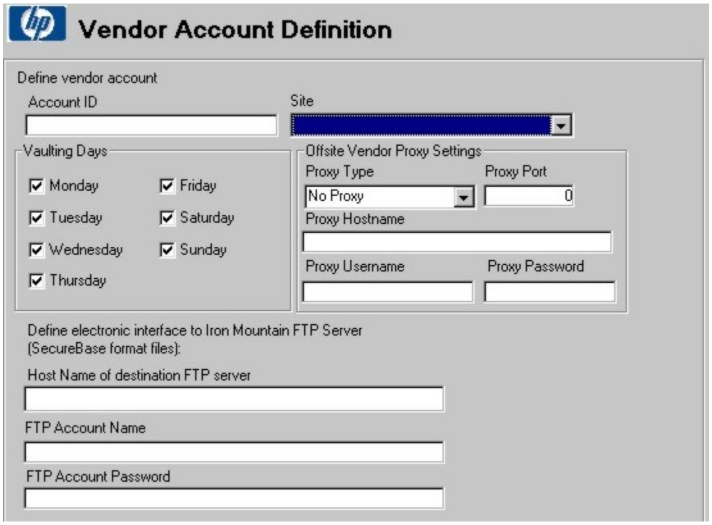
Account Password:

Figure 10 Vendor account definition - Media Operations vendor

- **Iron Mountain Vendor**

  Enter:

  - Account ID
  - Hostname defining the system name of the Iron Mountain Server used to store the offsite media
  - FTP account name
  - FTP password
  - If the connection to your offsite Iron Mountain Server passes through a firewall, type the proxy settings for this connection.



Vendor Account Definition

Define vendor account

Account ID

Site

Vaulting Days

☑ Monday ☑ Friday

☑ Tuesday ☑ Saturday

☑ Wednesday ☑ Sunday

☑ Thursday

Offsite Vendor Proxy Settings

Proxy Type: No Proxy

Proxy Port: 0

Proxy Hostname

Proxy Username

Proxy Password

Define electronic interface to Iron Mountain FTP Server
(SecureBase format files):

Host Name of destination FTP server

FTP Account Name

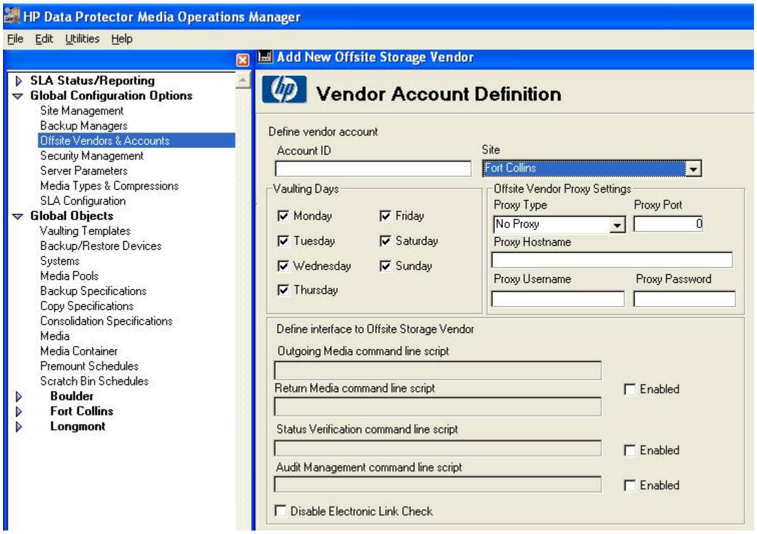
FTP Account Password

Figure 11 Vendor account definition—Iron Mountain vendor

- **Generic Vendor**

  Enter:

  - Unique account ID
  - If the offsite vendor has the proprietary electronic link interface, specify optional configuration settings



Vendor Account Definition

Define vendor account

Account ID:

Site: Fort Collins

Vaulting Days

☑ Monday ☑ Friday

☑ Tuesday ☑ Saturday

☑ Wednesday ☑ Sunday

☑ Thursday

Offsite Vendor Proxy Settings

Proxy Type: No Proxy

Proxy Port: 0

Proxy Hostname:

Proxy Username:

Proxy Password:

Define interface to Offsite Storage Vendor

Outgoing Media command line script:

Return Media command line script:

□ Enabled

Status Verification command line script:

□ Enabled

Audit Management command line script:

□ Enabled

□ Disable Electronic Link Check

Figure 12 Vendor account definition—generic vendor

When configuring offsite accounts for a Generic vendor, you can create scripts to take the information from Media Operations and convert it to the offsite vendors electronic link protocol.

- Select the **Enabled** check box for **Outgoing/Return Media command line script** if the vendor supports an interface to manage outgoing and returning media. Type the script/utility command to link Media Operations to the vendor.
- Select the **Enabled** check box for **Status Verification command line script** if the vendor supports an interface to notify that previously submitted outgoing and returning media jobs are complete. Type the script/utility command to link Media Operations to the vendor.
- Select the **Enabled** check box for **Audit Management command line script** if the vendor supports an interface to audit stored media. Type the script/utility command to link Media Operations to the vendor.
- Use **Vaulting Days** check boxes to define the days 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 53).

When you have configured your offsite vendor account, click **OK**to return to the **Offsite Storage Vendor Definition** window. Click **OK** to save the new offsite vendor and its accounts and return to **Vaulting Cycle Action**.

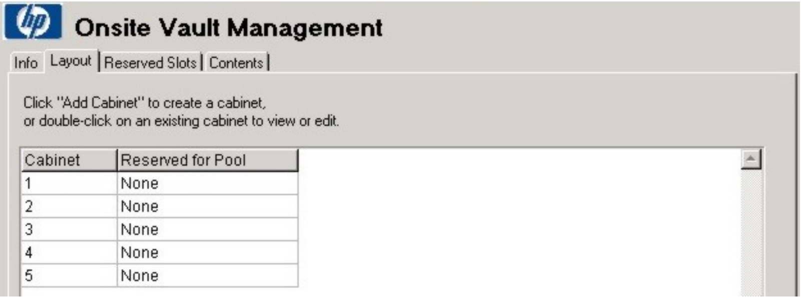
9. Specify the destination offsite vendor and its account. Click **OK** to save the vaulting policy cycle. You are now back to **Vaulting Cycle**.

NOTE:

If you click **Next** without editing the vaulting cycles, you receive an alert message. To proceed, edit the vaulting cycle referred to in the alert by either double-clicking that cycle, or selecting the cycle and clicking **Edit**.

10. Click **Add Vault** to create vault capacity in the destination site. If your destination is another site, select the correct destination site.

11. In the **Onsite Vault Management** window (the**Info** tab), type a vault name as well as other required information. Click the **Layout** tab to define the vault configuration and capacity.



Click "Add Cabinet" to create a cabinet,
or double-click on an existing cabinet to view or edit.

Cabinet	Reserved for Pool
1	None
2	None
3	None
4	None
5	None

Figure 13 Onsite vault management—layout

Adding cabinets You now need to create cabinets manually by clicking **Add Cabinets** or automatically by clicking **Auto-Create Layout**.

To create a cabinet manually:

1. In the **Create Cabinets** page, enter a unique cabinet name, and click **Add Drawers** or **Auto-Create Drawers**.
2. To add drawers manually, type the name of the first drawer, and click **Add Rows**.
3. In the **Create Rows** page, type the name of the first row in the drawer, starting and ending slot numbers, and specify the number and type of media.

   Repeat until all rows are created, then click **Cancel** to return to the **Create Drawers** window. Create all the new drawers you need, and then click **Cancel** to return to **Create Cabinets**. Create all the cabinets you need for that vault, and then click **Cancel** to return to **Onsite Vault Management**.

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

Click the **Contents** tab for a list of the media storage locations contained in the onsite vault and a list of media contained in those vault slots.

12. When you have configured your vault, click **OK** to save the new vault and return to **Vaulting Cycle Action**.

    Click **OK** to save the vaulting policy cycle. You are now back to **Vaulting Cycle**.

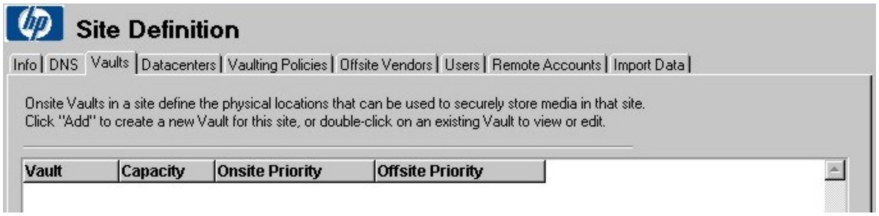
    Click **Finish**to save your new site configuration.

Editing an existing site

When you have added a site, you can modify the physical layout of its devices and the available onsite and offsite vault locations from:

- **Global Configuration Options -> Site Management** (top-level administrators)
- **Global Configuration Options -> Server Parameters** under the `Sites` tab (top-level administrators)
- The **Site Configuration** option under each site in the shortcut bar (top-level and site-level administrators)

To update an existing site, change its properties under the appropriate tab in the **Site Definition** window.



Onsite Vaults in a site define the physical locations that can be used to securely store media in that site.
Click "Add" to create a new Vault for this site, or double-click on an existing Vault to view or edit.

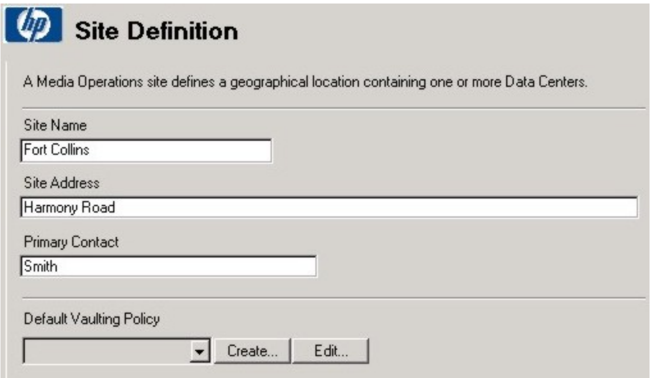
Vault	Capacity	Onsite Priority	Offsite Priority

Figure 14 Site properties

Site properties are described in detail below.

Info

The **Info** tab shows the geographical location containing data centers for a site. Each site has a unique site name and default vaulting policy. It has at least one default data center, but you can define additional data centers and onsite vaults.



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

Default Vaulting Policy

Figure 15 Site definition—info

NOTE:

If you exit this screen without defining a vaulting policy, you receive an alert message.

When you click **Create**, you need to:

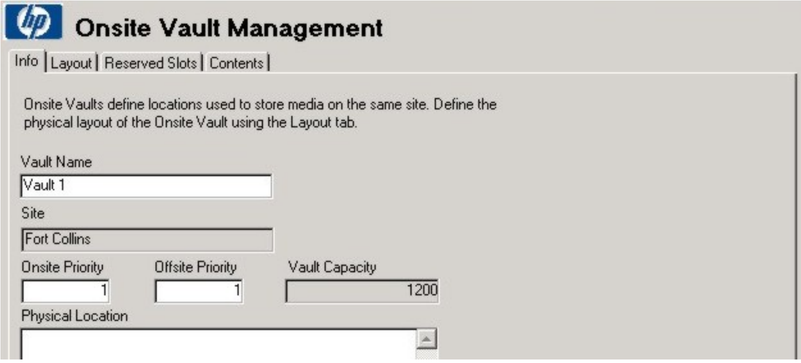
- type the name of the vaulting policy,
- select a template to use,
- type site-specific vaulting location information (for example, if you have a vaulting cycle implementation with an offsite vendor destination),
- select the offsite vendor and the offsite vendor account.

DNS

The **DNS** tab allows you to associate the site with a set of DNS suffixes (such as `*.fc.hp.com`). The system objects added to the Media Operations configuration are automatically assigned to the appropriate sites based on their DNS name. Click **Edit** to view or edit an existing DNS suffix, or **Add** to create a new one.

Vaults

The **Vaults** tab defines the onsite vaults in the site. To view or edit a vault, double-click it. To add a new vault, click **Add** or **Add Many**. The **Add New Onsite Vault** wizard is displayed.



Onsite Vaults define locations used to store media on the same site. Define the physical layout of the Onsite Vault using the Layout tab.

Vault Name: Vault 1

Site: Fort Collins

Onsite Priority: 1

Offsite Priority: 1

Vault Capacity: 1200

Physical Location:

Figure 16 Onsite vault management—info

1. Under the **Info** tab of the **Add New Onsite Vault** wizard, enter the vault name, as well as other required information.
2. Under the **Layout** tab, define the vault configuration and capacity. You can add cabinets manually by clicking **Add Cabinets**, or automatically by clicking **Auto-Create Layout**. For instructions, see step 11 in "Adding a new site" on page 42.

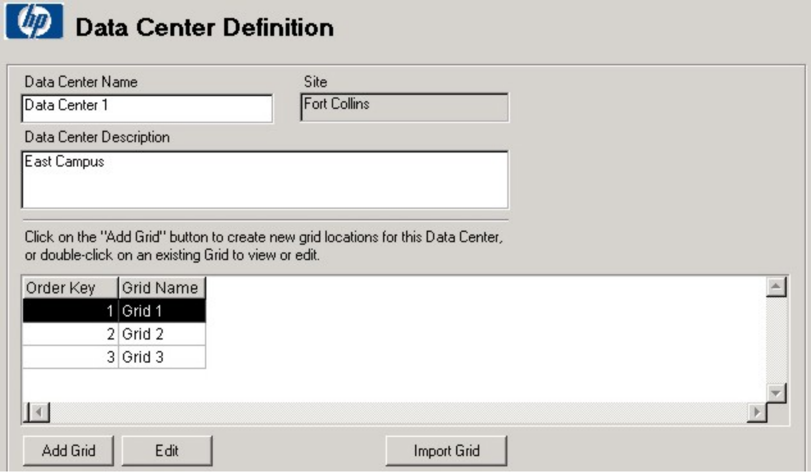
The **Reserved Slots** tab displays a list of all slots reserved for single media pools (as opposed to general slots).

The **Contents** tab displays a list of all media storage locations contained in the onsite vault together with the media belonging to those vault slots.

Data centers

The **Data Centers** tab defines the physical grouping of backup/restore devices and systems. To add new data centers, click **Add** or **Add Many**, and follow these steps:

1. Type a unique name for the data center and its description.



Data Center Definition

Data Center Name: Data Center 1

Site: Fort Collins

Data Center Description: East Campus

Click on the "Add Grid" button to create new grid locations for this Data Center, or double-click on an existing Grid to view or edit.

Order Key	Grid Name
1	Grid 1
2	Grid 2
3	Grid 3

Figure 17 Data center definition

Data center grids define the data center physical layout and the grid walk-through order. You can assign locations to systems and devices in that data center to optimize the walk-through order of devices during premount jobs.

In addition, you can add grids manually, or import a grid definition file. See "Import data" on page 58 for import instructions.

2. Enter the grid name and the order key for 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.

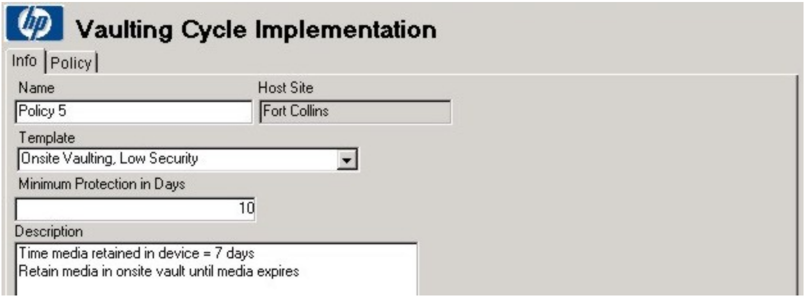
   After you have finished adding grids, click **Cancel** to exit. Click **Cancel** again to return to **Site Definition**.

Vaulting policies

The **Vaulting Policies** window defines active vaulting policies used by objects in this site. You can create your own vaulting policy, or use one of the pre-defined templates. See "Vaulting templates" on page 81 for templates' description.

To view or edit a defined vaulting policy, double-click it or click **Edit**. To add a new vaulting policy, click **Add** or **Add Many**, and follow this procedure:

1. Enter a name for a new vaulting policy. Select a template, and type the minimum number of protection days.



Vaulting Cycle Implementation

Name: Policy 5

Host Site: Fort Collins

Template: Onsite Vaulting, Low Security

Minimum Protection in Days: 10

Description:
Time media retained in device = 7 days
Retain media in onsite vault until media expires

Figure 18 Vaulting cycle implementation—info

2. Click the **Policy** tab. Click **Add** to add a new or **Edit** to edit an existing vaulting cycle.

3. Type the day number. Select the destination location and the destination site. To specify the days for the cycle to occur, select the appropriate **Vaulting Days** check boxes.

   Click **OK** to return to the previous window, then click **OK** to return to **Site Definition**.

Offsite vendors

The **Offsite Storage Vendor Definition** window defines locations used to store the media offsite.

1. Enter a unique vendor name to define a vendor location. The offsite vendor type can be Media Operations, Iron Mountain, or Generic. The **Contact Details** field is used to enter unique information about that vendor.

NOTE:

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

2. Use **Vaulting Days** check boxes to define the days 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 53).

   Then, depending on the vendor type you selected, proceed as follows:

   Media Operations Vendor

   Enter:

   - Unique vendor account ID
   - Hostname of the system on which the offsite Media Operations system resides
   - The password

   Account ID and password must match a remote account on the offsite Media Operations Server.

   Iron Mountain Vendor

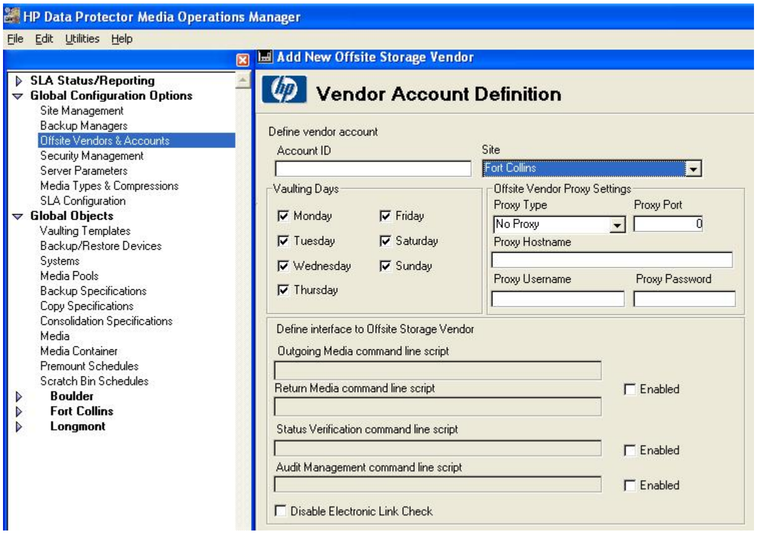
   Enter:

   - Account ID
   - Hostname defining the system name of the Iron Mountain Server used to store the offsite media
   - FTP account name
   - FTP password
   - If the connection to your offsite Iron Mountain Server passes through a firewall, type the proxy settings for this connection.

   Use the media link **Filename Format** if you need to provide FTP files to Iron Mountain using the old MediaLink file name format. FTP contents are always in SecureBase format, so this only affects the file name.

   Generic Vendor

   Enter a unique account ID. If the offsite vendor has the proprietary electronic link interface, specify optional configuration settings.



Vendor Account Definition

Define vendor account

Account ID:

Site: Fort Collins

Vaulting Days

☑ Monday ☑ Friday
☑ Tuesday ☑ Saturday
☑ Wednesday ☑ Sunday
☑ Thursday

Offsite Vendor Proxy Settings

Proxy Type: No Proxy
Proxy Port: 0
Proxy Hostname:
Proxy Username:
Proxy Password:

Define interface to Offsite Storage Vendor

Outgoing Media command line script:

Return Media command line script: ☐ Enabled

Status Verification command line script: ☐ Enabled

Audit Management command line script: ☐ Enabled

☐ Disable Electronic Link Check

Figure 19 Vendor account definition—generic vendor

When configuring offsite accounts for a Generic vendor type, you can create scripts to take information from Media Operations and convert it to the offsite vendors electronic link protocol.

- Select the **Enabled** check box for **Outgoing/Return Media command line script** if the vendor supports an interface to manage outgoing and returning media. Type the script/utility command to link Media Operations to the vendor.
- Select the **Enabled** check box for **Status Verification command line script** if the vendor supports an interface to notify when previously submitted outgoing and returning media jobs are complete. Type the script/utility command to link Media Operations to the vendor.
- Select the **Enabled** check box for **Audit Management command line script** if the vendor supports an interface to audit stored media. Type the script/utility command to link Media Operations to the vendor.
- Select **Disable Electronic Link Check** to disable the check for an electronic link interface to the offsite vendor account.

3. Click **OK** to complete the operation and return to **Offsite Storage Vendor Definition**. Click **OK** when you finished adding offsite vendors to return to **Site Definition**.

Users

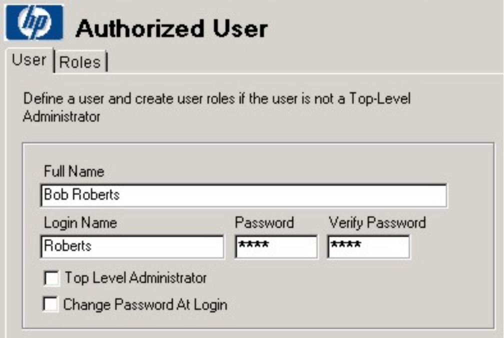
The **Users** window defines site-level users. Top-level administrators are not listed as they have full access to every site.

To edit or view an existing user, click **Edit**. To add a new user, click **Add** and perform these steps:

1. Type the username, login name, and password for the new user. Select the **Change Password at Logon** check box if you want the user to change the password at the first logon.

NOTE:

The password has a maximum length of 10 characters.



Authorized User

Define a user and create user roles if the user is not a Top-Level Administrator

Full Name: Bob Roberts

Login Name: Roberts

Password: ****

Verify Password: ****

□ Top Level Administrator

□ Change Password At Login

Figure 20 Adding a user

Select the **Top Level Administrator** check box if the new user will be a top-level administrator.

2. If the new user will not be a top-level administrator, assign a role for this user by first clicking the **Roles** tab, and then clicking **Add**.

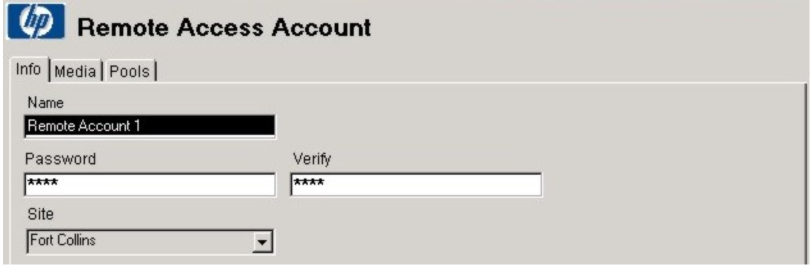
   After you have finished, click **Cancel** to return to the **Authorized User** window, and then **OK** to return to **Site Definition**.

For more information about users, refer to "Security management" on page 59.

Remote accounts

The **Remote Accounts** window defines accounts used by other Media Operations Servers that can store the media in this site. These accounts must match the vendor account records on remote Server.

To view or edit an existing account, double-click it or click **Edit**. To add a new remote account, click **Add** or **Add Many**. Type the remote account name and the password, then verify the password.



Remote Access Account

Name: Remote Account 1

Password: ****

Verify: ****

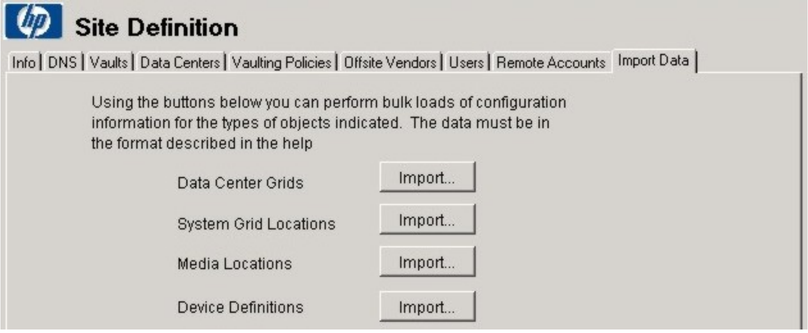
Site: Fort Collins

Figure 21 Remote access account—info

After finishing, click **OK** to return to **Site Definition**.

Import data

The **Import Data** window allows you to perform bulk loads of configuration information for data center grids, system grid locations, media locations, device definitions, and manual media.



Site Definition

Using the buttons below you can perform bulk loads of configuration information for the types of objects indicated. The data must be in the format described in the help

Figure 22 Site definition—import data

For field values for importing different information types, and for importing examples, see "Bulk configuration file import" on page 152.

Deleting a site

If you delete a site, you also delete vaults, offsite vendor accounts, data centers, and site-level user roles associated with that site. Any manually added backup objects created within the site are deleted as well. Any backup objects automatically created within the site by a Backup Manager specific to the site are either moved to another site (if you specify one) or the Backup Manager is deleted with the site. If the Backup Manager is not specific to the site (spread across multiple sites), its objects are moved to another Backup Manager site.

When deleting a site, consider the following:

- You cannot delete a site unless you delete or move Backup Managers that use the site (for example, Backup Managers that have the site as their home site).
- Sites that contain remote devices or systems (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.
- Manually created objects are deleted when the site is deleted. You receive a warning before the deletion, so you can manually move manual pools, devices, systems, backup specifications via **Global Object Lists**.

NOTE:

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

Security management

Security management is based on user roles. There are two basic types of users:

- Product administrators and operators
- Remote accounts

You can access users from:

- **Global Configuration Options -> Security Management** or **Users**/**Remote Accounts** tabs from **Global Configurations Options -> Server Parameters**. From these windows, you can view or create top-level administrators. You can also edit the initial top-level administrator defined during the installation.

- The **Users**/**Remote Accounts** tabs of the **Site Configuration** window give you site-level access to users for the current site. You cannot view or add top-level administrators from these tabs.

Product administrators and operators

NOTE:

A single user cannot have multiple roles for the same site but can have multiple roles for different sites.

Product administrators include:

- Top-level administrators, who have permissions to:
  - perform any operation for any site,
  - access **Global Configuration Options** and **Global Objects** and make additions, modifications, and deletions,
  - create other top-level administrators,
  - map unassigned devices to a site in a multi-site Backup Server configuration.

NOTE:

There must be at least one top-level administrator for a site.

- Site-level administrators, who have permissions to:
  - perform site-level operations for a particular site,
  - assign site-level, super operator-level, and operator-level administrator roles for new/existing Media Operations users.
- Super operator-level administrators, who have permissions to perform site-level daily Media Operations. These include:
  - premount, vaulting, scratch bin maintenance, checkout request, exception list, and mount request functions,
  - modifying media-level vaulting policies,
  - overriding media locations,
  - manually adding new media into manual media pools,

- reassigning systems/devices between data centers in the same site.

  Super operator-level administrators have read-only access to some site-level information but not to site-specific configuration options.

- Operator-level administrators, who can:
  - perform site-level daily operations, including premount jobs, vaulting jobs, scratch bin maintenance, checkout requests, exception list actions, and mount requests,
  - have read-only access to some site-level information.

  Operator-level administrators do not have access to site-specific configuration options.

Remote accounts

Remote accounts are users set up to give secure access to the current Media Operations Server from another Media Operations Server. Another Media Operations Server can link to this server electronically using the current server as an offsite vendor.

An offsite vendor account (configured with the name of the current Media Operations Server, account ID, and password) on another server must match 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 retrieve previously stored media) received by this server are secure.

When creating the remote account, define the site to be used to store the media from another 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 will be KLAXON-LTO. This allows you to audit media you are currently storing.

You can view media pools information from global or site level for the site associated with that account, or from **Media**/**Pools** tabs on the **Remote Accounts** window.

Configuring backup processes and objects

Media Operations deals with media lifecycle components (media, media pools, backup specifications, devices, and systems) either controlled and automatically created by Backup Managers, or media existing outside the Backup Manager.

Automatic backup

Automatic backup processes and objects are configured through integration with supported Backup Managers. Automatic copy processes (such as scheduled copy jobs) and objects are configured through integration with those Backup Managers that support copy operation.

NOTE:

Currently, the XML Gateway supports copy operations available on HP Data Protector A.06.00, A.06.10, A.06.11, and A.06.20, and the Inline copy feature of Symantec NetBackup 6.0.

There are two ways of integrating with Backup Managers:

- Through XML Gateway, linking Media Operations directly with a supported Backup Manager. This interface provides fast response time and does not require any complex communication path setup. It runs over a standard HTTPS connection, which normally passes through firewalls without any special configuration. XML Gateway passes requests to Backup Managers and receives responses from them. This allows it to initiate device actions (such as device scans, media initialization, library load/eject of media) through the Backup Manager.

  XML Gateway requires no configuration because Media Operations specifies the Backup Manager to connect to and all required security parameters.

  If XML Gateway supports remote connectivity, you can install it directly on the Backup Manager, on the Media Operations Server, or on another server.

  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).

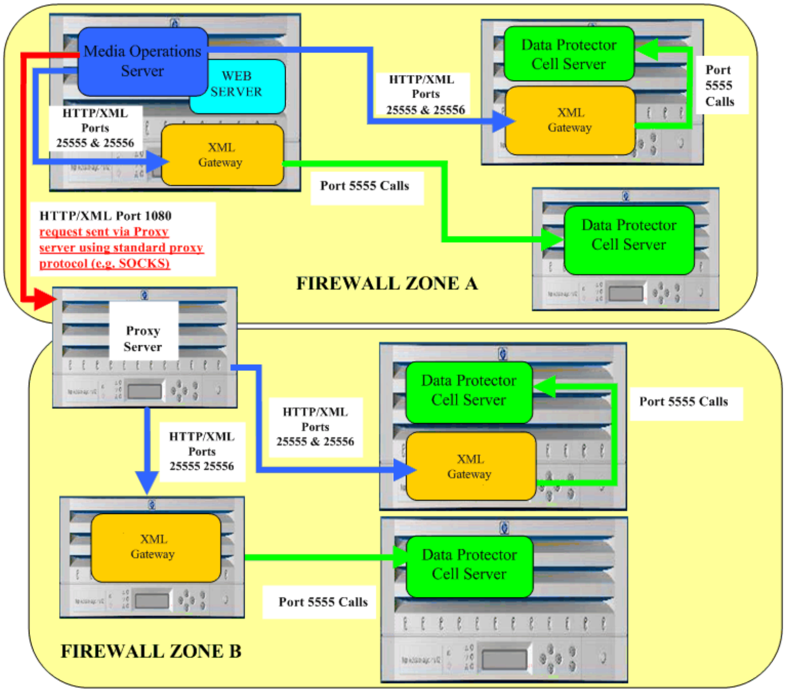

Media Operations Server
WEB SERVER
HTTP/XML Ports 25555 & 25556
XML Gateway
HTTP/XML Ports 25555 & 25556
Data Protector Cell Server
XML Gateway
Port 5555 Calls
Port 5555 Calls
Data Protector Cell Server
HTTP/XML Port 1080
request sent via Proxy server using standard proxy protocol (e.g. SOCKS)
FIREWALL ZONE A
Proxy Server
HTTP/XML Ports 25555 25556
HTTP/XML Ports 25555 & 25556
Data Protector Cell Server
XML Gateway
Port 5555 Calls
XML Gateway
Port 5555 Calls
Data Protector Cell Server
FIREWALL ZONE B

Figure 23 Media Operations deployment options with Data Protector

NOTE:

Communication between XML Gateway and Data Protector does not normally pass through firewalls, so XML Gateway running on the Media Operations Server or another server can only communicate with a Backup Manager within the same firewall zone. If XML Gateway and Data Protector Cell Manager are behind a firewall, Media Operations Server must communicate with XML Gateway by passing requests to XML Gateway via a Proxy Server (such as SOCKS).

NOTE:

Symantec NetBackup master server commands must be executed locally on the master system. Therefore, XML Gateway must be installed on the Symantec NetBackup master server system.

- Through the XML file import interface, allowing integration with other types of Backup Servers not supported by XML Gateway.

  This file-import interface uses files formatted in HTTP/XML protocol, such as:

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

  See “External interfaces” on page 141 for details.

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 backup

You model the manual backup environment separately for each system (or its part, such as directory or volume), so each has its own manually created backup specification.

The manual backup flow consists of the following:

1. Create media resources:

   a. Create a media pool using **Global Objects -> Media Pools** (top-level administrators) or the site-level **Media Pools** list (site-level administrators). Specify media characteristics of the pool: media type (such as LTO), media compression type (such as LTO-1), and, optionally, barcode labelling policy.

   b. Create media within the pool from the **Media** tab of the **Media Pools Add/Edit** window. Created media acquire characteristics of their parent media pool.

2. Configure a backup:

   a. Create the system (if the system has not been created by a Backup Manager) using **Global Objects -> Systems** (top-level administrators) or the site-level **Systems** list (site-level administrators). Specify characteristics of the system, such as data center and grid location (in the site to which the system is assigned).

   b. Create devices (if the devices have not been created by a Backup Manager) from **Global Objects -> Backup\Restore Devices** (top-level administrators) or the site-level **Backup\Restore Devices** list (site-level administrators).

      Specify device properties, 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.

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

   c. Create a backup specification specifying the system, drives and media pools, as well as media retention/protection period from **Global Objects -> Backup Specifications** (top-level administrators) or the site-level **Backup Specifications** list (site-level administrators).

      When creating the backup specification from the site level, ensure the drives associated with the specification are in the same site as the specification. When creating the backup specification from the global level, the specification site is set based on the first drive associated with the specification. All drives thereafter must be from the same site. Pools associated with the drives must be manual pools matching the drive media type and located in the same site.

Implementing the backup process

A medium goes from being scratch to being used for backup. There are two ways of managing this part of the manual media lifecycle:

- When editing manual media, click **Mark as Used** to specify date of use and the relevant backup specification, and **Mark as Scratch** to force a used manual medium to return to scratch status. This is done under the **Vaulting** tab on the Media window.
- Use the `Reactive Mount` command-line utility to create a reactive mount job for a manual backup specification. When you mark the job as complete, selected media are marked as used.

NOTE:

Manual backup specifications are not supported by scheduled premount jobs.

Backup managers

Backup Managers control backup functions. Media Operations interacts with them to track and provide media use in two ways:

- Via XML Gateway (available for supported Backup Managers)
- Via XML file import (Backup Manager type "Other")

NOTE:

When adding a Data Protector backup manager that has secure communication enabled, keep the following points in mind:

- The XML Gateway should *not* be installed on the Cell Manager system that has secure communication enabled.
- The XML Gateway system should be added to the exception list on the Data Protector Cell Manager system that has secure communication enabled.

XML Gateway interface

Install XML Gateways before you configure Backup Manager. Consider your environment carefully before deploying XML Gateway. See Figure 23 on page 63 for a representation of deployment options. XML Gateway can be installed on a variety of server platforms, such as Windows, HP-UX, Linux, or Solaris.

For optimal Media Operations performance, install XML Gateway on each Backup Manager System. If this causes Backup Manager performance issues, put XML Gateway on other, preferably dedicated, servers. In this configuration, you can group XML Gateways allowing Media Operations to dynamically balance the request load and failover transparently to a working XML Gateway should an XML Gateway fail. The failed XML Gateway is re-integrated in the group when it returns online.

Also, you can install XML Gateway on the Media Operations Server. 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 Data Protector Manager-of-Managers (MoM) configuration and you add a Backup Manager Server that is part of MoM, the Backup Manager and all systems in its corresponding Media Management Database (MMDB) cluster are added automatically. See "Manager-of-Managers configuration" on page 162 for more information.

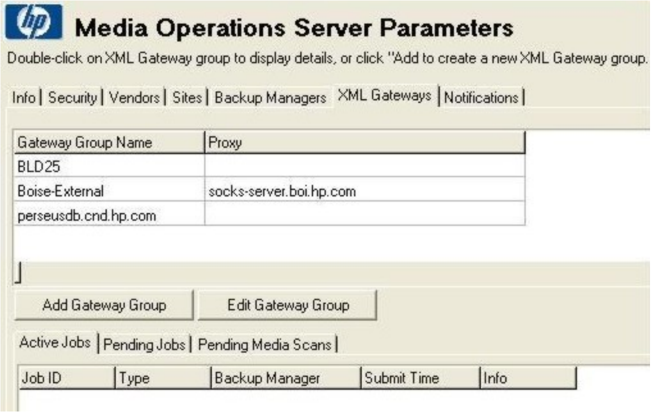
Monitoring XML Gateway

When you add a Backup Manager, a baseline synchronization runs, during which any communications problems between XML Gateway and the Backup Manager are noted on screen and/or in the log.

NOTE:

Errors occurring while parsing the XML received from XML Gateway are written to alert logs. See "Viewing alerts" on page 126 for more information.

- To test synchronization or force an update, click **Manually Synchronize** under the **Polling** tab on the **Backup Manager** window.
- To view a list of all previous communications from the Backup Server to XML Gateway, click History. This shows whether the request from the Media Operations Server has reached successfully. Use this to diagnose communications problems between Media Operations Server and its XML Gateways.
- To monitor the XML Gateway job queue, click the **XML Gateways** tab on the **Server Parameters** window. You can view active and pending jobs and cancel pending jobs if needed.



Media Operations Server Parameters

Double-click on XML Gateway group to display details, or click "Add to create a new XML Gateway group.

Gateway Group Name	Proxy
BLD25	
Boise-External	socks-server.boi.hp.com
perseusdb.cnd.hp.com	

Job ID	Type	Backup Manager	Submit Time	Info

Figure 24 Server parameters - XML Gateways

XML Gateway groups

If XML Gateway is installed elsewhere than on the Backup Manager, configure XML Gateway groups. Create or edit XML Gateway groups from the **Info** tab on the **Add/Edit Backup Manager** window or the **XML Gateways** tab on **Global Parameters -> Server Parameters**.

NOTE:

Add several XML Gateways to a group to activate load balancing and failover.

Media Operations can communicate with the XML Gateway group using proxy settings defined for that group. Backup Manager, its XML Gateway, and the Media Operations Server can then be in different networks separated by a firewall.

Media Operations supports the following proxy types:

- SOCKS4 basic
- SOCKS4 with username/password
- SOCKS5 with username/password

These proxy parameters are used for all communications to the XML Gateway group.

TIP:

If you install XML Gateway on the Backup Manager and select **Use Backup Manager as XML Gateway**, you need not create an XML Gateway group. However, an XML Gateway group is required to support a proxy connection from the Media Operations Server to XML Gateway.

Polling schedule

The polling schedule defines when configuration information needs to be extracted from the Backup Manager through configured XML Gateways. You can create or edit a polling schedule from the **Polling** tab on the **Add/Edit Backup Manager** window if you have XML Gateway selected as the interface type.

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

Media Operations polls for four reports:

- Configuration Report containing the Backup Manager, media pools, devices, and backup specific information. There must be at least one configuration report defined in the Backup Server polling schedule.
- Device Scan scanning the media contents of *all* devices on the Backup Server. It performs library barcode scans for every barcode-capable tape library on the Backup Server and media scans on all standalone tape drives, library slots (except cleaning slots) in non-barcode capable libraries, and slots containing “blank” or “unknown” media in barcode-enabled libraries. Run this scan:
    - before the premount calculation process starts (see the **Info** tab on the **Global Configuration -> Server Parameters** window for this time), so it can accurately determine the required scratch media and what media to unload,
    - after premount jobs have finished, so that Backup Manager is aware of new scratch media.
- Full Media Information, listing all media in a Cell Manager. At least one full media information event must be defined in the Backup Server polling schedule.
- Incremental Media Information, listing all media in a Cell Manager used since the last full or incremental media information event. This report includes usage information on backup specifications that used the media. It allows 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 for setting a unique directory on the Data Protector Server. This directory is used for the XML File Import interface for the specified Backup Server. Data Protector monitors this directory for any new incoming files and imports each new file. It automatically updates the Data Protector Database using information in the file.

To change the polling frequency, go to **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 incoming files does not match the defined Backup Server name for that file-passing directory, the incoming file is ignored.

Errors occurring while parsing the XML are written to alert logs. See "Viewing alerts" on page 126 for details.

Adding backup managers

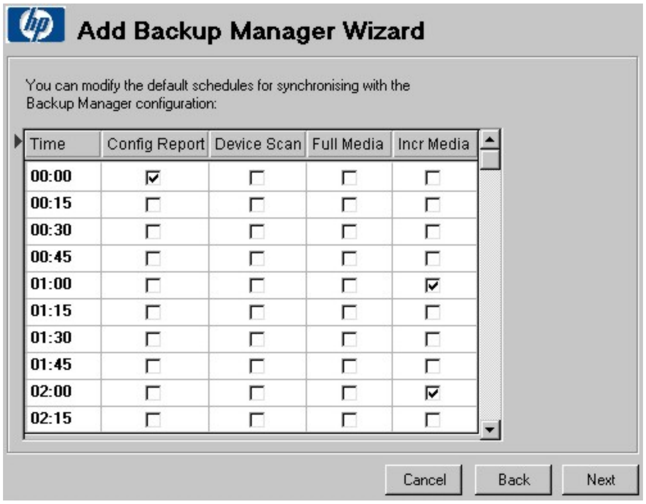
Launch **Add Backup Manager Wizard** from either the **Add Site Wizard** window or **Global Configuration Options -> Backup Managers**, and proceed as follows:

1. Select the Backup Manager type.
2. Type the network name of the Backup Manager system. If this is different from the primary network name of its host system (for example, if the host system has multiple network interfaces), select the host system primary network name from a list of current systems in Media Operations by clicking the **Backup Manager Host System** arrow.

   Select the operating system and locale of the backup manager.

   Click **Next**.
3. If you have more than one site configured, specify the home site for the Backup Manager. Otherwise, this step is skipped.
4. Specify security settings for connecting to the Backup Manager. You can also enter the port number if you changed the default value.

5. Set scheduling options by checking the appropriate boxes.



Add Backup Manager Wizard

You can modify the default schedules for synchronising with the Backup Manager configuration:

Time	Config Report	Device Scan	Full Media	Incr Media
00:00	☑	□	□	□
00:15	□	□	□	□
00:30	□	□	□	□
00:45	□	□	□	□
01:00	□	□	□	☑
01:15	□	□	□	□
01:30	□	□	□	□
01:45	□	□	□	□
02:00	□	□	□	☑
02:15	□	□	□	□

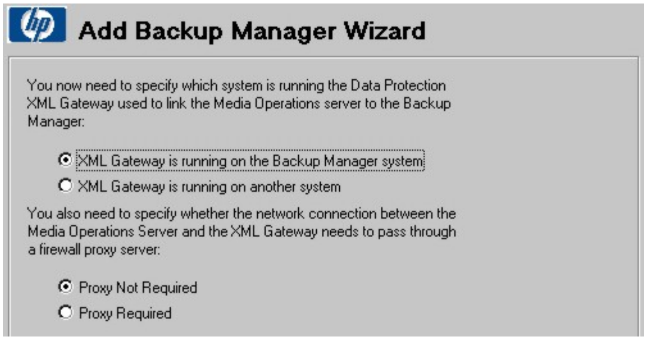
Figure 25 Setting scheduling options

Scheduled events keep Media Operations in sync with the Backup Manager:

- **Config Report** collects clients on the Backup Manager, MMDB configuration, media pools, devices, and backup specifications.
- **Device Scan** scans all devices to determine media loaded in them.
- **Full Media** retrieves all media from the Backup Manager.
- **Incr Media** retrieves all media modified in the past hour plus their usage information.

6. Check **Enable Location Updates** if you want requests to change a media location in Media Operations to be automatically copied back to the Backup Manager media location. Click **Next**.

7. Select a radio button to indicate whether you will create a new XML Gateway configuration or use an existing one.



Add Backup Manager Wizard

You now need to specify which system is running the Data Protection XML Gateway used to link the Media Operations server to the Backup Manager:

● XML Gateway is running on the Backup Manager system

○ XML Gateway is running on another system

You also need to specify whether the network connection between the Media Operations Server and the XML Gateway needs to pass through a firewall proxy server:

● Proxy Not Required

○ Proxy Required

Figure 26 XML Gateway

NOTE:

NetBackup gateway must always be present on the Master server. If you are using Data Protector Manager-of-Managers (MoM) configuration, the gateway must be present on the MoM server. See "Manager-of-Managers configuration" on page 162 for more information.

If a user is using HP Data Protector as the backup manager and it runs in a locale other than English, you must install the gateway on a system for which the default encoding is same as the backup manager system.

8. If you are creating a new XML Gateway configuration, type the full network name of the system the XML Gateway is running on. After clicking **Next**, you are taken to **Proxy Settings** (if you selected **Proxy Required**) or to **Save Backup Manager**.
9. Type details of the Proxy Server used to connect the Media Operations Server and XML Gateway. Click **Next**.
10. Click **Finish** to save the Backup Manager and perform the initial configuration. A window shows the configuration progress. When it completes, click **OK**.

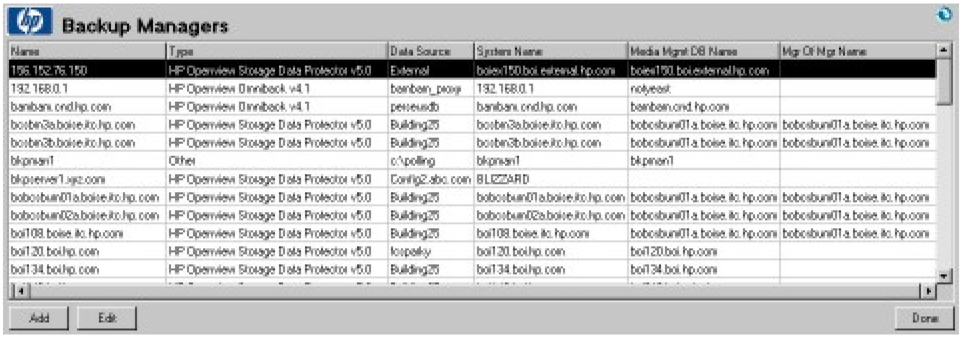
What's next?

You have successfully configured a site and added a Backup Manager to it. To tune the configuration further:

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

Editing a backup manager

To access a list of Backup Managers managed by the Storage Media Operations Server, click **Backup Managers** under **Global Configuration Options**.



Name	Type	Data Source	System Name	Media Mgmt DB Name	Mgr Of Mgr Name
156.152.76.150	HP Openview Storage Data Protector v5.0	External	boiex150.boi.external.hp.com	boiex150.boi.external.hp.com	
192.168.0.1	HP Openview Omniback v4.1	banban_proxy	192.168.0.1	notyeast	
banban.cnd.hp.com	HP Openview Omniback v4.1	perseusdb	banban.cnd.hp.com	banban.cnd.hp.com	
bosbin3a.boise.itc.hp.com	HP Openview Storage Data Protector v5.0	Building25	bosbin3a.boise.itc.hp.com	bobosbun01a.boise.itc.hp.com	bobosbun01a.boise.itc.hp.com
bosbin3b.boise.itc.hp.com	HP Openview Storage Data Protector v5.0	Building25	bosbin3b.boise.itc.hp.com	bobosbun01a.boise.itc.hp.com	bobosbun01a.boise.itc.hp.com
bkpman1	Other	c:\polling	bkpman1	bkpman1	
bkpserver1.xyz.com	HP Openview Storage Data Protector v5.0	Config2.abc.com	BLIZZARD		
bobosbun01a.boise.itc.hp.com	HP Openview Storage Data Protector v5.0	Building25	bobosbun01a.boise.itc.hp.com	bobosbun01a.boise.itc.hp.com	bobosbun01a.boise.itc.hp.com
bobosbun02a.boise.itc.hp.com	HP Openview Storage Data Protector v5.0	Building25	bobosbun02a.boise.itc.hp.com	bobosbun01a.boise.itc.hp.com	bobosbun01a.boise.itc.hp.com
boi108.boise.itc.hp.com	HP Openview Storage Data Protector v5.0	Building25	boi108.boise.itc.hp.com	bobosbun01a.boise.itc.hp.com	bobosbun01a.boise.itc.hp.com
boi120.boi.hp.com	HP Openview Storage Data Protector v5.0	loopsky	boi120.boi.hp.com	boi120.boi.hp.com	
boi134.boi.hp.com	HP Openview Storage Data Protector v5.0	Building25	boi134.boi.hp.com	boi134.boi.hp.com	

Figure 27 Backup managers

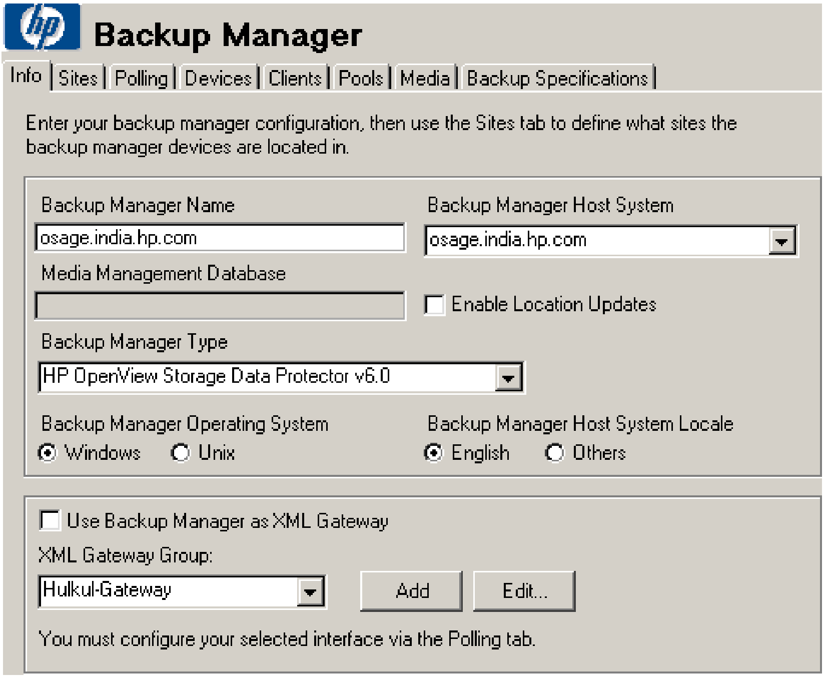
To view or edit an existing Backup Manager, double-click it or click **Edit**. Properties for the selected Backup Manager are displayed.

Info

The **Info** tab displays the Backup Manager configuration information.

Select the primary network name of the host system running the Backup Manager. If the Backup Manager does not appear in the drop-down list, either type it in the Backup Manager Name field and select **<Use Backup Manager Name>** in the drop-down list of host system, or add it manually under **Global Objects -> Systems**.

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



Backup Manager

Info | Sites | Polling | Devices | Clients | Pools | Media | Backup Specifications

Enter your backup manager configuration, then use the Sites tab to define what sites the backup manager devices are located in.

Backup Manager Name: osage.india.hp.com

Backup Manager Host System: osage.india.hp.com

Media Management Database:

□ Enable Location Updates

Backup Manager Type: HP OpenView Storage Data Protector v6.0

Backup Manager Operating System: ● Windows ○ Unix

Backup Manager Host System Locale: ● English ○ Others

□ Use Backup Manager as XML Gateway

XML Gateway Group: Hulkul-Gateway

You must configure your selected interface via the Polling tab.

Figure 28 Backup manager - info

If your Backup Manager is supported by XML Gateway, either install XML Gateway onto the tape Backup Manager system or use the XML Gateway group to communicate with the Backup Manager.

NOTE:

NetBackup gateway must always be present on the Master server.

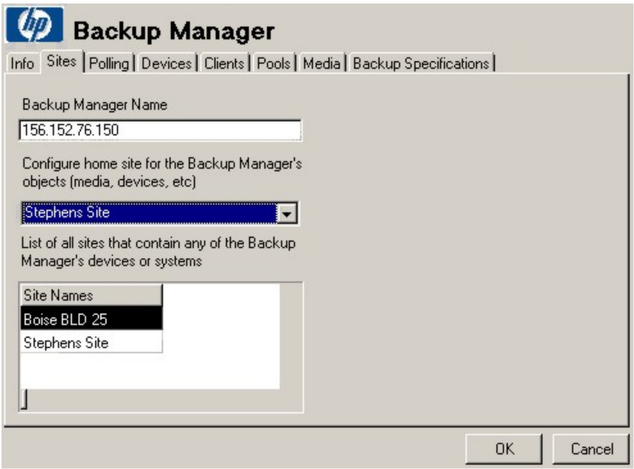
Click **Add** to add a new XML Gateway group. If the Cell Manager has the XMLGW installed but you will not use an XMLGW group, check the **Use Backup Manager as XML Gateway** box. The drop-down list and **Add** buttons are disabled.

Type the name of the XML Gateway group made up of one or more XML Gateways. Media Operations automatically load balances communications across all XML Gateways in the group. Enter proxy settings and then click **Add**.

Type the hostname and click **OK** to return to the **XML Gateway** window. Click **OK** to return to **Backup Manager - Info**.

Sites

The **Sites** tab shows the sites containing objects from a Backup Manager. Each Backup Manager has a home site where its media and pools are located and where its systems, devices, and backup specifications are placed by default if there is other appropriate site to locate them (if the sites have DNS suffixes defined). When a device or system associated with a Backup Manager is moved to another site, a list of used sites is shown on the **Backup Manager - Sites** window.



Backup Manager Name: 156.152.76.150

Configure home site for the Backup Manager's objects (media, devices, etc): Stephens Site

List of all sites that contain any of the Backup Manager's devices or systems

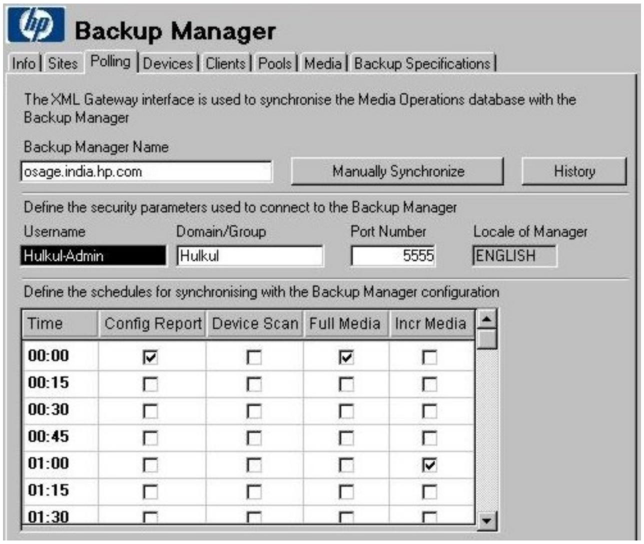
Site Names
Boise BLD 25
Stephens Site

Figure 29 Backup manager - sites

If you change the home site for a Backup Manager, all Backup Manager objects in the original home site are moved to the new site. Any vaulting policies (plus any associated offsite vendor accounts) and premount job schedules associated with moved objects are automatically copied to the new site. If a policy exists in the new home site that has the same name as the policy being copied but different rules, the copied policy name is made unique by applying the original home site name to it. This also applies to premount job schedules.

Polling

If the Backup Manager XML interface is set to one of the XML Gateway groups or to Backup Manager as XML Gateway, the **Backup Manager - Polling** window is displayed.



The XML Gateway interface is used to synchronise the Media Operations database with the Backup Manager

Backup Manager Name: osage.india.hp.com

Define the security parameters used to connect to the Backup Manager

Username: Hulkul-Admin
Domain/Group: Hulkul
Port Number: 5555
Locale of Manager: ENGLISH

Define the schedules for synchronising with the Backup Manager configuration

Time	Config Report	Device Scan	Full Media	Incr Media
00:00	☑	□	☑	□
00:15	□	□	□	□
00:30	□	□	□	□
00:45	□	□	□	□
01:00	□	□	□	☑
01:15	□	□	□	□
01:30	□	□	□	□

Figure 30 Backup manager - polling

To synchronize configuration information from the Backup Manager (pools, media devices, systems, and backup specifications) immediately, click **Manually Synchronize**.

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

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

If the Backup Manager type is **Other**, you need to configure a directory path for Media Operations to import XML configuration files.

Deleting backup manager objects

You cannot delete Backup Manager objects (media, pools, devices, systems, and backup specifications) from the Media Operations GUI, because they are automatically synchronized with the Backup Manager. You can however delete manually created objects.

A Backup Manager object is automatically deleted from Media Operations when it is deleted from the Backup Manager. Media Operations detects deleted objects during the **Config Report** and **Full Media** scheduled polling events, so there is a delay between deleting the object in the Backup Manager and in Media Operations.

The following objects are not immediately deleted from Media Operations:

- Medium is *not* immediately deleted; instead it is set to pending delete and added to a blank media vaulting job the next time vaulting jobs are created. The blank media vaulting job retrieves the deleted medium from its current storage locations and returns 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.
- Media pools containing the pending delete media are retained until the media are fully deleted.
- If a medium is deleted from a Backup Manager and 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.
- Backup specifications deleted from the Backup Manager are not deleted from Media Operations if there are media present in the Backup Manager containing backups from that backup specification. This allows 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.

Media Operations database backup

The Media Operations Server must be protected by backup against loss of database information in a disaster.

Use the Media Operations Server console to configure and schedule backups of the server database. See the server online help for instructions.

IMPORTANT:

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

Tuning backup objects

This section discusses methods of optimizing backup objects performance.

Refining physical locations

Configuring data centers helps you optimize premount jobs. Premount jobs are faster and more efficient if the premount walk-through is grouped in a logical order by physical location (to use the shortest/quickest path from device to device).

By default, any system or device is placed in the default data center. You can change the data center assignment if you have additional data centers in your site. Also, if you created data center grid locations and assigned a system or device to the data center, you can also specify its grid location.

Modify locations for systems and devices from **Global Objects -> Backup/Restore Devices**, **Global Objects -> Systems**, or **Backup/Restore Devices and Systems** at the site level.

If systems and devices are assigned to a Backup Manager, you can edit them from **Devices** and **Hosts** tabs in the **Edit Backup Manager** window.

Finally, you can import system grid locations from the **Import** tab on the **Site Configuration** window. Any devices attached to those systems automatically inherit the host system grid location.

Refining media compressions

All devices and media 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 is essential when estimating scratch media needs during premount jobs. Leaving a default attribute may result in overestimating the number of media.

To modify compressions for pools, go to **Global Objects -> Media Pools** or **Media Pools** at the site level. If pools are assigned to a Backup Manager, you can also edit them from **Pools** in the **Edit Backup Manager** window.

To modify compressions for devices, go to **Global Objects -> Backup/Restore Devices** or **Backup/Restore Devices** at the site level. You can not modify the compression of a device if it belongs to any backup manager.

Adding and modifying media types

Media Operations contains a set of predefined media types and compressions for most current tape technologies., which you may add to or modify.

If you add a new media type and you use a supported Backup Manager or XML File Import interface, Media Operations automatically creates the basic media type. You must also create compression types for the media. If the new media type does not match an existing vault slot type, configure a new vault slot type using **Global Configuration Options -> Media Types and Compressions**.

Defining media policies

There are three basic types of media policies:

- **Media Vaulting Policies**, defining how long a medium is retained in a device, onsite and offsite vault locations.
- **Scratch Media Policies**, defining premount jobs that manage loading new scratch media into backup/restore devices and removal of media to be vaulted from the devices (based on the vaulting policies).
- **Server Parameters**, defining schedule settings that indicate when vaulting, scratch, and premount jobs run.

Configuring media vaulting policies

Vaulting policies configured in each site are built on global vaulting policy templates. You can deploy these policies in a site at various levels to control which media in that site they affect.

If you modify a template, the changes immediately apply to every vaulting policy to which the template was originally applied. This saves you modifying the policy multiple times. Every vaulting policy template is defined in terms of:

- "Media vaulting policy hierarchy" on page 80
- "Basic vaulting policy concepts" on page 81
- "Vaulting templates" on page 81
- "Active vaulting policies" on page 82
- "Defining barcode labeling policies" on page 84

Media vaulting policy hierarchy

- **Default Site-Wide Vaulting Policy.** When creating a new site, configure a default vaulting policy for all new media pools created in that site using the **Site Configuration** window.
  - Create onsite vaults or offsite vendor locations for use in the site-wide vaulting policy before you apply this policy.
  - If you modify a policy, you can apply the changes to any media pools that use the old default policy. You can also apply the new policy to any media in those media pools (by default, policy change only applies to new media).
  - The site-wide vaulting policy cannot be deleted.
- **Media Pools.** Each pool has a vaulting policy that applies to all media in the pool. This policy is configured in the **Edit Media Pools** window. If you modify a pool-level vaulting policy, you can apply the changes to all media in that pool.
- **Backup Specifications.** You can define a vaulting policy that applies to a specific backup specification (and all media used by that backup specification). Use this to define vaulting policies for media that contain critical data (based on the backup specification used to back up critical data) and require specific vaulting policies. Configure this policy via the **Edit Backup Specification** window.
  - Any policy set at this level overrides pool-level policies.
  - If you modify a backup-level vaulting policy, you can apply the changes to all media used by the backup specification.
  - If a backup specification uses devices in multiple sites, you cannot set a backup-level policy for that backup specification.
- **Systems.** Vaulting policies that apply to a system (and all media used by the backup specifications that reference that system) are configured via the **Edit Systems** window.
  - A policy set at this level overrides backup-level and pool-level policies.
  - If you modify a system-level vaulting policy, you can apply this change to all media associated with that system.
- **Vaulting Policies for Copy Media.** For any media belonging to Backup Managers that support copy operations (such as Data Protector A.06.00, A.06.10, A.06.11, and A.06.20), you can define different vaulting policies (at site, pool, backup specification, and system levels of the policy hierarchy).

  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. Media used for backups then have `Policy1`, and copy media have `Policy2`. If you do not define a copy policy to an object in the hierarchy, the primary policy is applied to copies.

- **Vaulting Policies for Consolidation Media.** For any media belonging to Backup Managers that support consolidation operations (such as Data Protector A.06.20), you can define different vaulting policies (at site, pool, backup specification, and system levels of the policy hierarchy).

  For example, in pool `AB_PROD`, you can set `Policy1` as the primary policy for that pool, and `Policy2` as the policy for consolidation media. Media used for backups then have `Policy1`, and consolidation media have `Policy2`. If you do not define a consolidation policy to an object in the hierarchy, the primary policy is applied to consolidations.
- **Single Pieces of Medium.** In the **Edit Media** window, you can override the vaulting policy set by the hierarchy. While that override is in place, media are protected from any policy changes.

Basic vaulting policy concepts

Vaulting policies consist of a series of vaulting cycles. Each cycle defines when and where to move used media. Vaulting cycles then combine in a time-based scheme controlling media progress through scheduled vaulting locations.

Typical vaulting locations include a vault in the media home site, a vault in another site on the same server, or an offsite vendor location. Select a location based on how secure and protected against a disaster media should be and how quickly you may need to retrieve them.

Vaulting templates

Media Operations uses templates as a framework for creating active vaulting policies in each site. Templates define one or more vaulting cycles, but 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 does not have the offsite vendor and account defined because these are different for each site.

The following vaulting templates are pre-defined:

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

- **Medium Recovery Access, Medium Media Security:** Medium is not retained in the device. It is kept 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 nor in an onsite vault. It is kept in an offsite vault until it expires.

You can modify pre-defined or create your own templates using **Global Objects -> Vaulting Templates**.

Active vaulting policies

To apply an active policy, first add it to the site using **Add/Edit Pools**, **Add/Edit Backup Specs**, or **Add/Edit Systems**, or through the **Vaulting Policies** tab on the **Site Configuration** window.

Adding a Policy

1. Choose a policy name and a template.

2. Edit the vaulting cycles to complete their configuration:

    a. If the vaulting policy destination is an offsite vendor, choose the offsite vendor and offsite vendor accounts.

    b. If the vaulting policy destination is a vault, leave it at the default destination or specify another site on your Media Operations Server.

    c. Optionally, alter **Day Number**, representing the number of days before you move your policy to destination in this vaulting cycle.

    d. If the **No Later Than** day number is zero, but your backup jobs straddle two days, vaulting job service level agreements (SLAs) may not be achievable (for example, media are only available from the backup after the shipment for the offsite vendor). In this case, set Day Number to 2 and use **No Later Than** to keep in compliance with SLA.

       This option allows some flexibility: for example, if media are not available in time for the first day's shipment to the destination vault, they can be manually checked into the onsite vault by clicking **Manual Vaulting**. When the next day's vaulting job is created, it automatically asks you to move the media from the onsite vault to the destination. The **Optional** tab on the **Vaulting Job Confirmation** window lists all media not yet sent to their destination, which are within their **No Later Than** window.

    e. 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, the appending scheme will not work, because the media will be vaulted immediately after backups. In this case, set **Vault When Full**, which will vault the media when they have reached their vaulting day if the media contain a full backup or the media are physically full. For example, if you set **Day Number** to five and enable **Vault When Full**, incremental media remain in the device until they are full or more than five days old. The **Optional** tab on the **Vaulting Job Confirmation** window lists all media not yet sent to their destination, with the **Vault When Full** policy enabled and having become full since the vaulting job was created.

    f. Use **Container Storage** to enforce container-based media movements when moving media to and from offsite locations (if your offsite vendor requires you to send media in locked containers). 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 (vaulting, scratch bin, and checkout request jobs).

    g. Use **Vaulting Days** to define which days to ship media to their destination location.

Selecting a Policy

ⓘ IMPORTANT:

If multiple vaulting policies are applied at the same level (such as backupspec, or system), the recently created vaulting policy is applied to the qualified media.

After adding the policy, select it from the **Vaulting Policy** list for the object to which the policy needs to be applied.

If the new policy changes the object from a previous policy, the change is implemented only when you save it by clicking **OK**. If there are media associated with the old vaulting policy, you are prompted to apply the policy to existing and new media, or to new media only.

Viewing a Policy

Backup objects list the vaulting policies currently configured for them. You can edit the policy and view the information listed under **Pools**, **Systems**, **Backup Specs**, and **Media** tabs.

Defining barcode labeling policies

If you print your own barcode labels, you can define barcode labeling policies to improve identification of media 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 number range for a barcode string from 6-9 characters (default: 6). You can set a character prefix (up to "barcode length -1"), a number range (barcode length minus prefix length), and a suffix representing the compression of the media type. How many prefix characters you use 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, and Extended Numeric.

Example

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

You could add to this a suffix such as `L1` for LTO-Ultrium type tapes.

Printing barcodes

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

When 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

Scratch media policies are based on premount jobs, which calculate the number of scratch media required in a device and the time needed for a specified backup job.

You can define a single default premount job, which calculates how many scratch media are needed in every device for all backup jobs in a site or multiple custom premount jobs, to split your scratch media operations across multiple sets of backup jobs. Premount jobs to load scratch media into devices are used to dismount media from those devices for vaulting.

To edit scratch bin schedules, go to **Global Objects -> Scratch bin schedules** or **Scratch bin levels** at site level.

Configuring premount jobs

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

To edit/add premount job schedules, go to **Global Objects -> Premount Schedules** or **Premount Schedules** at the site level.

To assign backup specifications to premount jobs, go to **Edit Backup Specifications**; to assign copy/consolidation specifications to premount jobs, go to **Edit Copy/Consolidation Specifications**. You can also bulk assign multiple backup specifications to a specific premount schedule by clicking **Assign to Premount** on the **Backup Specifications** window. You can bulk assign multiple copy/consolidation specifications to a specific premount schedule by clicking **Assign to Premount** on the **Copy/Consolidations Specifications** window.

NOTE:

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

Premount jobs manage scratch premount processes for every backup/copy/consolidation specification assigned to them. Premount processes are arranged around backup/copy/consolidation specification objects (rather than devices), because a backup/copy/consolidation job can use multiple tape libraries or standalone drives that need the appropriate scratch media loaded before the job starts. Otherwise, the job fails.

Each site has a default premount job that cannot be deleted, to which all backup/copy/consolidation specifications in the site are assigned. You can create additional premount jobs 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/consolidation specifications assigned to that job. The schedule specifies when to run mount and dismount, as well as 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, backup sizes, and media compressions defined for the pools in the backup specification. If the Backup Manager does not provide history, you can set the schedule manually together with average backup sizes. These values are overwritten if the Backup Server starts to provide historical average size data.

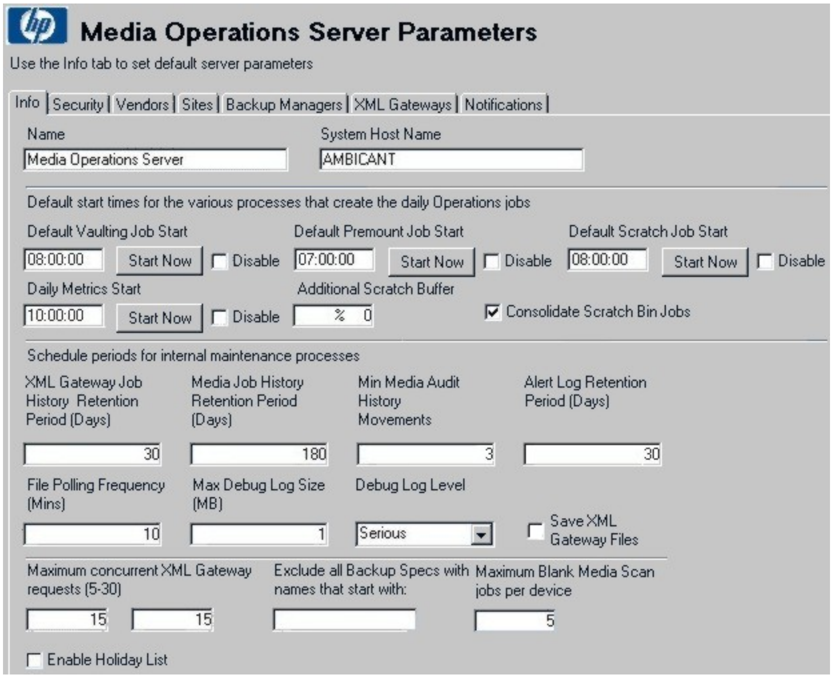
You can optimize scratch media levels by editing the backup specifications and, under the **Drives** tab, configuring the percentage allocation of scratch media for each drive in the specification. Normally, scratch media are distributed equally across all drives (for example, if there are two drives, 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 allocation numbers. You can also adjust the balance across multiple libraries within the same backup specification.

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 141 for details.

Server parameters

The **Server Parameters** window allows you to tune start times of daily Media Operations, define how much audit history is retained in your database, and define maximum numbers for scheduled Backup Manager synchronization jobs.



Media Operations Server Parameters
Use the Info tab to set default server parameters
Info | Security | Vendors | Sites | Backup Managers | XML Gateways | Notifications

Name: Media Operations Server

System Host Name: AMBICANT

Default start times for the various processes that create the daily Operations jobs

Default Vaulting Job Start: 08:00:00 [Start Now] □ Disable

Default Premount Job Start: 07:00:00 [Start Now] □ Disable

Default Scratch Job Start: 08:00:00 [Start Now] □ Disable

Daily Metrics Start: 10:00:00 [Start Now] □ Disable

Additional Scratch Buffer: % 0

☑ Consolidate Scratch Bin Jobs

Schedule periods for internal maintenance processes

XML Gateway Job History Retention Period (Days): 30

Media Job History Retention Period (Days): 180

Min Media Audit History Movements: 3

Alert Log Retention Period (Days): 30

File Polling Frequency (Mins): 10

Max Debug Log Size (MB): 1

Debug Log Level: Serious

□ Save XML Gateway Files

Maximum concurrent XML Gateway requests (5-30): 15 15

Exclude all Backup Specs with names that start with:

Maximum Blank Media Scan jobs per device: 5

□ Enable Holiday List

Figure 31 Server parameters - info

Under the **Info** tab, you can adjust the following values:

- **Default Vaulting Job Start**—the time when the vaulting job is performed.

  Click the **Start Now** button to start the job immediately.

Disable check box: In this and the next three parameters, check the disable boxes to prevents jobs starting by default.

- **Default Premount Job Start**—the time when the premount job is performed (when the contents of the days premounts is calculated).
- **Default Scratch Job Start**—the time when the scratch job is performed.
- **Daily Metrics Start**—the time when activity metrics are performed.
- **Additional Scratch Buffer**—the additional scratch buffer percentage defining a global adjustment to all premount job calculations.
- **Consolidate Scratch Bin Jobs**—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 has its own scratch bin job.
- **XML Gateway Job History Retention Period (Days)**—how long entries in the XML Gateway job history log are retained, from 1–180 days.
- **Media Job History Retention Period (Days)**—how long entries in the media transit job history log are retained, from 1 to 730 days.
- **Min Media Audit History Movements**—the minimum number of media movements to be retained in the media audit history.
- **Alert Log Retention Period (Days)**—how long entries in the alert history log are retained, from 1–180 days.
- **File Polling Frequency (Mins)**—the frequency of checking for new files (in minutes).
- **Max Debug Log Size (MB)**—the level of message to 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)**—the maximum number of XMLGW report jobs (such as config info, media info) that can run concurrently, and the maximum number of XMLGW device jobs (such as device scans) that can run concurrently.
- **Exclude all Backup Specs with Names that Start with**—for filtering backup specifications.
- **Maximum Blank Media Scan jobs per device**—the maximum number of blank media scan jobs that can run concurrently.
- **Enable Holiday List**—if enabled, the holiday list prevents Media Operations from starting jobs on holidays. For more information about holiday lists, see "Holiday list configuration" on page 162.

Vaulting jobs

The vaulting job start time defines when vaulting jobs are created across all sites in the Media Operations Server. This is also the start time on which SLA measurements are based.

Scratch bin maintenance

The scratch bin start time defines when scratch bin and scratch initialization jobs are created across all sites in the Media Operations Server. This is also the start time on which SLA measurements are based.

Premount jobs

The premount start time defines when premount jobs are processed and created across all 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.

When scheduling and optimizing premount jobs, ensure that:

- Start times in the premount schedule are after the premount processing start time.
- The device scan, if any, scheduled before the premount, runs before the premount processing start time (so that the scan happens before premount needs are calculated).

Audit history

You can adjust the following settings for the audit history:

- How long entries in the XML Gateway job history log are retained (1–180 days)
- How long entries in the media transit job history log are retained (1–730 days)
- How long entries in the alert history log are retained (1–180 days)
- The minimum number of media movements to be retained in the media audit history.

Setting up offsite transfer of media

To transfer media offsite using Media Operations, you need to set up both the receiving server (server A) and the sending server (server B):

Setting up the receiving server

1. Create a new site on server A.
2. For the vaulting policy template, select **Onsite Vaulting, Medium Security**.
3. Edit the first policy cycle entry on the vaulting cycle and click the **Add Vault** button.
4. Type a name for the vault.
5. Select the **Layout** tab and click **Auto-Create Layout**.
6. In the **Starting Slot** and **Ending Slot** fields, type valid numbers depending on your site layout.
7. Select the correct **media slot type** and click **Create**.
8. When the site has been created, edit it and click the **Remote Accounts** tab.
9. Click **Add** to add a new remote account.
10. Type in a valid username and password. Remember these because you will need them when you configure the second server.

Setting up the sending server

1. Create a new site on server B.
2. For the vaulting policy template select **Slow Recovery Access, High Security**.
3. Edit the first policy cycle entry on the vaulting cycle and click the **Add On Site Vendor** button.
4. Type a name for the new vendor.
5. Add a new offsite vendor account.
6. In the account ID field enter the account username you specified on the receiving server (server A).
7. In the Hostname field, enter the TCP/IP hostname of the receiving server.
8. In the account password field, enter the password you specified on the receiving server.
9. Perform a backup on a backup server to create some protected media that will need to be vaulted.
10. Add the backup server to this site.

11. After the polling is done for the backup server, open the **Server Parameters** window.

This should trigger communication between the two servers. The vaulting job will show up on the receiving server and should work in a similar fashion to onsite vaulting jobs.

NOTE:

Even after the media is confirmed on the source server and the job is **Marked as Complete**, the job remains open. A vaulting job gets created automatically on the destination server. The media then needs to be vaulted on the destination site and the job should be marked as complete at the destination. Once this is done, the job is automatically closed in the source site as well.

4 Performing daily Media Operations

Overview

NOTE:

To perform daily Media Operations for a particular site, you must have appropriate user rights.

This chapter describes the following:

Running jobs through the CLI

The daily operation of Media Operations can be started using `startjob` on the command line interface (CLI).

`startjob` is a Java-based command-line utility that starts Media Operations jobs from any client system. The utility can be used to start any premount, vaulting, scratch bin or daily metrics job.

To start the utility, you can use `startjob.bat`, available in the *`<MediaOperations_install_dir>`*`\MediaOps\Client` and the *`<MediaOperations_install_dir>`*`\MediaOps\DBServer` folders.

By default, the installation directory is `c:\Program Files\Hewlett-Packard\DataMgt`.

Syntax:

```
startjob servername username password jobname
```

Parameters:

`servername` Name of the Media Operations Server on which the job is to be started.

`username` Valid username for the Media Operations Server.

`password` Valid password for the Media Operations Server.

`jobname` Name of the job to be started on the Media Operations Server. Valid job names are:

```
Vault
Premount
Scratch
DailyMetrics
```

Example:

```
startjob server.india.hp.com foobar foobar Vault
```

NOTE:

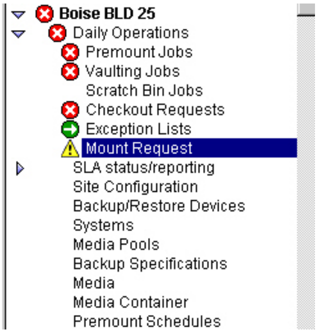
The `startjob` utility only triggers the command to start the job. The actual starting of the job depends completely on the policy set for individual jobs on the Media Operations Server.

To run the utility on a system on which only the Media Operations client is installed, Java (v.1.2 or higher) must be installed.

On the Media Operations Server installation, the utility uses the Java runtime environment available by default in the DMComms module.

Job status indicators

Status indicators show the overall vaulting status (green - OK, yellow - warning, red - critical) and the status for each job category based on SLA status settings for each active job in that category. For example, if one job in a category are red while all others are green, the whole category is marked red.



Boise BLD 25
Daily Operations
Premount Jobs
Vaulting Jobs
Scratch Bin Jobs
Checkout Requests
Exception Lists
Mount Request
SLA status/reporting
Site Configuration
Backup/Restore Devices
Systems
Media Pools
Backup Specifications
Media
Media Container
Premount Schedules

Figure 32 Job status indicators

Premount jobs

NOTE:

Media Operations does not support daily premount jobs on file devices, RISS devices, Virtual Tape Library (VTL) and file libraries.

Premount jobs preload scratch media into backup devices to minimize the number of media used and prevent mount requests with scheduled backup jobs. A job:

- Retrieves sufficient scratch media from the scratch bin,
- Confirms that the media are scratch and of good quality,
- Loads the media into the assigned devices,
- Dismounts media, needed for daily vaulting jobs, from the devices.

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, and not search for devices in the data center or on mount/dismount lists.

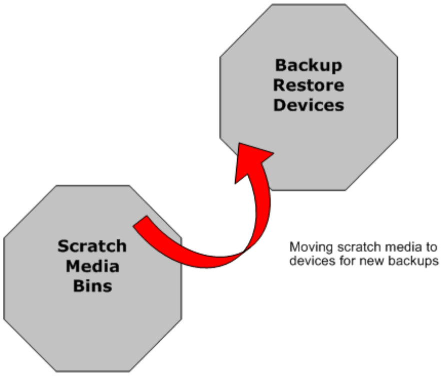
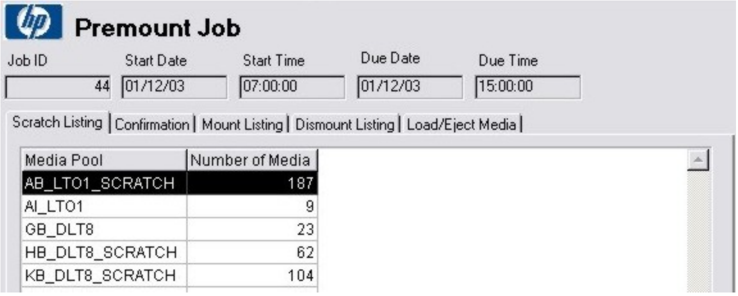


Figure 33 Scratch media movement

Viewing Premount Jobs:

To view a list of active premount jobs, double-click **Premount Jobs** on the **Daily Operations** menu on the shortcut bar. Double-click a job or click **Edit** to get the premount job properties.

Scratch Listing tab — Displays the total number of media required from each scratch bin to complete the mount process.



Premount Job

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

Scratch Listing | Confirmation | Mount Listing | Dismount Listing | Load/Eject Media

Media Pool	Number of Media
AB_LTO1_SCRATCH	187
AI_LTO1	9
GB_DLT8	23
HB_DLT8_SCRATCH	62
KB_DLT8_SCRATCH	104

Figure 34 Premount job - scratch listing

Confirmation tab

Assigns scratch media 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.

To verify the medium, either barcode scan or type a medium description, and click **Verify**. To skip the medium, click **Skip**.

Confirm (by clicking **Verify** or **Skip**) all required scratch media before clicking **Mark As Complete**.

NOTE:

Click **Print Unknown Media** to print a list of all unknown, foreign and blank media.

Poor quality media cannot be used for confirming Scratch Bin jobs.

Mount Listing tab

Displays devices requiring media, the type and quantity of media.

Dismount Listing tab

Displays the media that need to be removed and placed into the holding bin for manual checking, or for that current day's vaulting jobs.

Load/Eject Media tab

Moves the media into/out of the cartridge access port (CAP) for library devices in the mount/dismount lists.

To run the mount cycle, click **Run Mount Cycle** (note that this functionality is not supported for GRAU and DAS devices with this release). The first time, only a dismount cycle is performed (which uploads the CAP with the number of media listed on **Premount Job - Dismount Listing**). This dismount cycle unloads from all libraries listed on **Premount Job - Load/Eject Media**. After the dismount verification, removed media are marked off. The second and subsequent cycles involve selecting the libraries from the list that 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 dismount media are removed.

Silo-type libraries

NOTE:

Run Mount Cycle functionality is not supported for GRAU and DAS devices with this release.

When performing load/eject operations for silo-type libraries (such as ACSLS or DAS), consider the following:

- When you click **Run Mount Cycle** for the first time , silo libraries eject *all* media listed on **Premount Job - Dismount Listing** during this first cycle (on non-silo libraries, it only ejects one CAP's worth of media). To eject the media from a silo library:
  1. Wait for the CAP to be filled and unlocked. Open the CAP and remove all media from it.
  2. Close the CAP. Note that 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.
  3. If there are more media to be ejected, repeat this sequence.
- You cannot put scratch media into the silo CAP until *after* you have clicked **Run Mount Cycle** for the second and any subsequent times. Therefore, after performing the initial eject cycle, proceed as follows:
  1. Select the silo library from **Premount Job - Load/Eject Media**. Click **Run Mount Cycle**.
  2. Go to the silo library and wait for the CAP to unlock. Open the CAP and load the required scratch media into it.
  3. Close the CAP. The load starts.
  4. After all media in the CAP are loaded, any media to be dismounted are automatically unloaded into the CAP. This occurs only if there has been a problem in the first mount cycle.
  5. Wait for the unload to complete and the CAP to unlock. Open the CAP and remove media from it.
  6. Close the CAP to complete the load/eject cycle.

Free/scratch pool handling

A free/scratch pool is an auxiliary source of media when there are no scratch media available in the regular pool. If a media pool, required for a premount job, is able to use media from a dedicated free/scratch pool, you can select the scratch media from either regular or free/scratch pool.

Vaulting jobs

NOTE:

Media Operations does not support daily vaulting jobs on file devices, RISS device, Virtual Tape Library (VTL) and file libraries.

Vaulting jobs consist of:

- Listing the job
- Confirming it

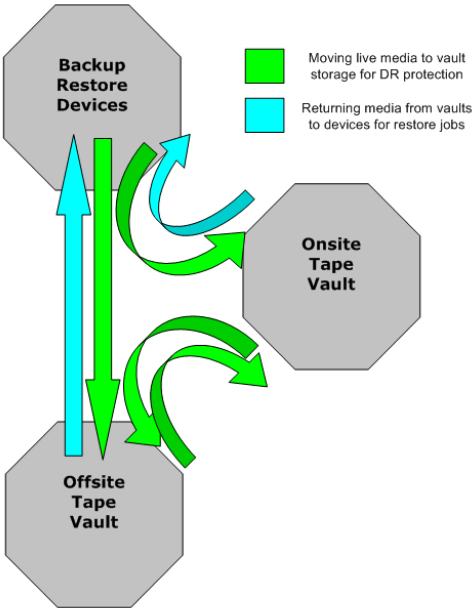
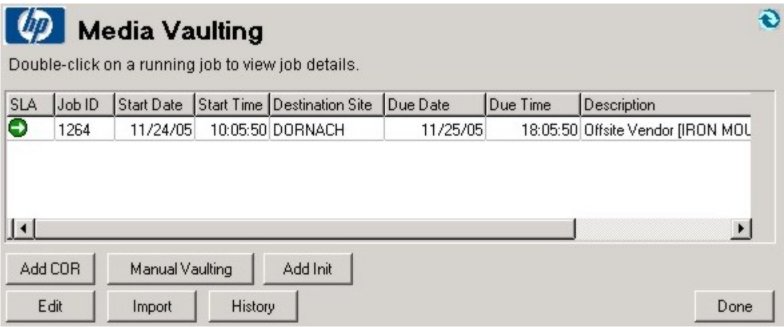

Backup Restore Devices
🟩 Moving live media to vault storage for DR protection
🟦 Returning media from vaults to devices for restore jobs
Onsite Tape Vault
Offsite Tape Vault

Figure 35 Vaulting jobs media movement

Listing vaulting jobs

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

To view a list of active vaulting jobs, double-click **Vaulting Jobs** on the site **Daily Operations** menu.



Media Vaulting

Double-click on a running job to view job details.

SLA	Job ID	Start Date	Start Time	Destination Site	Due Date	Due Time	Description
●	1264	11/24/05	10:05:50	DORNACH	11/25/05	18:05:50	Offsite Vendor [IRON MOU

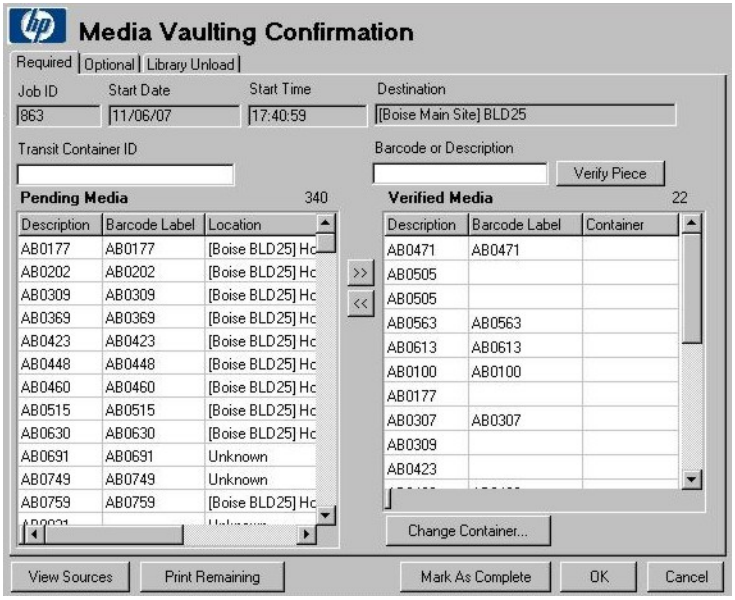
Figure 36 Vaulting job listing

In this window, you can click:

- **Add COR** to create checkout requests for removing media for restore, DRP sessions, special projects, and so on. See "Checkout requests" on page 114 for details.
- **Manual Vaulting** to submit a manual vaulting job. See "Manual vaulting jobs" on page 119 for details.
- **Add Init** to add a new request for media initialization.
- **Edit** or double-click the job to view job details and process the requested media movements.
- **Import** to import vaulting job requests from remote accounts. Use this to create jobs not automatically created on the system due to communication/access issues.
- **History** to view or re-send completed checkout request job to an offsite vendor. You can reprint the media destination details for a completed vaulting job. See "Viewing job history" on page 120 for additional information.

Confirming vaulting jobs

Select a job and click **Edit**, or double-click a job. The following screen appears.



Job ID	Start Date	Start Time	Destination
863	11/06/07	17:40:59	[Boise Main Site] BLD25

Transit Container ID

Barcode or Description

Pending Media 340

Description	Barcode Label	Location
AB0177	AB0177	[Boise BLD25] Hc
AB0202	AB0202	[Boise BLD25] Hc
AB0309	AB0309	[Boise BLD25] Hc
AB0369	AB0369	[Boise BLD25] Hc
AB0423	AB0423	[Boise BLD25] Hc
AB0448	AB0448	[Boise BLD25] Hc
AB0460	AB0460	[Boise BLD25] Hc
AB0515	AB0515	[Boise BLD25] Hc
AB0630	AB0630	[Boise BLD25] Hc
AB0691	AB0691	Unknown
AB0749	AB0749	Unknown
AB0759	AB0759	[Boise BLD25] Hc

Verified Media 22

Description	Barcode Label	Container
AB0471	AB0471	
AB0505		
AB0505		
AB0563	AB0563	
AB0613	AB0613	
AB0100	AB0100	
AB0177		
AB0307	AB0307	
AB0309		
AB0423		

Figure 37 Media vaulting confirmation

To confirm a job:

1. Retrieve the required media from their current locations. Media locations are displayed on the **Pending Media** list.
   - If media come from multiple source locations, you can view them on a source-by-source basis by clicking **View Sources**. From here, you can print a list of required media from any source and see the status of the media movement from each source location. After finishing, click **Done** to return to **Premount Job - Confirmation**.
   - Pending media highlighted in red are marked as exceptions at the source site. This occurs if there is an electronic link to the source site (which is another Media Operations Server or an offsite vendor with electronic status reporting).

   Click **Print Remaining** to print the pending media. This allows you to print a sublist of missing media.

2. Verify the requested media were found. After the media are retrieved from their current locations, you can either:

   - Barcode scan each medium by typing the number and clicking **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 an offsite vendor), you can load the currently verified medium into the vault without marking the whole job as complete by clicking **Vault Confirm**. This 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. You are asked if you want to make any missing media exceptions. If you say no, the confirmation is cancelled and you are returned to verify the remaining media.

5. Print out media destinations. On accepting the print dialog, you get printouts detailing the destination locations for all media you verified for this job. If printing fails, you can reprint the information later by clicking **History** on the job list.

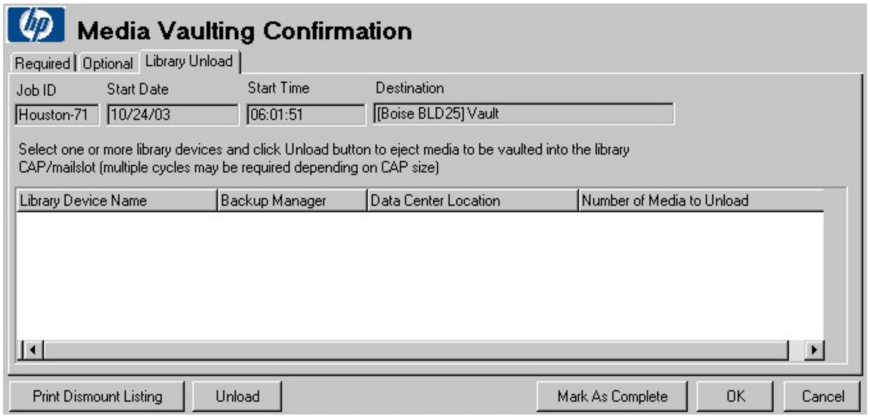
6. Wait for offsite completion. Vaulting jobs sending media to an offsite vendor with an electronic status link remain visible on the job list, because they wait for the job to complete at the offsite vendor. You can still view the vaulting job, but not change it. The vaulting job is automatically closed when notification is received that it is complete. To close the job manually, click **Mark as Complete at Destination** on the **Premount Job - Confirmation** window.

   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. Qualified media are listed on the **Media Vaulting Confirmation - Optional** window. The process of confirming optional media is the same as for required media from the main screen.

   Scanned remote account media are vaulted in the order scanned in the appropriate vaults. You can vault the tapes scanned from the beginning or since the last vaulting (vault sub-lists as you go) without marking as complete. This allows you to place into the vault without completing the entire job first.

Library unload tab

Lists the libraries that contain media required for this vaulting job. It lets you eject the media directly from the vaulting job.



Media Vaulting Confirmation

Job ID: Houston-71
Start Date: 10/24/03
Start Time: 06:01:51
Destination: [Boise BLD25] Vault

Select one or more library devices and click Unload button to eject media to be vaulted into the library CAP/mailslot (multiple cycles may be required depending on CAP size)

Library Device Name	Backup Manager	Data Center Location	Number of Media to Unload

Figure 38 Media vaulting confirmation - library unload

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).

Verifying media

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

- **Verify Piece** to verify the medium entered using the Media Name field.
- **>>** to verify the pending media and move them to the **Verified Media** list.
- **<<** to remove the verified media and return them to the **Pending Media** list.
- **View Source** to print media from each source location. It also allows you to re-notify a source location at another site.
- **Print Remaining** to print all pending media.
- **OK** to save the job.
- **Cancel** to cancel any actions completed since opening the job for processing.
- **Mark As Complete** to close the job and mark any remaining pending media as vaulting exceptions.
- **Change Container** to move any highlighted media in the **Verified Media** list to another specified container.

Containers

The containers used in vaulting jobs are:

- **Lockable Containers:** Use if your vaulting job moves the media to an offsite vendor and the vaulting policy specifies that media must be sent in a lockable container. Consider the following:
  - all media must have the same vaulting policy,
  - all media should have the same protection expiry date.

  If there is a lockable container already in use by the job, media are assigned to this container with the option of marking the container as full. If there is no appropriate container or the container is full, you are prompted to select a different container. To reassign media to a different container, select media under **Verified Media** and click **Change Container**.
- **Transit Containers:** Use if your vaulting job is moving media to another location that does not require a lockable container. Assign the media to a transport container by typing the container ID into the **Container ID** field before verifying a medium. To assign/reassign verified media to a container manually, select media under **Verified Media** and click **Change Container**.

NOTE:

Container columns on pending and verified lists identify the container to which the media belong.

Multiple users

Multiple operators can work on the same job confirmation at the same time. The first user opening **Premount Job - Confirmation** (Windows GUI) is the primary owner of the job; this user will have access to **Mark as Complete**. Any subsequent operators receive a warning that they are assisting the primary job owner. This allows multiple users to retrieve and verify media (each user only sees the media 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, a vaulting job can appear on the job list for multiple sites (depending on your vaulting policy). The behavior for the vaulting job depends on the site type:

- **Home Site** is defined as the site that owns the media. If your home site is not the media destination site and there are media currently located in the home site that need to be moved to the destination site, home site acts as a source site. Otherwise, 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 are sent to the destination. This does not affect **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 stored in their destination and the job is closed.

Scratch media jobs

NOTE:

Media Operations does not support daily scratch bin jobs on file devices, RISS device, Virtual Tape Library (VTL) and file libraries.

Scratch media jobs can be:

- **Scratch Bin Jobs:** Move scratch media from onsite/offsite vendors to scratch bins for reuse. A medium stored in a vault becomes scratch if its protection date expires.
- **Scratch Bin Schedules:** Produce a list of current scratch bin schedules for each site.
- **Scratch Initialization Jobs:** Request the initialization of new media into scratch bins if there are not sufficient scratch media in the ID scratch bins for premount jobs.
- **Media Order Jobs:** Order new blank media if there are not sufficient blank media for scratch initialization jobs (**Blank Bin** is enabled on the **Site Configuration** window).

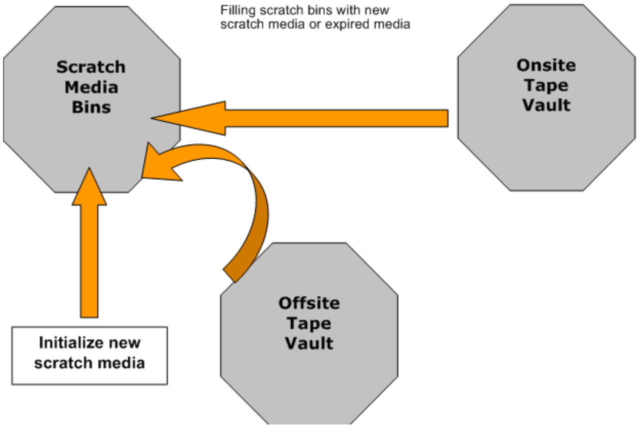
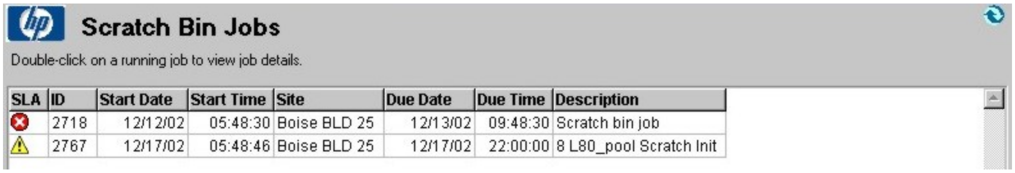

Filling scratch bins with new scratch media or expired media
Scratch Media Bins
Onsite Tape Vault
Offsite Tape Vault
Initialize new scratch media

Figure 39 Scratch media movement

Listing scratch jobs

To view an active list of scratch jobs, double-click **Scratch Bin Jobs** on the shortcut bar under the **Daily Operations** menu.



Double-click on a running job to view job details.

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	8 L80_pool Scratch Init

Figure 40 Scratch bin jobs

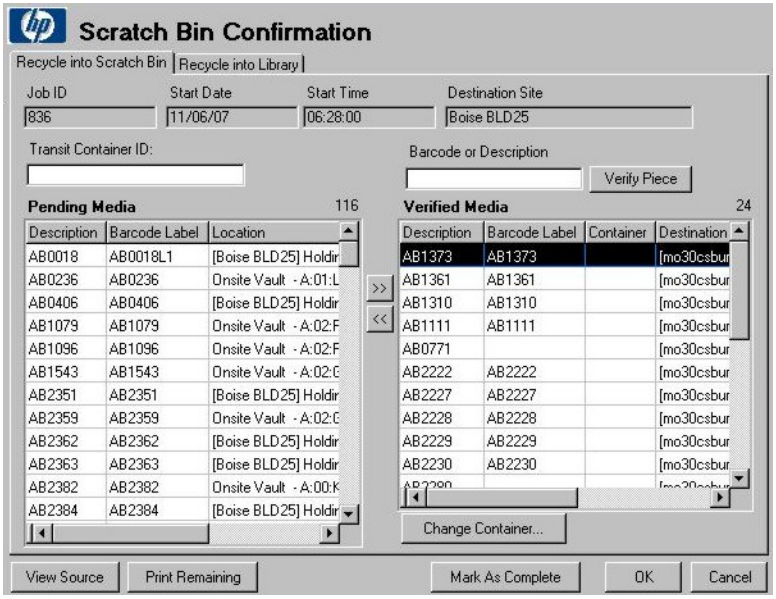
In this window, click:

- **Edit** to view job details and process requested media movements.
- **Add COR** to create a new checkout request. See “Checkout requests” on page 114 for details.
- **Manual Vaulting** to move media into/out of the scratch bin. You can also remove a medium from the scratch bin and place it into the holding bin or vault. See “Manual vaulting jobs” on page 119 for details.
- **Import** to import scratch bin job request from remote accounts. Use to create jobs not automatically created on the system due to communication/access issues.
- **History** to view or re-send completed checkout request jobs to an offsite vendor. You can reprint the media destination details for a completed scratch bin job. See “Viewing job history” on page 120 for additional information.

- **Add Init** to manually create a new scratch initialization job (type the number of media to initialize and select the pool).
- **Add Media Order** to manually create a new media order job (type the number of media and media type). Appears only if **Blank Bin Tracking** is enabled.

Confirming scratch bin jobs

If you edited a scratch bin job, the following window appears:



Scratch Bin Confirmation

Job ID: 836
Start Date: 11/06/07
Start Time: 06:28:00
Destination Site: Boise BLD25
Transit Container ID:
Barcode or Description:

Pending Media 116

Description	Barcode Label	Location
AB0018	AB0018L1	[Boise BLD25] Holdir
AB0236	AB0236	Onsite Vault - A:01:L
AB0406	AB0406	[Boise BLD25] Holdir
AB1079	AB1079	Onsite Vault - A:02:F
AB1096	AB1096	Onsite Vault - A:02:F
AB1543	AB1543	Onsite Vault - A:02:C
AB2351	AB2351	[Boise BLD25] Holdir
AB2359	AB2359	Onsite Vault - A:02:C
AB2362	AB2362	[Boise BLD25] Holdir
AB2363	AB2363	[Boise BLD25] Holdir
AB2382	AB2382	Onsite Vault - A:00:K
AB2384	AB2384	[Boise BLD25] Holdir

Verified Media 24

Description	Barcode Label	Container	Destination
AB1373	AB1373		[mo30csbur
AB1361	AB1361		[mo30csbur
AB1310	AB1310		[mo30csbur
AB1111	AB1111		[mo30csbur
AB0771			[mo30csbur
AB2222	AB2222		[mo30csbur
AB2227	AB2227		[mo30csbur
AB2228	AB2228		[mo30csbur
AB2229	AB2229		[mo30csbur
AB2230	AB2230		[mo30csbur

Figure 41 Scratch bin confirmation

NOTE:

Poor quality media cannot be used for confirming a Scratch Bin job.

If you are at the destination site, **Scratch Bin Confirmation** with Recycle Into Scratch Bin and Recycle Into Library tabs appears.

Proceed as follows to confirm a scratch bin job:

1. Retrieve the required media listed under **Pending Media** from their current location. Consider the following:

   - If the media come from multiple source locations, click **View Sources** to view the required media on a source-by-source basis. From here, you can print a list of required media from any source and see the status of the media movement from each source location. After finishing, click **Done** to return to **Premount Job - Confirmation**.
   - Pending media highlighted in red are marked as exceptions at the source site. This only occurs if there is an electronic link to the source site (which is another Media Operations Server or an offsite vendor with electronic status reporting).

   Click **Print Remaining** to print the pending media. This allows you to print a sublist of missing media.

2. Verify the requested media were found. After the media are retrieved from their current locations, you can either:

   - Barcode scan each medium by typing the number and clicking **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.

   At the destination site, you can verify media to go to scratch bins by clicking **Verify** under **Recycle into Library**. Load verified media 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. You are asked if you want to make any missing media exceptions. If you say no, the confirmation is cancelled and you are returned to verify the remaining media. The media marked as verified under **Recycle into Library** but not loaded are converted to be recycled into the scratch bin.

4. Print out media destinations. On accepting the print dialog, you get printouts detailing the destination locations for all media verified for this job. If printing fails, you can reprint the information later by clicking **History** on the job list.

Containers

If your scratch job is moving media to another site, you can transport the media in a transit container. Assign the media to a container by typing the container ID into the **Container ID** field before verifying a medium. To manually assign or reassign verified media to a container, select media in the **Verified Media** list and click **Change Container**.

NOTE:

Container columns on pending and verified lists identify the container to which the media belong.

Multiple users

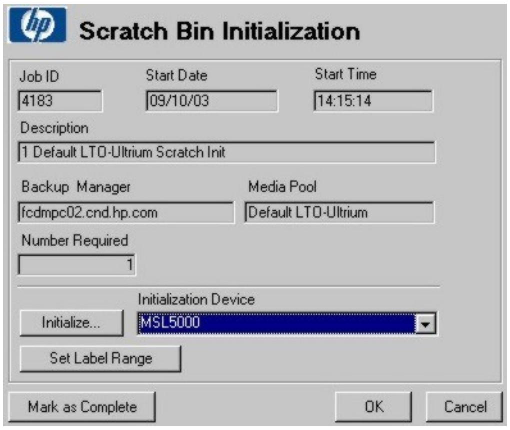
Multiple operators can work on the same job confirmation at the same time. The first user opening **Premount Job - Confirmation** (Windows GUI) is the primary owner of the job; this user will have access to **Mark as Complete**. Any subsequent operators receive a warning that they are assisting the primary job owner. This allows multiple users to retrieve and verify media (each user only sees the media they have verified).

Multiple sites

If you have multiple sites configured on your Media Operations Server, a scratch job can appear on the job list for multiple sites (depending on your vaulting policy). The behavior for the vaulting job depends on the site type—home, source, or destination site. For the sites' description, see "Multiple sites" on page 105.

Initializing scratch media

If you edited a scratch init job, the following window appears:



Job ID: 4183
Start Date: 09/10/03
Start Time: 14:15:14
Description: 1 Default LTO-Ultrium Scratch Init
Backup Manager: fcdmpc02.cnd.hp.com
Media Pool: Default LTO-Ultrium
Number Required: 1
Initialization Device: MSL5000

Figure 42 Scratch init job confirmation

There are two ways to initialize media:

- Initializing a standalone drive
  1. Select a standalone drive from a list of initialization devices and define the label range of media to be initialized.
  2. Click **Set Label Range** to reserve a barcode label range for the media, and then click **Initialize**. If you do not define the label range, you are prompted to define the label for each medium manually.
  3. Mount the first medium with the first label on the specified device, and click **Initialize**. Enable **Force Initialize** if a medium contains data.
  4. After initialization finishes, you are prompted to load the second medium with the second label. This process continues until you either cancel it or the last medium is initialized.
- Initializing using a barcode library

  After the media are properly labelled and loaded into the library slots:
  1. Select the library from the device list and click **Initialize**. A barcode scan is performed on the library and a list of blank or unknown media is displayed along with their barcode labels.

2. Select the medium you want to initialize and click **Initialize Highlighted Media**. Media Operations automatically initializes selected medium using the barcode label for the media label. Enable **Force Initialize** if a medium contains data. **Max Drives Used** determines how many drives inside the library can be used for initialization. Media Operations automatically selects idle drives inside the library; if more media are selected than drives available, the request is queued until a drive becomes available. This is shown as **Waiting for open drive** in the status.

3. 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 (32k or 64k), so that only the drives matching the specified block size are used for initialization.

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

   If media initialization fails, the status is displayed with the red error icon. Double-click the failed medium for additional details.

5. After all media are initialized, click **Mark As Complete** to finish the job.

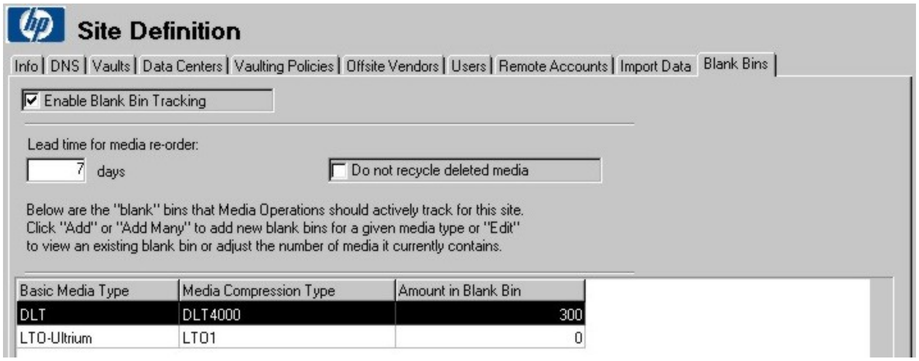
6. On accepting the print dialog, you get printouts detailing all initialized media for this job. If printing fails, you can reprint the information later by clicking History on the job list.

Media order jobs

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

To activate media reordering:

1. Click the **Blank Bin** tab on the **Site Definition** window and select **Enable Blank Bin Tracking**.



☑ Enable Blank Bin Tracking

Lead time for media re-order:

7 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
DLT	DLT4000	300
LTO-Ultrium	LTO1	0

Figure 43 Site definition - blank bins

Configuration

This predicts the amount of media needed for upcoming scratch initialization jobs based on the criteria set when adding a new blank bin.

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

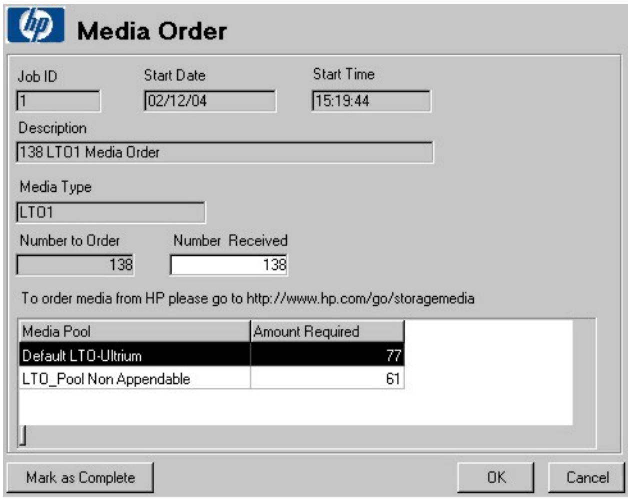
Click **Add** or **Add Many** to add new blank bins for a given media type, or **Edit** to view/edit an existing blank bin.

Confirmation

To order media, click **Scratch Bin Jobs** and then double-click the job.

2. In the **Media Order** window, the ID, start date and time of the job are displayed, together with:

   - Media type description, starting with the amount of required media,
   - Type of media being ordered,
   - The number of media being ordered,
   - The actual number of received media,
   - A description of media types in the pool and the amount of each media type.



Job ID: 1

Start Date: 02/12/04

Start Time: 15:19:44

Description: 138 LT01 Media Order

Media Type: LT01

Number to Order: 138

Number Received: 138

To order media from HP please go to http://www.hp.com/go/storagemedia

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

Figure 44 Media order

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

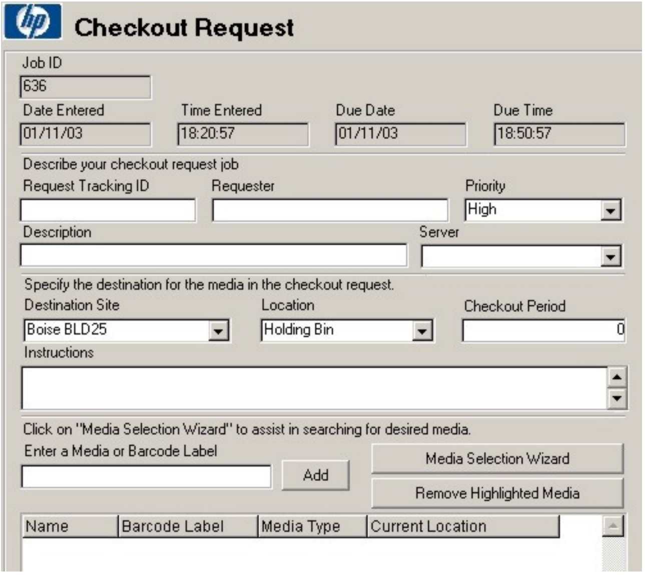
3. Click **Mark as Complete** to finish and return to **Site Configuration**. You now see the total number of added blank media.

Checkout requests (CORs)

Submitting checkout requests

1. In the **Checkout Request** window:

   - Type either the tracking ID from the initiator (OpenView Solutions ID, Remedy ID) or `NONE`.
   - Type the name of the person who placed the request, select the priority, and type a job description.
   - Optionally, select the server the media will be used on, destination site and location, and type the number of days the media need to be removed from their vaulting cycle for this request.
   - Type any special instructions.



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

Figure 45 Checkout request

   - 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), or click **Media Selection Wizard**.

2. Using the **Media Selection Wizard**, query for media meeting the selected filters. This allows you to move a group of media into the COR quickly. Type the desired date range and select the appropriate filters (**Backup Manager**, **Media Pool**, **Backup Specification**, and **System**). After each date/filter selection, the media list is updated. Select the desired media and click **Request Highlighted Media** to move them into the COR job.

   To remove a medium from the list, select it and click **Remove Highlighted Media**.

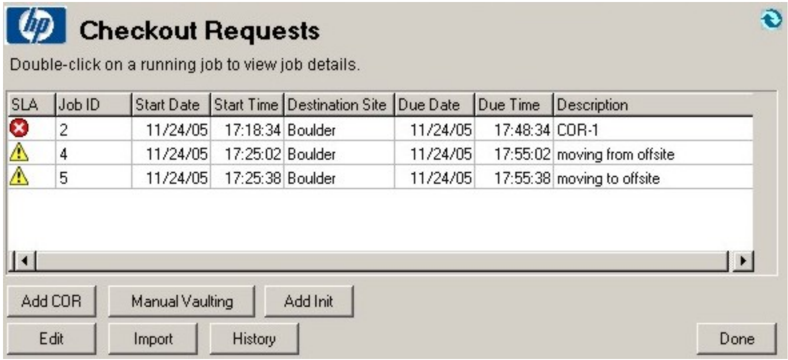
3. When you are done, click **OK** to process the request. This sends notifications to each source location of the medium and prints out a COR report.

NOTE:

You can only add media belonging to your site.

Listing checkout requests

To view an active list of checkout requests, double-click **Checkout Requests** under **Daily Operations** on the shortcut bar for the required site.



Checkout Requests

Double-click on a running job to view job details.

SLA	Job ID	Start Date	Start Time	Destination Site	Due Date	Due Time	Description
✖	2	11/24/05	17:18:34	Boulder	11/24/05	17:48:34	COR-1
⚠	4	11/24/05	17:25:02	Boulder	11/24/05	17:55:02	moving from offsite
⚠	5	11/24/05	17:25:38	Boulder	11/24/05	17:55:38	moving to offsite

Figure 46 Checkout request job listing

In this window, click:

- **Edit** or double-click the job to view job details and process the requested media movements.
- **Add COR** to create a new checkout request. See "Checkout requests" on page 114 for details.

- **Manual Vaulting** to move media into/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 119 for details.
- **Add Init** to add a new request for media initialization.
- **Import** to import a media job from remote accounts. Use this to create jobs not automatically created on the system due to communication/access issues.
- **History** to view or re-send any completed checkout request job to an offsite vendor. You can reprint media destination details for a completed checkout request job. See "Viewing job history" on page 120 for additional information.

Confirming checkout requests

To confirm a COR job:

1. Retrieve the required media from their current locations. Media locations are displayed on the **Pending Media** list.

   - If media come from multiple source locations, view them according to source by clicking **View Sources**. Here, you can print a list of required media from any source and see the status of media movement from each source location. After finishing, click **Done** to return to **Premount Job - Confirmation**.
   - Pending media highlighted in red are marked as exceptions at the source site. This occurs if there is an electronic link to the source site (which is another Media Operations Server or an offsite vendor with electronic status reporting).

   Click **Print Remaining** to print pending media. This allows you to print a sublist of missing media only.

2. Verify that the requested media were found. After media have been retrieved from their current locations, you can either:

   - barcode scan each medium by typing the number and clicking **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. You are asked if you want to make any missing media exceptions. If you say no, confirmation is cancelled and you are returned to verify remaining media.

4. Print out media destinations. On accepting the print dialog, you get printouts detailing the destination locations for all media you verified for this job. If printing fails, you can reprint the information later by clicking **History** on the job list.

Containers

If your scratch job is moving media to another site, you can select a transit container for transporting the media. Assign media to a transport container by typing the container ID into the **Container ID** field before verifying a medium. To assign or reassign verified media manually to a container, select media in the **Verified Media** list and click **Change Container**.

NOTE:

Container columns on pending and verified lists identify the container to which the media belong.

Multiple users

Multiple operators can work on the same job confirmation at the same time. The first user opening **Premount Job - Confirmation** (Windows GUI) is the primary owner of the job; this user will have access to **Mark as Complete**. Any subsequent operators receive a warning that they are assisting the primary job owner. This allows multiple users to retrieve and verify media (each user only sees the media they have verified).

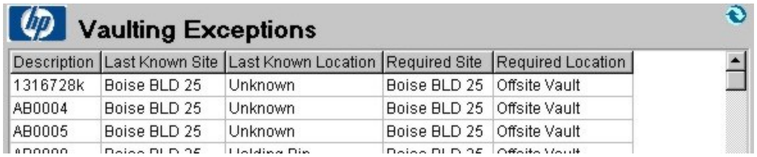
Multiple sites

If you have multiple sites configured on your Media Operations Server, a scratch job can appear on the job list for multiple sites (depending on your vaulting policy). The behavior for the vaulting job depends on the site type—home, source, or destination site. For the sites' description, see "Multiple sites" on page 105.

Exceptions

The **Vaulting Exceptions** window displays a list of media placed into vaulting exception status (required for vaulting, scratch bin, or checkout request jobs that could not be located). Whenever you verify a medium in any medium movement and mark the job as complete, the medium is removed from exception status when successfully verified.

To clear a medium from the exceptions list manually, 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.



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
AB0009	Boise BLD 25	Holding Bin	Boise BLD 25	Offsite Vault

Figure 47 Vaulting exceptions

Mount requests

An *asynchronous* mount request mounts one medium at a time using the **Interactive Mount Request** window.

A *reactive* mount request is an ad hoc mount request that reacts to unforeseen demand for backup media by loading scratch media into a specified drive. The Java-based command-line utility allows you to submit reactive mount requests from any client system into the Media Operations Server. See "Reactive mount request utility" on page 146 for additional information.

Listing mount requests

To view a list of mount requests, double-click **Mount Requests** under **Daily Operations.**

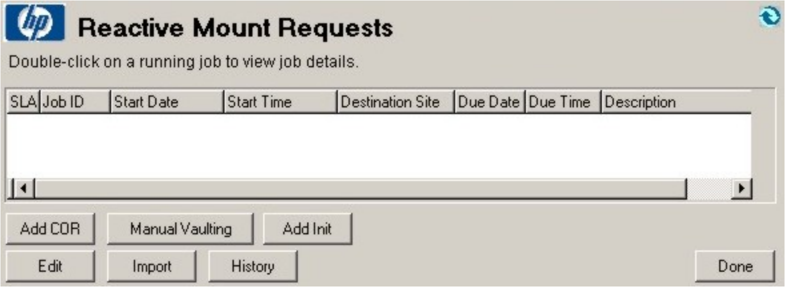


Figure 48 Reactive mount requests

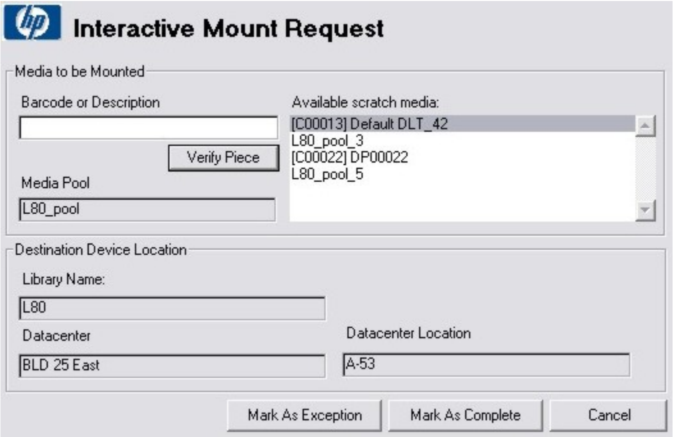
In this window, click:

- **Edit** or double-click the job to view job details and process the requested media movements.
- **Add COR** to create a new checkout request. See "Checkout requests" on page 114 for details.

- **Manual Vaulting** to move media into/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 119 for details.
- **Add Init** to add a new request for media initialization.
- **Import** to import a media job from remote accounts. Use this to create jobs not automatically created on the system due to communication/access issues.
- **History** to view or re-send a completed checkout request job to an offsite vendor. See "Viewing job history" on page 120 for additional information.

Confirming mount request jobs

1. Select a scratch medium from the **Available scratch media:** list or scan/type a medium into the verify field.
2. 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.
    - If you cannot locate any of the available scratch media, select one and mark the request as an exception to remove it. This adds the lost scratch medium to the exceptions list.



Interactive Mount Request

Media to be Mounted

Barcode or Description:

Available scratch media:
[C00013] Default DLT_42
L80_pool_3
[C00022] DP00022
L80_pool_5

Media Pool: L80_pool

Destination Device Location

Library Name: L80

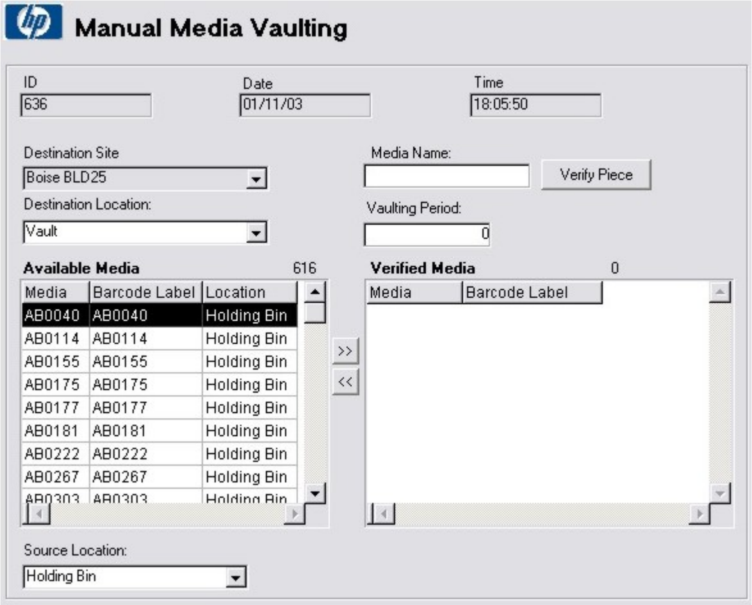
Datacenter: BLD 25 East

Datacenter Location: A-53

Figure 49 Interactive mount requests

Manual vaulting jobs

Manual vaulting moves media into/out of the vault in mass. You can also move media from dismount lists 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 or scratch bin.



Manual Media Vaulting

ID: 636

Date: 01/11/03

Time: 18:05:50

Destination Site: Boise BLD25

Destination Location: Vault

Media Name:

Vaulting Period: 0

Available Media 616

Media	Barcode Label	Location
AB0040	AB0040	Holding Bin
AB0114	AB0114	Holding Bin
AB0155	AB0155	Holding Bin
AB0175	AB0175	Holding Bin
AB0177	AB0177	Holding Bin
AB0181	AB0181	Holding Bin
AB0222	AB0222	Holding Bin
AB0267	AB0267	Holding Bin
AB0303	AB0303	Holding Bin

Verified Media 0

Media	Barcode Label

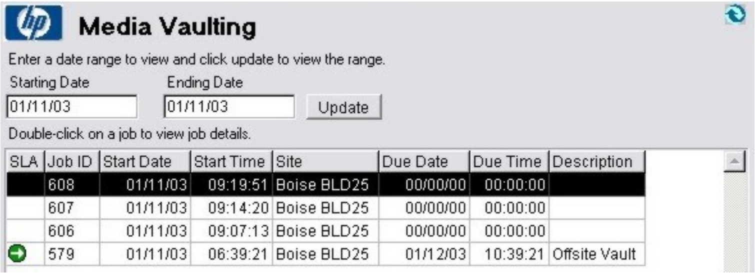
Source Location: Holding Bin

Figure 50 Manual media vaulting

1. Select the destination site and location.
2. Select media from **Available Media** and click **>>** to include them into this movement job. You can type the medium number and click **Verify Piece** or barcode scan it. Media are queried from all locations, not just the source location. To remove a medium, select it in the **Verified Media** list and click **<<**.
3. When all media are entered, click **OK**to assign them to the new location. A vaulting sheet is printed listing the media in the order scanned, which is also the order they are assigned to vault slots.

Viewing job history

Media Vaulting - History allows you to view a completed job for audit reviews or re-send it to an offsite vendor. Type a date range and click **Update** to view a list of completed vaulting jobs.



Media Vaulting

Enter a date range to view and click update to view the range.

Starting Date: 01/11/03

Ending Date: 01/11/03

Double-click on a job to view job details.

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	01/12/03	10:39:21	Offsite Vault

Figure 51 Media vaulting - history

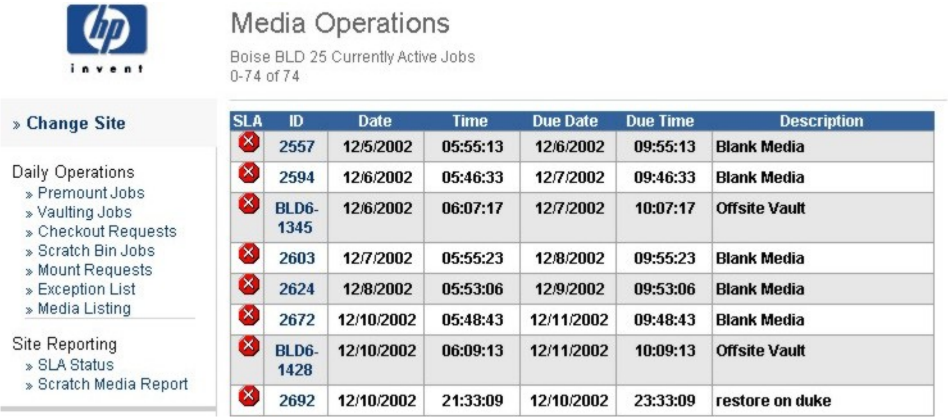
Double-click a job or click **View** to view job details. Vaulting, scratch bin, checkout request, manual vaulting, and mount request details are displayed, together with a list of media that were due to be moved by that job, their origin and destination. Media marked as exceptions are shown in the status column. Also, the user who marked the job as complete and verified it, and the completion date/time are shown.

If the job is a scratch list job, scratch job details are displayed.

Web interface

Media Operations web GUI is another way of performing daily operations. It also provides media information and SLA reporting to assist in running daily operations

The interface allows you to view 250 jobs at once. To view the next set of 250, click **Next**.



Media Operations

Boise BLD 25 Currently Active Jobs

0-74 of 74

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

Figure 52 Web interface

5 Status and reporting interfaces

Overview

This chapter describes service level agreements (SLA) status and reporting options. It is organized as follows:

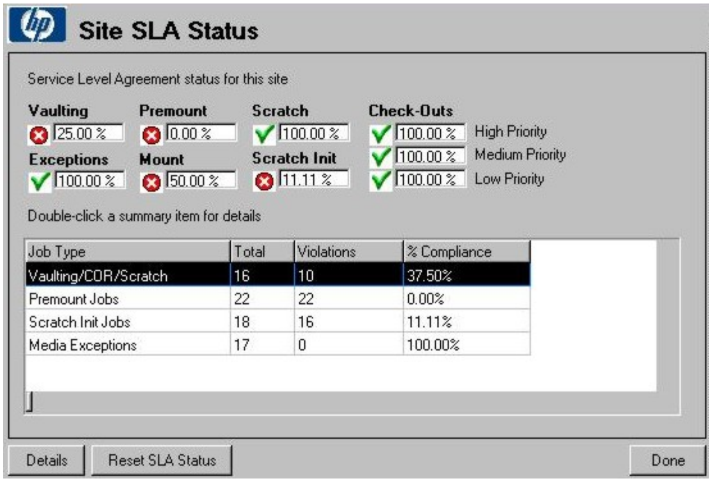
Viewing current SLA status

SLA status settings are available for vaulting, premount, mount request, scratch, and scratch init jobs, and for checkout requests. See Chapter 4 on page 93 for more information about job types and checkout requests.

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 overall SLA status settings measured across all sites and the site-level SLA status indicators for each site are shown.

Click a site on the **Global SLA Status** window or go to **SLA Status** from the site level to see SLA status indicators. Click **Details** to see overdue jobs details.


Site SLA Status

Service Level Agreement status for this site

Vaulting	Premount	Scratch	Check-Outs	
✗ 25.00 %	✗ 0.00 %	✓ 100.00 %	✓ 100.00 %	High Priority
Exceptions	Mount	Scratch Init	✓ 100.00 %	Medium Priority
✓ 100.00 %	✗ 50.00 %	✗ 11.11 %	✓ 100.00 %	Low Priority

Double-click a summary item for details

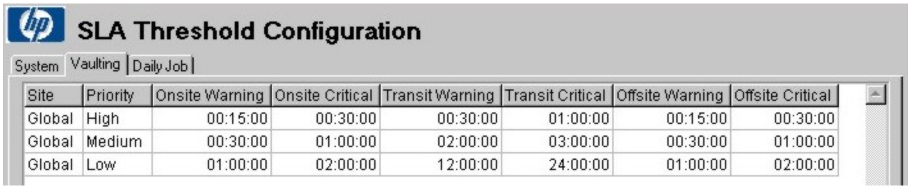
Job Type	Total	Violations	% Compliance
Vaulting/COR/Scratch	16	10	37.50%
Premount Jobs	22	22	0.00%
Scratch Init Jobs	18	16	11.11%
Media Exceptions	17	0	100.00%

Figure 53 Site SLA status

The summary list shows how many jobs were overdue in the main job types for a selected site. To list all overdue jobs for a selected category, click a required job type. Detailed job information is displayed.

SLA status configuration

Use **Global Configuration Options -> SLA Configuration** to set SLA status thresholds for all sites. You can also change thresholds that determine how SLAs are measured against media activities.


SLA Threshold Configuration

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

Figure 54 SLA threshold configuration

System tab

Current settings for SLA status indicators representing various job types. These settings are based on the percentage of each job type completed successfully (within due time) over the defined time period. For example, if the warning is set to 99% and the timeframe is 30, the SLA indicator is set to warning status when the percentage of successful jobs over the last 30 days falls below 99%. To edit settings, click **Edit** or double-click the item. In the **Manage System Threshold** window, make changes and click **OK**.

Vaulting tab

Warning and overdue times for vaulting, scratch, and checkout request jobs. These show up as the warning and critical icons for the jobs; status icons for the job types and the site in the shortcut bar are based on these measures. Each phase of media movement (within the site, from the site to an offsite location, within the offsite location) has its own warning/critical status.

Total overdue time for any job depends on whether the job moves media offsite. If media stays onsite, only onsite times count. The due time is therefore the "onsite critical" time after the job starts. If media are moved offsite, the due time is the sum of the critical times. Automatic vaulting and scratch jobs are always considered low priority. Checkout request jobs have their priority set when they are submitted.

To edit settings, double-click a job or click **Edit**. Make changes in the **Manage System Threshold** window, then click **OK**.

Daily Job tab

Warning and critical times for premount, mount request, and scratch init jobs. Time warning and time critical settings for each job specify the time after the job started before it goes into the warning or critical (overdue) status. To edit settings, double-click a job or click **Edit**.

The **Daily Job** tab also includes SLA status threshold settings for exceptions. The number of media in the exception list is defined in terms of:

- The total number of media exceptions
- The percentage of media exceptions compared to the amount of managed media in the site (site-level exception SLA status) or total managed media (global exception SLA status).

Settings for the total number of exception media take precedence over 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.

Resetting current SLA status

Media Operations 6.2 provides an option to reset the SLA status at both global and site level. Resetting the SLA resets the SLA status for all jobs and restarts the SLA calculation to start from the reset date and time. The **Reset SLA Status** button (as shown in "Figure 53" on page 124) is provided on both the global and site level SLA Status GUIs. The web GUI also lets you reset the SLA Status for a particular site.

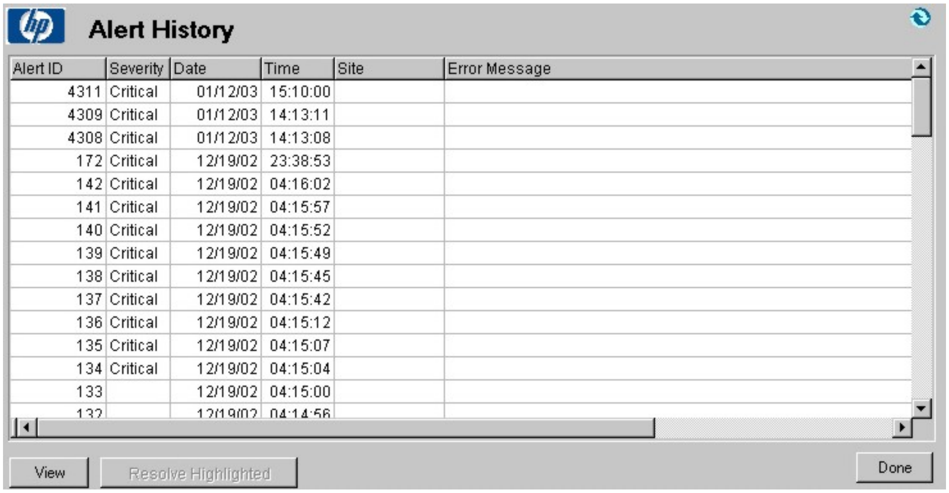
If you click the **Reset SLA Status** button (on the Global & Site SLA status window) the SLA status calculations are performed for the last 30 days (the timeframe configured for SLA) starting from the reset date and time.

NOTE:

The Global level SLA reset resets the SLA status for all associated sites, while the Site level SLA reset only resets the current site's SLA status.

Viewing alerts

Alerts are used to show configuration problems and problems occurring when running requests via XML Gateways to Backup Managers. Alerts are viewed at the site or global level. From the **SLA Status/Reporting** window, double-click **Alert History for All Sites**, or click **Alert History** from **SLA Status/Reporting** for a specific site.



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		
141	Critical	12/19/02	04:15:57		
140	Critical	12/19/02	04:15:52		
139	Critical	12/19/02	04:15:49		
138	Critical	12/19/02	04:15:45		
137	Critical	12/19/02	04:15:42		
136	Critical	12/19/02	04:15:12		
135	Critical	12/19/02	04:15:07		
134	Critical	12/19/02	04:15:04		
133		12/19/02	04:15:00		
132		12/19/02	04:14:56		

Figure 55 Alert history - global

To list pending alerts for all sites, click the **Current Alerts for All Sites** tab in the **SLA Status/Reporting** window.

To view/resolve an alert, double-click it and click **View**. To select multiple alerts and resolve them all at once, click **Resolve Highlighted**. The alerts are moved to **Alert History**.

To resolve an alert (so it switches from the current alerts list to the historical alerts list), click to clear the **Alert is Pending** check box. This returns you to **Pending Alerts**—if you click **Refresh**, the list is updated without the acknowledged alert.

Reports

Use the **Reports** window to generate reports that assist in monitoring activities on the Media Operations Server. There are four types of reports:

- **Vault Audit**—prints a list of media contents located in a cabinet or drawer of a specified onsite vault, which can be used to physically audit the media. Select the site containing the vault, cabinet and drawer names, and click **Print Audit Report**. This report is available at global and site levels.You can save the report to a file if you wish by clicking **Save Audit Report**.
- **Scratch Media**—shows the last 24 hours of activity in the scratch media bins in a specific site. If you select this report via the global SLA Status/Reporting, specify which site to report on. The report includes current and optimal scratch bin levels, whether you have too many or not enough scratch media in each pool (for you

to decide whether to initialize new or remove existing media), and the number of scratch media used by backups in the last 24 hours. This report is also available from the Media Operations web site.

- **Media Movement**—shows the last 24 hours of activity for all media movements caused by vaulting policies, scratch bin maintenance, and checkout requests on a specific site. Example media movements include:
  - moving media from a device to an onsite/offsite vault,
  - moving media from an onsite to an offsite vault,
  - moving media from an offsite vault to another offsite vault (advanced vaulting policy),
  - moving media from an onsite/offsite vault back to a device (advanced vaulting policy or checkout request),
  - moving media from onsite/offsite vaults to scratch bins.

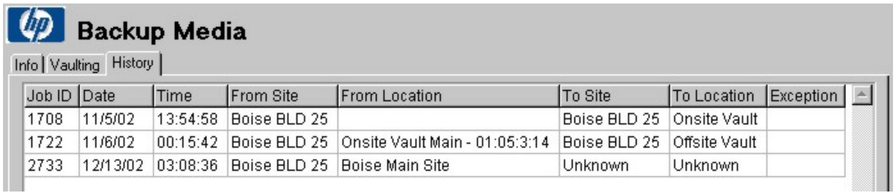
  For each media movement, the report details whether it was overdue or not.
- **Unknown Media**—shows the details of all unknown, blank, and foreign media.

Additional reports

Use the **Feature** tabs in objects to get additional media information reports, such as:

- **Pool Media List** (**Media** tab on the media pools detail form)—lists media in a specified pool.
- **Backup Specifications Media List** (**Media** tab on the backup specifications detail form)—lists media used by a particular backup specification.
- **Systems Media List** (**Media** tab on the system detail form)—lists media used for backups of a specific system.
- **Device Media List** (**Library** tab on the devices detail form for library devices)—shows the media contents of a library device.
- **Container Media List** (**Media** tab on the container detail form)—shows media that are currently in the container.

Backup Media - History lists all movements for a selected medium.



Backup Media

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	11/6/02	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	

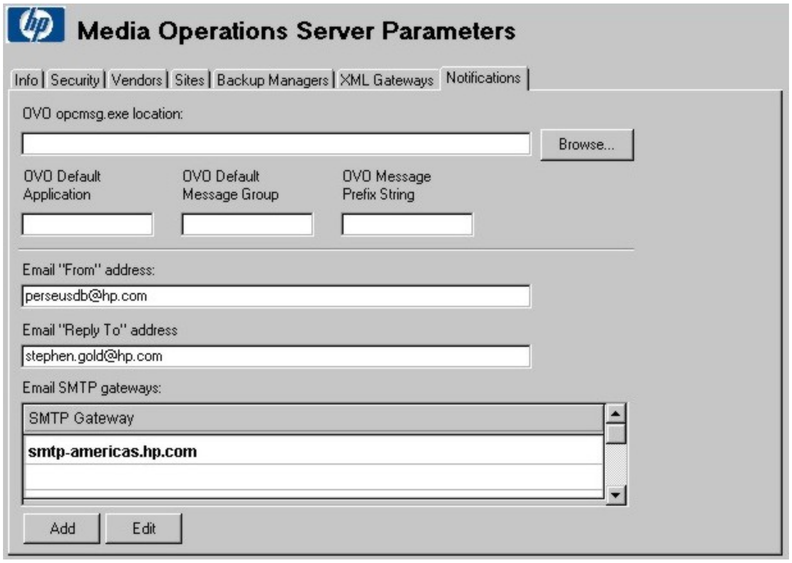
Figure 56 Backup media - history

Notifications

You can configure automatic notifications for key events, such as alerts, job creation, SLA warnings, and metrics.

Configuring notification interfaces

Before configuring notifications, configure the notification interface in the **Server Parameters - Notification** window:



Email "From" address: perseusdb@hp.com

Email "Reply To" address: stephen.gold@hp.com

Email SMTP gateways:

SMTP Gateway
smtp-americas.hp.com

Figure 57 Server parameters - notifications

Two types of notification interfaces are:

- E-mail
- HP Operations Manager

E-mail interface configuration

Configure the following e-mail interface options to enable e-mail notification:

- **E-mail "From" Address**—shown in the From field in all messages sent by the notification system.

- **E-mail “Reply To” Address**—used if anyone replies to an e-mail sent by the notification system.
- **E-mail SMTP Gateways**—a list of one or more SMTP Gateway Servers with their network addresses. At least one gateway is required, because it forwards e-mails from Media Operations to defined users. If you define several gateways, the connection is performed in the order stated in the list, until there is a response or there are no gateways available.

Operations Manager interface configuration

Prerequisite

To use Operations Manager notification, Media Operations Server must be already configured to use Operations Manager.

Configure the following Operations Manager interface options to enable Operations Manager notification:

- **Operations Manager opcmsg.exe Location**—type the path to the `opcmsg.exe` utility, which is used to send notifications to Operations Manager. Click **Browse** to locate the directory containing the utility.

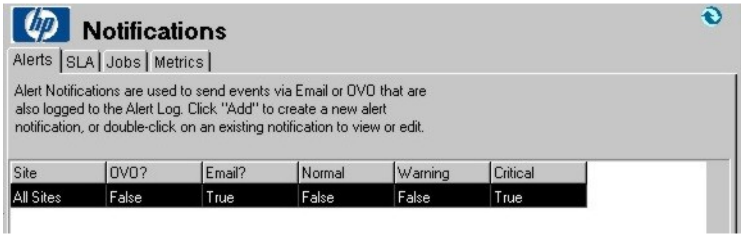
NOTE:

If in the earlier installation of Media Operations the path length of the Operations Manager file was greater than 80 characters, reselect the path after upgrading to Media Operations A.06.20.

- **Operations Manager Default Application**—type an application name (such as `MediaOps`) that will be displayed in Operations Manager for any notifications sent from this Media Operations Server.
- **Operations Manager Default Message Group**—type a message group name that will be displayed in Operations Manager for any notifications sent from this Media Operations Server. You can override this default message group when defining each Operations Manager notification trigger.
- **Operations Manager Message Prefix String**—type a string to prefix every Operations Manager notification sent from this Media Operations Server.

Configuring notification triggers

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



Notifications

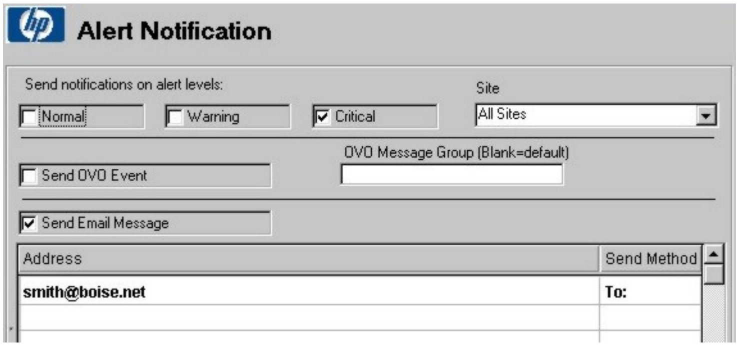
Alert Notifications are used to send events via Email or OVO that are also logged to the Alert Log. Click "Add" to create a new alert notification, or double-click on an existing notification to view or edit.

Site	OVO?	Email?	Normal	Warning	Critical
All Sites	False	True	False	False	True

Figure 58 Notifications

Alerts — Sends events logged to the alert log via e-mail or Operations Manager. Click **Add** to add a new alert notification, or double-click an existing notification to view/edit.

Select **Normal**, **Warning**, or **Critical** check boxes to define the alert level. Click the **Site** arrow and select the site from the drop-down list. Select **Operations Manager Event** and/or **Send Email Message** check box and configure a list of e-mail addresses (by clicking **Add** and/or **Edit**) to receive the notification.



Alert Notification

Send notifications on alert levels:

□ Normal □ Warning ☑ Critical

Site: All Sites

□ Send OVO Event

OVO Message Group (Blank=default):

☑ Send Email Message

Address	Send Method
smith@boise.net	To:

Figure 59 Alert notification - add/edit

SLA

Sends alerts via e-mail or Operations Manager when an SLA is in warning or violation. Click **Add** to add a new SLA, or double-click an existing notification to view/edit.

Choose SLA measures for notification and select the site (select **All Sites** for global SLAs). Select the **Operations Manager Event** and/or **Send Email Message** check box and configure a list of e-mail addresses (by clicking **Add** and/or **Edit**) to receive the notification.

Jobs

Sends alerts via e-mail or Operations Manager when a new job is created. Click **Add** to create a new job notification, or double-click an existing notification to view/edit.

Select job types and the site for notification. You can also select the **Attach Media Listings** check box, which includes document attachments (in HTML format) on the job e-mail notifications that detail the media required for that job. Select the **Operations Manager Event** and/or **Send Email Message** check box and configure a list of e-mail addresses (by clicking **Add** and/or **Edit**) to receive the notification.

Metrics

Sends 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/edit.

Select a period of time for the notification to cover. Note that you can define multiple notification triggers for different metric periods.

Frequency options are:

- **Daily**—metrics are sent every day after they are collected. Default collection time is 10:00 am.
- **Weekly**—metrics are sent summarized for a 7-day period.
- **Monthly**—metrics for the last month are sent on the first day of each month.

The number of units sent is defined by timeframe. If this is 0 or 1, only one unit is sent (one day, one week, one month). If you type 12, you get a report for the last 12 days/weeks/months. If the number is 0 or 1, you get a media pool detail report. >1 gives you totals for all pools.

Select the days the report will be sent from the **Day of Week** drop-down list. The everyday option sends metrics each day for the week ending the previous day.

Metric report description

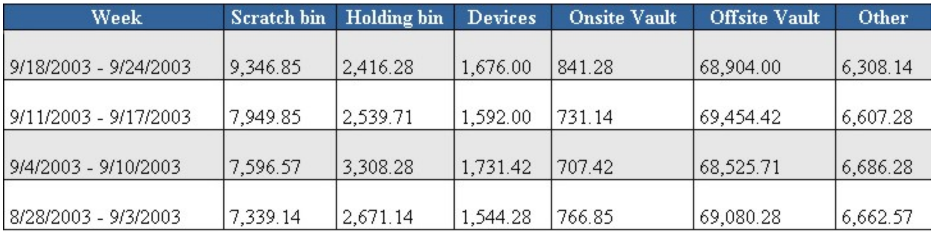
The durations are:

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

Media location summary

The Media Location Summary is the total on a daily report and the average for the number of metric days for weekly and monthly reports. Metric days are days for which metrics are collected and reported in the required timeframe. For example, if a system is installed on the 15th day of a month, the monthly report does not include the first 14 days of the month and the number of metric days will be from the 15th to the end of the month.

Ideally, the `Holding bin` and `Other` columns should be as low as possible. `Other` consists of the COR, unknown and in transit location media.

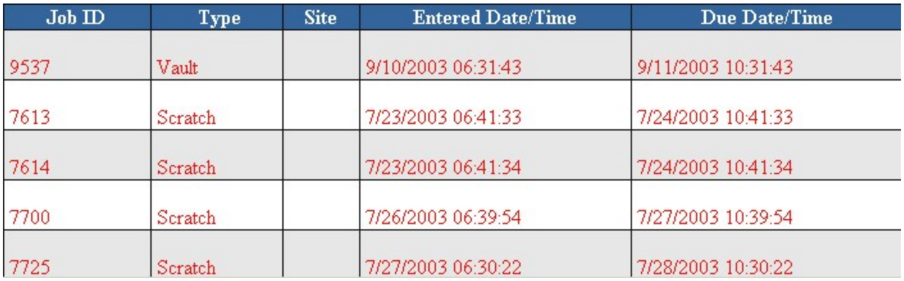


Week	Scratch bin	Holding bin	Devices	Onsite Vault	Offsite Vault	Other
9/18/2003 - 9/24/2003	9,346.85	2,416.28	1,676.00	841.28	68,904.00	6,308.14
9/11/2003 - 9/17/2003	7,949.85	2,539.71	1,592.00	731.14	69,454.42	6,607.28
9/4/2003 - 9/10/2003	7,596.57	3,308.28	1,731.42	707.42	68,525.71	6,686.28
8/28/2003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

Figure 60 Media location summary (daily average)

Job status

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



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

Figure 61 Open job summary

Job metrics

Job metrics are:

- Job Summary (Daily Average)—the average number of each job typed during the specified period.
- Job Period Totals—the total number of each job type during the period.

Pool health metrics

Pool health metrics are:

- Media Pool Health Summary (Daily Average)—the average of how many tapes you had in a media pool for a specified period.
- New Vaulting Exceptions Period Total—the total new vaulting exceptions for the period.

Premount metrics

Premount metrics are:

- Media Premount Summary (Daily Average)—the average number of standalone devices, libraries, media required, and media mounted. The difference between media mounted and media required is that media are mounted without verification in the premount job. If a site requires these scratch media be verified in the pre-mount job, your media may or may not be mounted before the backup starts.
- Media Premount Period Totals—the total number of standalone device mounts, library device mounts, media required, and media mounted.

Vaulting metrics

Vaulting metrics are:

- Protected Media Summary (Daily Average)—the average number of tapes, how many are written, and how many vaulted.
- Protected Media Period Totals—the total number written and the total number vaulted.

Scratch metrics

Scratch metrics are:

- Expired Media Summary (Daily Average)—daily averages for the total number of tapes and expired tapes, and the number of tapes and expired tapes in the scratch bin.
- Expired Media Period Totals

Remote metrics

Remote Account Summary (Daily Average)—the average number of media currently vaulted.

Vendor metrics

Vendor Account Summary (Daily Average)—the average number at the vendor site.

Vault metrics

Media Vault Summary (Daily Average)—the average number at the vendor site.

Location metrics

Media Location Summary (Daily Average)—the average number of media in the scratch bin, holding bin, devices, onsite, and offsite vaults.

Location audits

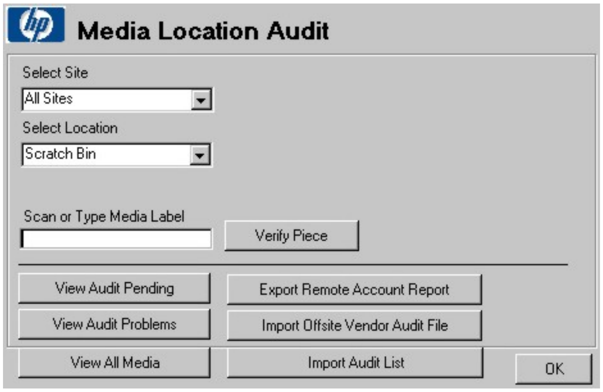
Location audits verify that media are stored in the appropriate place. This allows you to account for each medium and clear exceptions when necessary.

NOTE:

Poor quality media cannot be used.

To start a location audit:

1. Go to **Utilities -> Location Audit**.



Select Site: All Sites

Select Location: Scratch Bin

Figure 62 Media location audit

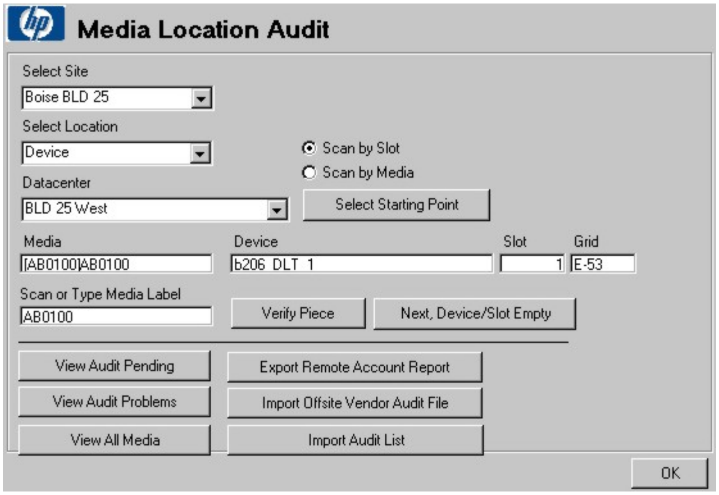
NOTE:

The bottom six buttons are only displayed for top-level administrators.

2. Select a site and location. The following locations are available:
   - **Scratch Bin**
   - **COR Holding Area**
   - **Device**
   - **Vault**
   - **Holding Bin**
3. For most locations, scan the medium or type the media label, then click **Verify Piece**.

   For Device/Vault, go to step 4.

4. *For Device/Vault only:* The following window is displayed:



Select Site: Boise BLD 25

Select Location: Device

Datacenter: BLD 25 West

● Scan by Slot
○ Scan by Media

Media	Device	Slot	Grid
[AB0100]AB0100	b206 DLT 1	1	E-53

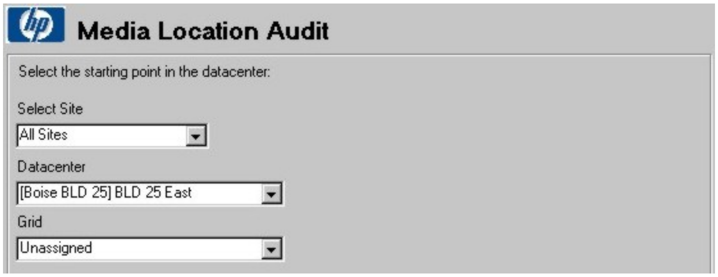
Scan or Type Media Label: AB0100

Figure 63 Media location audit - device/vault screen

a. Select one of the following:

- **Scan by Slot**—verifies the exact location of the media using the walk-through order of the vault/data center.
- **Scan by Media**—verifies the general, not the exact, location in the vault/data center.

b. Select a data center and click **Select Starting Point**.



Select the starting point in the datacenter:

Select Site: All Sites

Datacenter: [Boise BLD 25] BLD 25 East

Grid: Unassigned

Figure 64 Media location audit - select starting point screen

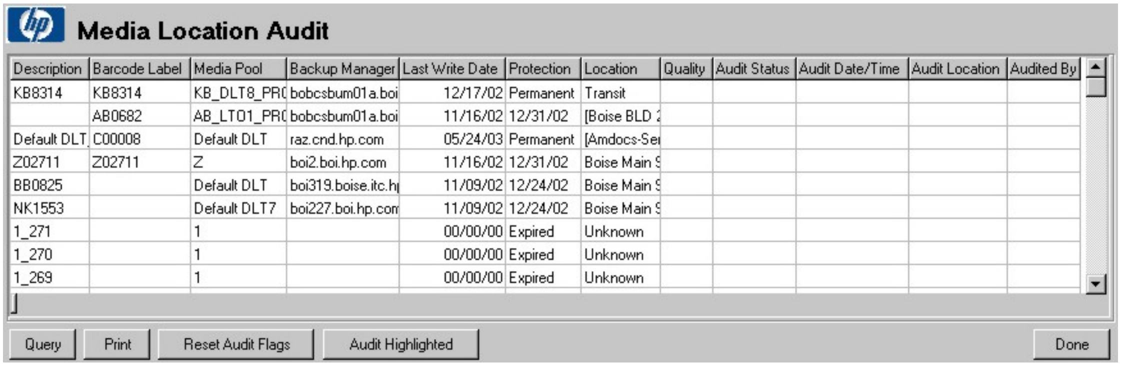
If you choose a starting point in the Unassigned data center, the first medium meeting the set criteria will be displayed. If there is a medium available to audit, you see the media label, device name, slot, and grid ID. To verify a medium, either scan or type the media label and click **Verify Piece**.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

View

You can view the following:

- **Audit Pending**
- **Audit Problems**
- **All Media**

Clicking any of these buttons displays media details for selected sites.



Media Location Audit

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_PR	bobcsbum01a.boi	12/17/02	Permanent	Transit					
	AB0682	AB_LTO1_PR	bobcsbum01a.boi	11/16/02	12/31/02	[Boise BLD					
Default DLT	C00008	Default DLT	raz.cnd.hp.com	05/24/03	Permanent	[Amdocs-Se					
Z02711	Z02711	Z	boi2.boi.hp.com	11/16/02	12/31/02	Boise Main					
BB0825		Default DLT	boi319.boise.itc.h	11/09/02	12/24/02	Boise Main					
NK1553		Default DLT7	boi227.boi.hp.co	11/09/02	12/24/02	Boise Main					
1_271		1		00/00/00	Expired	Unknown					
1_270		1		00/00/00	Expired	Unknown					
1_269		1		00/00/00	Expired	Unknown					

Figure 65 Media location audit - view

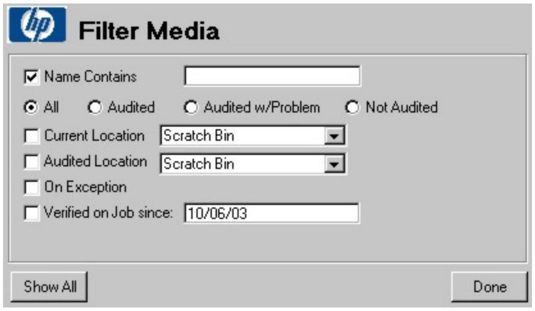
Query

Reloads the media list using the following filters:

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

Example:

If you want to query the media, not audited but vaulted since 10/6/03, leave **Name Contains** blank and select **Not Audited** radio button. Select the **Verified on Job since:** check box and type `10/6/2003`.



Filter Media

☑ Name Contains

● All ○ Audited ○ Audited w/Problem ○ Not Audited

☐ Current Location: Scratch Bin

☐ Audited Location: Scratch Bin

☐ On Exception

☐ Verified on Job since: 10/06/03

Figure 66 Filter media

Print

Click **Print** to produce an audit report describing medium characteristics, such as medium number, current location and status, time stamp, and the person who audited the medium.

Reset audit flags

Before doing a location audit, click **Reset Audit** to purge old audit data.

Audit highlighted

Select media you want to audit (for example, those verified using a paper listing) and click **Audit Highlighted**.

Import/export

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

```
AB0100
BC0123
```

```
AB1285
    :
```

You can type in each number, scan them to notepad, and so on. Export/import for remote accounts/OSVs requires a special XML file, so it is currently only used for Media Operations-to-Media Operations accounts.

Export remote account report

This produces an XML file for a remote account managed by the Media Operations Server. It is useful for transferring audit results to the sending system. Only media in the vault for the remote account are 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 imports the file on the home system 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. To change current locations to offsite, click **Request Audit** from the vendor account entry.

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

Import audit list

Select the location from which the media are being audited. This does not change current media locations. All media imported are 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 find media that either did not match media in the Home Server, or media with more than one match.

A External interfaces

Overview

This appendix describes the following external interfaces:

- "XML file import interface" on page 141
- "XML offsite vendor interface" on page 143
- "Bulk configuration file import" on page 152

XML file import interface

For Backup Managers not supported by XML Gateway, 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:

Assign a unique directory to each file-import Backup Server when you add it to the Media Operations configuration.

File import

Every unique file-import directory is polled by Media Operations for incoming files containing response data blocks (files not coming from the server defined for that directory are ignored). By default, the polling frequency is 1 per minute. You can modify it through **File Polling Frequency** in **Global Configuration Options -> Server Parameters**.

New devices, pools, backup specifications, and media detected in the HTTP/XML response data in valid incoming files are automatically added to the Media Operations Server (in the same way that new devices, pools, and so on in XML response data from the XML Gateway are).

When creating files, you must:

- Provide scripts to convert information from your Backup Server (not supported by 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 and must parse against the applicable Media Operations XML file format DTD. See “XML import file format” on page 142 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 together with incremental media information (preferably once an hour throughout the day). For incremental data:
  - 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/system.
  - If you cannot support media usage information, provide a standard media information file consisting of a list of media that changed since the last media update.

If the script generating the XML import files has an error (for example, if 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. These 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 on the installation media under `docs\xml` for a guide to creating valid Media Operations XML.

XML offsite vendor interface

Media Operations supports electronic links to offsite vendors. This allows Media Operations to send electronic verification of media shipped to offsite storage and request media from offsite storage back to the data center.

Media Operations administrators can 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 three offsite vendor types (Media Operations, Iron Mountain interface, and Generic offsite vendor) that support electronic links. For a description of offsite vendors, see "Site management" on page 39.

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 all request types, Media Operations passes the following parameters into the script that you create.

- *Parameter 1:* **Request type**

  1 - Transit request
  2 - Status request

3 - Request audit
4 - Send audit

- *Parameter 2:* **XML parameters file**

  Filename of the XML parameters file, delimited by quotation marks. Media Operations creates this file before calling the script.

- *Parameter 3:* **Results filename**

  Filename passed into the script by Media Operations, delimited by quotation marks. Media Operations expects any results of the script to be written to this file.

- *Parameter 4:* **Proxy type**

  Whether a Proxy Server is needed to connect to the offsite vendor and, if so, what type:

  0 - No proxy
  1 - HTTP proxy
  2 - Socks proxy

- *Parameter 5:* **Proxy server name**

  Network name of the Proxy Server.

- *Parameter 6:* **Proxy port**

  Port number used to connect to the Proxy Server.

- *Parameter 7:* **Proxy username**
- *Parameter 8:* **Proxy password**

Media transit requests

Transit requests are electronic notifications of media movements to/from an offsite vendor. There are two types:

- **Outgoing** —notify offsite vendors about media shipped to them (including media details).
- **Return** —notify offsite vendors that you want them to return media to you and which sets of media to return.

The XML parameters file conforms to the `TransitRequest.dtd` file. If the transit request is a return request (for example, transit type is cor or scratch), XML includes a destination with address and contact details.

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 these result codes:

1 - Job/request successful
3 - Error parsing XML parameters file
5 - Bad account or password

Request and receive audit requests

Receive audit sends a request to an offsite vendor to verify that the list of media sent in the request matches media for your account currently in the offsite vendor's possession.

Request type = 3: The XML parameters file conforms to the Request Audit DTD. The script must create the specified XML results file in compliance with the Audit List DTD.

Request type = 4: The XML parameters file conforms to the Offsite List DTD.

On exit, your script must return one of these result codes:

1 - Job/request successful (request type 4)
2 - Job/request successful with a result file to process (request type 3)
3 - Error parsing XML parameters file
5 - Bad account or password

Status checking requests

Status checking requests are electronic requests to the offsite vendor to monitor the progress of a previously submitted media transit.

The XML parameters file conforms 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 when 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 these result codes:

1 - Job/request successful
2 - Job/request successful with a result file to process
3 - Error parsing XML parameters file
4 - Job is still running
5 - Bad account or password
6 - No transit job exists (causes the job to be transmitted again)

NOTE:

An additional `Disable Electronic Link Check` is added to the Generic offsite vendor account definition. This option allows you to disable the check for an electronic link interface to an offsite vendor.

XML offsite vendor file format

See the following DTDs and examples 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

A Java-based command-line utility allows you to submit reactive mount requests from any client system to the Media Operations Server. A reactive mount request is an ad hoc request reacting 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 scratch medium to be loaded into a drive for a backup job. For example, if not enough scratch media was loaded into a library by scheduled premount jobs, the Backup Server needs more media when the backup runs. Reactive mount requests are also used to load scratch media for manually created backup specifications, when the backup job is outside the scope of your Backup Managers.

The command-line utility is `MediaOps\Client\reactivemount.jar` on the Media Operations Server and any Media Operations Manager system. If you installed with default locations, this file is at `C:\Program Files\Hewlett-Packard\DataMgt\MediaOps\Client`.

NOTE:

You must have Java (v1.2 or higher) installed on the system on which you want to run the utility.

Syntax

```
<java exe> -cp <full path to reactivemount.jar file>
com.hp.ov.dm.reactivemount.DoReactiveMount <param list...>
```

Parameters

Mandatory parameters:

`-m`	Name of the Media Operations Server name to which to send the reactive mount request.
`-s` or `-mp`	Name of the backup specification requiring media to be mounted. Name of the Media Pool needing to be mounted in the specified device. This parameter is only valid if you define `-c`.
`-d`	Name of the drive in the backup specification to which to load the scratch media.
`-u`	User Name (a valid Media Operations username for authentication)
`-p`	User Password (a valid Media Operations password for authentication)
`-c`	Backup Manager (the Cell Manager that has a mount request). If the reactive mount request is for a manually created backup specification, do not define this parameter.

Optional parameters:

`-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

`-id`	Session ID for the mount request on the backup manager

Return Codes

Return codes for the utility are:

`0`	Success
`1`	Invalid user
`2`	Invalid 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 the same name
`4201`	More than one user entry

NOTE:

If a mount request is for a medium from a pool with a strict policy, specify the media 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 media—the reactive mount job in the Media Operations Server will allow the operator to select from a list of valid scratch media.

Example 1

An example of the utility being executed on Windows:

```
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 processing this job loads the appropriate scratch media into the specified drive.

Example 2

The following examples show how to modify Omniback/Data Protector backup mount requests to present them as mount request jobs in Media Operations. This is accomplished by modifying the Omniback/Data Protector mount script (`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.

Windows: `mount.bat`

```
.@echo off
set THIS=%0
set USER=%1
set GROUP=%27
set HOSTNAME=%3
set DEVNAME=%5
set DEVHOST=%6
set DEVFILE=%7
set DEVCLSS=%8
set DEVCLASSNAME=%9
shift
shift
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 <MO Server username> -p <MO Server password>
done
```

UNIX: `mount.sh`

```
#!/sbin/sh
THIS=${0}USER=${1}  # unix login of user who started the backup
GROUP=${2}          # unix group of user who started the backup
HOSTNAME=${3}       # host where the backup was started
STARTPID=${4}       # pid of the backup process
DEVNAME=${5}        # logical device that generated mount request
DEVHOST=${6}        # host to which the device is attached
DEVFILE=${7}        # pathname of the physical device
DEVCLASS=${8}       # device type number
DEVCLASSNAME=${9}   # device type name
shift 9;
MEDID=${1}          # medium id of the reqested medium
MEDLABEL=${2}       # label of the requested medium
MEDLOC=${3}         # location of the requested medium
POOLNAME=${4}       # pool name to which requested medium belongs
POLICY=${5}         # media allocation policy
MEDCLASS=${6}       # media type number
MEDCLASSNAME=${7}   # media type name
SESSIONKEY=${8}     # sessionkey of the running session
MOSERVER="motestserver"
CELLSERVER="dptestserver"
MOUSER="test"
MOPWD="test"
JAVACMD="/opt/java/bin/java"
RCTMOUNT_JAR="/opt/omni/bin/reactivemount.jar"

INFO=/tmp/media_info

if [ "X${MEDID}" != "X" ]
then
  /opt/omni/bin/omnimm -media_info ${MEDID} -detail >${INFO}
  type=`grep "type" ${INFO} | awk '{print $4}'`
  if [ "X${type}" = "XHASCOPY" ]
  then
    echo "The Medium has the following copies:" >${INFO}
    /opt/omni/bin/omnimm -list_copy ${MEDID} >>${INFO}
    cat $INFO | sed 's/Medium Label/LABEL/'|\
    sed 's/MediumID/ID/'|\
    sed 's/Pool Name/POOL/' >${INFO}.tmp
  else
     echo "" >${INFO}.tmp
  fi
fi

echo "
```

```
$USER.$GROUP@$HOSTNAME,
You are the owner of the Data Protector session that is now in a mount
request  state.  In  order  for  the  session  to  proceeed,  please
insert/load the following medium:  (If the names are empty, then any)
   LABEL:     \"$MEDLABEL\"
   LOCATION:  \"$MEDLOC\"
   CLASS:     \"$MEDCLASSNAME\"
   POOL:      \"$POOLNAME\"   WITH POLICY: $POLICY

into device:

   NAME:        $DEVNAME
   HOST:        $DEVHOST
   DRIVE/SLOT: $DEVFILE/$DEVICESLOT
   CLASS:       $DEVCLASSNAME

`cat $INFO.tmp`

Then confirm the mount  request.  This can be done with the command
omnimnt with the session key $SESSIONKEY or the GUI xomnimonitor.
This mail has been sent by the script $THIS,
run by Data Protector.
" | mailx -s 'Data Protector Mount Request' $USER@$HOSTNAME

$JAVACMD -cp $RCTMOUNT_JAR com.hp.ov.dm.reactivemount.DoReactiveMount
-m "$MOSERVER" -c "$CELLSERVER" -u "$MOUSER" -p "$MOPWD" -d "$DEVNAME"
-mp "$POOLNAME" -id "$SESSIONID"

exit 0
```

NOTE:

The `reactivemount.jar` file is available only in the MO server and client installation. You need to copy it to a suitable location on the UNIX cell server.

Bulk configuration file import

This bulk loads configuration data. It is accessed via the **Import** tab on the **Site Definition** window.

NOTE:

When importing the information, field values must be separated by commas. There must be no more than one record per line.

You can import the following information types:

- Data Center Grid Information

  Example:

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

- System Grid Locations

  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

  Example:

  ```
  Media,Location,Site,Vault,Slot,Vendor,
  AccountAB0001,Vault,Akron BLD 3,closet,,
  1AB0002,Vault,Akron BLD 3,closet,,
  1AB0003,Offsite,Akron BLD 3,,Vendor1,1000
  ```

  `Location` can take the values:

  ```
  Scratch
  Device (in a device)
  Vault
  Container
  Offsite
  Transit
  Holding (in the holding bin)
  Other
  ```

  `Slot` is in the format: `<cabinet>:<drawer>:<row>:<slot>`. It must be consistent with the vault configuration in Media Operations.

  Example: `CABINET1:1:2:04`

  An eighth parameter, `Container`, is only needed if you define 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, it is created automatically. The following is an example with the `Container` value:

```
Media,Location,Site,Vault,Slot,Vendor,Account,Container
AB0003,Offsite,Akron BLD3,,,Vendor1,10,Cont1
```

- Device Definitions

  Example:

  ```
  System,Device,Type,Media Type,Compressions
  lc1036.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 (media, not associated with any Backup Manager, such as legacy media already stored in offsite or vault locations). `Pool` is the name of a manual media pool created in Media Operations in this site to which you want to import the media.

NOTE:

You cannot import media into a media pool that has been imported from a backup manager.

Example:

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

When creating manual media through the import function, all media are created as scratch media, with their last used date set to the time when the import was performed. Therefore, if the vaulting policy for the manual pool to which these media belong has a minimum retention time set, the manual media will have the vaulting policies applied to them even though they are scratch media.

B Diagnostics and tuning

Overview

This appendix describes how to change logging levels for various Media Operations components to facilitate diagnostics. It also discusses product tuning.

The sections in this appendix are:

- “Media Operation logs” on page 155
- “XML Gateway configuration, logs, and tuning” on page 156
- “Data management communications” on page 159
- “Holiday list configuration” on page 162
- “Manager-of-Managers configuration” on page 162

Media Operations logs

Media Operations logs include the following:

- Media Operations Server logs located in `<Install_Location>\DBServer\log\...`

  Example: `C:\ProgramFiles\HP\DataMgt\MediaOps\DBServer\log\log.0.txt.`

- Media Operations Manager logs located in `<Install_Location>\Client\log\...`

  Example: `C:\ProgramFiles\HP\DataMgt\MediaOps\Client\log\log.0.txt.`

Logging level is adjustable under the Log Level tab on the Server Parameters window under **Global Configuration Options**. Only top-level administrators can access this information.

XML Gateway configuration, logs, and tuning

This section discusses the XML Gateways configuration, logging, and considerations for tuning the gateway.

Configuration

Depending on the system that hosts XML Gateway, you can adjust the settings that affect:

- performance
- logging for XML Gateway
- logging for Backup Managers
- cleanup of unclaimed XML reports and their locations
- timeouts that affect termination of locked Backup Manager jobs

Example XML Gateway configuration file

```
<XmlgwConfig>
   <ResultsFilesPath cleanUpMin = "15" keepFilesMin = "15">
      $ARCHIVELOCATION</ResultsFilesPath>   <Logging level = "SEVERE">
   <LogFilePath>$LOGFILEPATH</LogFilePath>
   <Threading reportThreads="5" actionsThreads="5"
   <BkmgrLogging level = "0" socketTimeOut = "15">xmlgw1_0.log
      </BkmgrLogging>
   </Logging>
   <Threading reportThreads="5" actionsThreads="5"
        actionTimeoutMin="5"/>
       <BackupManagerPollTimeFrame hours ="150"/>
</XmlgwConfig>
```

Cleanup

XML reports are generated by XML Gateway based on requests 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 server fails to collect the reports, 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, adjust the cleanup.

In the example configuration file above, `cleanUpMin ="15"` indicates the frequency (in minutes) of cleanup, and `keep FilesMin ="15"` specifies the minimum age of files to be removed. So, to run cleanup every hour and remove files older than 20 minutes, set `cleanUpMin="60"` and `keepFilesMin="20"`.

File locations

The value between `<ResultsFilesPath>` and `</ResultsFilesPath>` is the location to which XML files are written.

△ CAUTION:

Do not change the `ResultsFilesPath` value without consulting support, as your Media Operations Server will no longer be able to retrieve the requested XML.

`<LogFilePath>` 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.

Logging

`<BkmgrLogging>` allows you to change logging level, file name, and timeout used for the Backup Manager. Valid values for level are “0”, or “*X*”, where *X* is between 10-200. The text between the tags is the file name that Backup Manager should use when logging requests from the gateway.

`<socketTimeOut>` 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 for XML Gateway to complete a request when there is a problem with the Backup Manager.

Threading

XML Gateway processes multiple requests simultaneously by generating several threads per request. If the host supporting 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.

`actionTimeoutMin` is specifically used to timeout actions requested by the gateway, such as entering and ejecting media, library and drive scans, and initialization. If the Backup Manager does not respond to the request every few minutes at least, 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 actions on your libraries or devices take longer than `actionTimeoutMin`, increase the value. There are, however, some side effects. For example, when a medium is not in the CAP, but the Backup Manager is instructed to load it, some Backup Managers, such as Data Protector, 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. When all threads are used, all requests wait until one of the other requests is complete. If you increase `actionTimeoutMin`, it is recommended that you increase your threading level as well.

Polling

`<BackupManagerPollTimeFrame>` is used to produce media reports during the polling cycle. Based on this parameter value, full and incremental media reports are requested by the backup manager. Running a Media Report for the entire timeframe on the backup manager is time and resource consuming. By default, the parameter is set to 150 hours, but you can reduced it when the DP RDS utilization is very high or the media report takes too long to produce.

NOTE:

Do not set the parameter to zero unless you want to run media reports for the entire timeframe.

The XML Gateway uses the parameter to run media reports with optimized CPU utilization on the Data Protector Cell Manager. The value is not used while running media reports during manual synchronization.

Logs

To change the logging level of XML Gateway:

1. Open the `xmlgw_config` file on the XML Gateway host:
   - *Windows:*
     `<xmlgw_Install_Loc>\dpxmlgw\config\xmlgw_config`
   - *HP-UX, Linux 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 "Configuration" on page 156 for details.

Log levels

Log level settings for XML Gateway 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 causes large log files.

Kernel tuning for XML Gateway on HP-UX

If you installed XML Gateway on HP-UX, you may need to adjust one of the HP-UX kernel tunable parameters to ensure reliable operation of 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 has the kernel setting `max_thread_proc` set to the default of 64 threads per process, change it to at least 512, and then recompile the kernel. For further details, see http://www.hp.com/products1/unix/java/infolibrary/prog_guide/configuration.html

Data management communications

This section covers logging and tuning for the Data Management Communications module (DMComms).

Service logs

Changing the logging level

1. Open the communications configuration file on the DMComms host:
   - *Windows:*
     `<DMComms_Install_Location>\DMComms\config\bbc_config`
   - *HP-UX, Linux and Solaris:*
     `/etc/opt/hpdmcomms/config/bbc_config`
2. Change the `LOG_LEVEL` in the `[com.hp.ov.ipcserver]` section. 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. *Windows only:*
   You can change `LOG_LEVEL` in the `[com.hp.ov.ipcclient.rpc]` section. Valid settings are:

```
[com.hp.ov.dm.ipcclient.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
REQUEST_TIMEOUT=0
RESPONSE_TIMEOUT=0
SSL_KEYSTORE_FILENAME = REPLACE_WITH_SERVER.JKS
SSL_KEYSTORE_FORMAT = JKS
```

Log file locations

Windows:
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`

HP-UX, Linux and Solaris:
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

Default port numbers used by the Media Operations communications service are 25555 and 25556. All communications over the network between Media Operations components use an HTTPS/XML format. If you need to change the port numbers (for example, if another application uses the same port numbers), proceed as follows:

1. Go to the directory containing the communications configuration file (in the config directory of DMComms). The default installation location is:
   - *Windows:* `C:\Program`
   - *HP-UX, Linux and Solaris:* `/etc/opt/hpdmcomms/config`
2. Edit the `bbc_config` file to change the port settings. There are two port numbers, one for HTTP-based RPC communications, the other for 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. *UNIX only:* When changing the port numbers, reflect the 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
```

Holiday list configuration

Holiday Lists prevent Media Operations from starting jobs on holidays.

The Holiday List Configuration file is provided in XML format in the <MO_INstall_Dir>/DBServer folder. You can modify the file to exclude holidays when Media Operations schedules daily jobs.

Example:

The following example is in mm/dd/yy format:

```
<HolidayList>
<Holiday DATE="02/14/05"/>
<Holiday DATE="05/30/05"/>
<Holiday DATE="07/04/05"/>
<Holiday DATE="09/05/05"/>
<Holiday DATE="11/24/05"/>
<Holiday DATE="11/25/05"/>
<Holiday DATE="12/26/05"/>
</HolidayList>
```

Manager-of-Managers configuration

While adding the MoM server as backup manager in Media Operations, note the following:

- You do not need to add all the Backup Manager servers that are part of the MoM manually. If you add one server that is part of the MoM, the backup manager and all systems in its corresponding Media Management Database (MMDB) cluster are added automatically.
- Add the gateway server name manually. Do *not* select the option "Use Backup Manager as XML Gateway" when adding a backup manager that is part of MoM.

C Application managers

Overview

Media Operations supports the following Application Managers:

- HP Data Protector A.06.00, A.06.10, A.06.11 and A.06.20
- Symantec NetBackup Enterprise Server and Server v6.0

The following matrix provides an overview of functionality supported by Application Managers.

Table 4 Application matrix

	Scratch Init	Library Load/ Eject	Copy Support	Location Update	Mixed Pools	Media Subtype	Remote Gateway	Object Consolidation
Data Protector A.06.00, A.06.10, A.06.11, and A.06.20	Yes	Yes[2]	Yes	Yes	No	No	Yes	Yes
NetBackup Enterprise Server and Server v6.0	Yes[1]	Yes[2]	Yes[3]	Yes	Yes	No	No[4]	No

[1] In libraries, NetBackup does not support media initialization on demand. It moves media from a blank (default) pool to a target pool. However, NetBackup does support on-demand initialization on standalone devices.

[2] Library load and eject is only supported on barcoded libraries.

[3] Only the Inline Tape copy feature of NetBackup is supported.

[4] The Gateway must be installed on the NetBackup master server.

- **Scratch Init**: whether the Backup Manager application can initialize/format new scratch media. See "Initializing scratch media" on page 109 for details.
- **Load/Eject**: whether the Backup Manager can trigger loading/unloading of scratch media into/from libraries. See "Premount jobs" on page 89 for additional information.
- **Copy Support**: whether automated copy jobs are detected and therefore factored into premount calculations, and whether any copy-specific vaulting policies are applied to these media.
- **Location Update**: media location change in Media Operations is automatically copied back to the Backup Manager's media location.
- **Mixed Pools**: enables the Backup Manager application without a fixed media type for its pools to get media pools with a "mixed" media type. For example, DDS1 and DDS2 media are not considered mixed; DDS1 and LTO1 are. Note that mixed pools are excluded from Premount and Scratch Init.
- **Media Subtype**: whether the Backup Manager automatically configures the media compression type of pools. For applications that do not support automatic configuration of media subtype, you need to configure the media subtype in the GUI manually for each pool.

  Media subtype is determined by the majority of subtypes. For example, DDS pools contain DDS1, DDS2, and so on. If there are five DDS1 and ten DDS2, the compression is that of the DDS2.
- **Remote Gateway**: whether the gateway can communicate remotely over the network with the new Backup Manager. If it can, you can install it on any Backup Manager. If it cannot, it *must* be installed directly on the Backup Manager.
- **Consolidation Support**: whether consolidation jobs are detected and therefore factored into premount calculations, and whether any consolidation-specific vaulting policies are applied to these media..

Depending on which Backup Manager you are using, consider the following:

- With HP Data Protector, when performing load/eject operations for all silo-type library devices (such as ACSLS or DAS), the cartridge access port (CAP) must be set manually.
- With Symantec NetBackup, consider the following:
  - **Permissions:** The `/usr/openv/var/authorize.txt` file 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 consist 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 media initialization on demand. It moves media from a blank (default) pool to a target 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 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 NetBackup settings, you can change **Add Override** to `NONE` — multiple pools to scratch.

Glossary

access rights Permissions to perform specific tasks. Users have the access rights of the user class to which they belong.

automatically created media Media 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.

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 and full backup.

backup specification A list of objects to be backed up, together with backup options and devices to be used. The objects can be entire disks/volumes or parts of them, such as files, directories, or Windows NT Registry. File selection lists, such as include-lists and exclude-lists, can be specified.

blank media Media that are ready to be used.

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. Central control is available to administer backup and restore policies.

checkout request The means for obtaining tapes from vaults for file restore and disaster recovery.

COR *See* checkout request.

data expiry policy The time before the data on the media can be erased.

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.

disaster recovery A process that restores a client's main system disk to a state close to the time when a (full) backup was performed.

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.

enterprise cell manager *See* Manager of Managers (MoM).

event logs Files where Windows NT logs all events (such as start or stop of services, and log on and log off of the users).

full backup A backup in which all selected objects are backed up, whether or not they have been recently modified.

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.

Inline tape copy A feature of NetBackup 6.0 that allows you to create up to four backup copies simultaneously.

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 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.

log retention time The length of time the media audit logs are saved on the server.

Manager of Managers (MoM) 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.

media audit log Tracks every movement performed with each 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 condition factors The user-assigned age threshold and overwrite threshold used to assert the condition of a medium.

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”.

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.

overwrite A media condition factor defining how many times a medium can be rewritten and influencing when a medium becomes POOR.

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 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.

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. 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/enter.

scratch media 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 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 events occur. By setting up a schedule, you automate the start of your Media Operations.

security protocol A communications protocol that encrypts and decrypts a message for online transmission. Security protocols generally provide authentication.

session *See* backup session and restore session.

SLA service level agreement

slot 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.

time entered The time that you entered the request (automatically entered).

user rights *See* access rights.

vault An onsite or offsite storage location for removable media.

vaulting job Performs daily Media Operations 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.

Windows NT Registry A database repository about the computer's configuration.

Index