



Platter Management

Reference Guide

Includes:

Administration Guide

User Guide

Copyright

Information in this document is subject to change without notice. The software described in this document is furnished only under a separate license agreement and may be used or copied only according to the terms of such agreement. It is against the law to copy the software except as specifically allowed in the license agreement. This document or accompanying materials contains certain information which is confidential information of Hyland Software, Inc. and its affiliates, and which is subject to the confidentiality provisions agreed to by you.

All data, names, and formats used in this document's examples are fictitious unless noted otherwise. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright law, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Hyland Software, Inc. or one of its affiliates.

Hyland®, Hyland Software®, Hyland Healthcare, and Hyland product names are registered and/or unregistered trademarks of Hyland Software, Inc. and its affiliates in the United States and other countries. All other trademarks, service marks, trade names and products of other companies are the property of their respective owners.

© 2021 Hyland Software, Inc. and its affiliates. All rights reserved.

Document Name Platter Management
Department/Group Documentation
Revision Number Foundation EP5

OVERVIEW

Disk Groups, Volumes, and Platters	2
System Interaction	3
Encrypted Disk Groups	3
Export and Publishing	4
Storage Integration for EMC Centera	4
Storage Integration for IBM Tivoli	5
Integration for KOMpliance	5
Windows User Account Control Statement	5
Licensing	6

ADMINISTRATION GUIDE**CONFIGURATION**

User Groups and Rights	8
Product Rights	9
Configuration Rights	10
Global Client Settings	10
Disk Group Configuration	11
Disk Group Folders Share/NTFS Permissions	12
Client document retrieval only	12
Client document retrieval, with import and/or processing	12
Application Server	12
Creating and Editing Disk Groups	12
Configuring Disk Group Settings	16
Core Access to Disk Groups Using FTP	25
Configuring Disk Group Volume	26
Platter Name	27
Platter Type	27
Platter Paths	30
Host Server	31
Configuring Disk Group Volume Information	31
Configuring Disk Group Force Promote	34
Force Promoting All Disk Groups	36
Configuration Information Tree	39
Configuration Tree Dialog Box	41
Component Information	42
Disk Group Configuration	42
User Names & Passwords	43
Document Types	44
Keyword Type Configuration	45
Changing the Platter Search Order Across a Range of Volumes	45
Convert Existing Disk Groups to Centera or Tivoli	49

S3 DISK GROUPS

S3 Considerations	52
Migrating to an S3 Disk Group	52
Configuring an S3 Disk Group.....	53
Configuring an S3 Provider	56
Verifying an S3 Provider	58
Viewing S3 Volume Information	60
Forcing the Promotion of S3 Disk Groups	61
Configuring S3 Upload Cache Processing	62
S3 Disk Group Administration.....	63
Viewing S3 Disk Groups.....	64
Viewing the Status of S3 Buckets	64
Viewing the Status of Multipart Uploads	66
Multipart Upload Statuses	67
Abandoning Orphaned Files	68
Viewing Pending Uploads	68
Viewing Analysis Jobs	70
Viewing Completed Analysis Jobs.....	71
Viewing Files Needing Repair	72
Viewing Repaired Files.....	73
Multipart Uploads	74
KMS Encryption	77
Configuring KMS Encryption	77
Rotating the KMS Key	78
S3 Disk Group Analysis	79
S3 Disk Group Analysis Rules.....	79
Creating an S3 Disk Group Analysis Rule	80
Editing the Settings of an S3 Disk Group Analysis Rule	82
Running Analysis Jobs.....	84
Best Practices for S3 Disk Groups	85

ENCRYPTED DISK GROUPS

Overview	86
Requirements	86
Licensing.....	86
Upgrading	87
Third Party Software	87
System Interaction	87
Distributed Disk Services	87
Document Import Processor	87
Export and Publishing	88

Externally Filled Disk Group Copies	88
Foreign Disk Groups	88
Storage Integration for EMC Centera	88
Storage Integration for FileNet	88
Storage Integration for IBM Tivoli	88
Storage Integration for Third Party ECM Systems	88
Configuration	89
Configuring a New Disk Group as an Encrypted Disk Group	89
Maintenance	91
Backup Procedures	91
Key Encryption Key Rotation	91
Rotating the Key Encryption Key	92
Deploying the Rotated Key Encryption Key	96
Upgrading After Rotating the Key Encryption Key	97
Unencrypting an Encrypted Disk Group	98
Migrating an Existing Encrypted Disk Group to a Different Encryption Algorithm	99
 DISK GROUP MIGRATION	
Overview	100
Configuring a Disk Group Migration Job	100
Creating a Disk Group Migration Processing Task	104
Using the Disk Group Migration Window	105
Job Status Tab	105
Changing the Job Status	107
Failed Files Tab	107
 PLATTER MANAGEMENT UNITY SCHEDULER TASKS	
Creating a Task	110
Disk Group Analysis Processing	111
Platter Deletion Processing	112
S3 Upload Cache Processing	114
Disk Group Analysis Processing for S3 Disk Groups	114
Disk Group Migration Processing	114
System Tasks	115
Incomplete Commit Queue Processing	115
Incomplete Delete Queue Processing	115
 USER GUIDE	
 USAGE	
Usage	117

System ID File.....	117
Missing System ID Files	118
Mass Storage System ID Files	118
Managing Disk Groups and Queues.....	119
Platter Management Functions	121
Copy	122
Write	122
Compute Volume Size	122
Analyze or Analyze Source	122
Verify Access	122
Promote	122
Export	122
Export to DIP	123
Reset on Backup Queue	123
Add to Export Queue	123
Move	123
Manual Delete	123
Process	123
Incomplete Commit Queue Functions	124
Commit	124
Open Document	124
Properties	124
Computing Volume Size and Splitting Volumes	124
Computing Volume Size	125
Splitting a Volume	127
Analyze.....	129
Repairing Files During Analysis	131
Viewing Analysis Reports	132
Analysis Results	133
Analysis Rules	134
Verify Access	138
Platter Management Services	139
Analysis Jobs	140
Analysis History.....	141
Platter Deletion Jobs.....	143
Approving or Denying Deletion Jobs	145
Platter Deletion History.....	147
Generating a Platter Deletion Report	148
Customizing a Filter's Display	148
Resizing Columns	148
Moving Columns	149
Grouping Data	149
Promoting a Volume in the Client	150
Copying, Moving, and the Storage Migration Queue	152

Copying Volumes and Platters	152
Copying Volumes and Platters to CD/DVD	155
Moving Platters	155
Storage Migration.....	158
Enabling and Disabling Jobs in the Storage Migration Queue	159
Reviewing Jobs in the Storage Migration Queue	160
Scheduling Copy or Move Processes	161
Calendar	163
Default Daily Schedule	164
Selected Day	165
Backing Up Platters.....	166
Backup to CD or DVD	167
Automated Backup to Rimage	167
Reset on Backup Queue.....	168
Deleting Platters	169
Manually Deleting Platters from the Disk Group	169
Platter Deletion Rules	171
Additional Resources	173
Exporting Platters.....	173
Adding a Platter to the Export Queue	176
Viewing Document Locations.....	177
Unity Scheduler Tasks for Platter Management	179
Disk Group Analysis Tasks	179
Incomplete Commit Queue Processing Tasks.....	179
Incomplete Delete Queue Processing Tasks	180
Platter Deletion Processing Tasks	180
Troubleshooting	180
Disk Group Errors	180
Mount Disk	180
Platter Management Error	181
Disk Group Analysis	181
Unable to Make File Read-Only	181
 PLATTER MANAGEMENT BEST PRACTICES	
Usage	182
Copying Missing Files	182
Deleting Platters from the Disk Group	182
Exporting Platters to Disc	182
Document Retention and Records Management	183
Configuration	183
Disk Groups	183
Security	183
Disk Group Settings	184
Volume Size	184

Backup Copies	184
Maximum Number of Volumes	184
Volume Paths	184
Backfile Conversions	185
E-Forms Disk Groups	185
Upgrade Considerations	185
Platter Management Upgrade Considerations.....	185

Platter Management is the administration of the physical data files that contain your data. Platter management functions are used to maintain redundant copies of data within a Disk Group (the logical groupings of the individual physical files), and manage the migration of that data to long-term storage devices.

Using a logical interface to configure the Disk Groups where the data actually resides on the network, OnBase is able to locate, relocate, categorize, track, and perform specialized Platter Management functions on the data without losing data integrity.

The Platter Management manual provides information concerning the logic, configuration, and administration of the physical files in the OnBase system. Most Platter Management operations are performed in the OnBase Client. Platters can be backed up, copied, moved, deleted, or exported. Volume configuration can be modified through Disk Group management, in the Configuration module.

Disk Groups, Volumes, and Platters

A **Disk Group** is a physical storage location for copies of files added to OnBase. Disk Groups are configured to allow OnBase to track, categorize, and perform specialized maintenance functions. The size and location of the Disk Group's volumes are specified when the Disk Group is configured, along with the number of copies the Disk Group contains.

Note: Disk Groups and volumes are logical storage bins while platters are physical storage bins. Each physical copy of a volume is referred to as a platter.

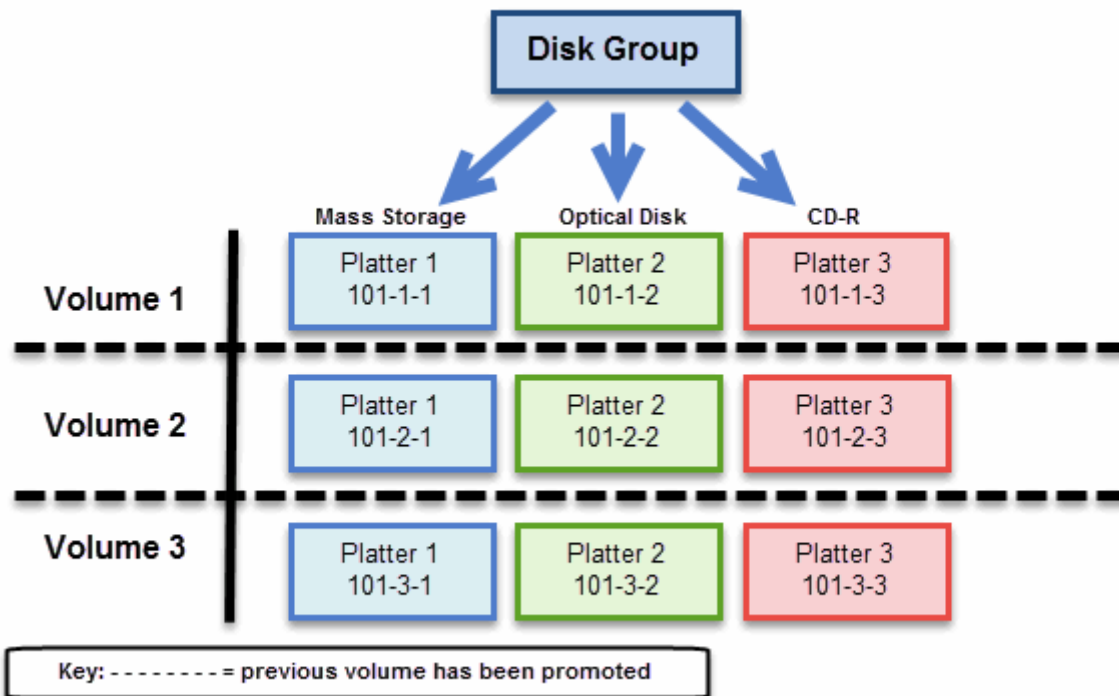
- A **volume** is the logical division for all of the copies of a Disk Group. Volumes consolidate data into discrete units. Using multiple volumes allows you to create blocks of data that can be easily tracked as well as moved near-line, off-line, and back.

You should set your volume size to the size of the smallest media that will be used to store this volume. In many cases a volume will eventually be backed up to a Compact Disc, which safely holds 500 MB. When set up in this way, volumes ensure that a complete set of document files can fit onto each storage media used by the Disk Group.

The process of creating a new volume is called **promoting** the volume. Volumes are promoted automatically by the system when the amount of data in the volume reaches the configured size of the volume, or manually using Platter Management. After a volume is promoted, the previous volume is closed and no additional files are stored in it (new files are written to the new volume that was created during promotion). Documents can be accessed from any online volume.

- A **platter** (or copy) is the physical storage location of the files in a single copy, which can be anywhere on the network. Platters can be created on different types of media, such as mass storage, CD, tape, or optical.

This figure illustrates Disk Group 101, which has three copies (platters) and has been promoted twice, creating three volumes. New documents are written to volume 3, until volume 3 is promoted to volume 4:



System Interaction

Platters can be backed up or exported to CD or DVD using the Export and Publishing module. The Encrypted Disk Groups module aids in securing your OnBase solution. Platters can also be converted for storage on several third-party storage systems, such as EMC Centera and IBM Tivoli.

Encrypted Disk Groups

The use of Encrypted Disk Groups helps organizations meet compliance regulations that surround the digital storage of documents, for example the processing, storing, and transmitting of sensitive financial information, such as credit card data.

The Encrypted Disk Groups module adds an additional layer of security to your OnBase solution that can be used separately or in conjunction with the other security practices employed by your organization. With Encrypted Disk Groups, the documents and images are encrypted using 128 or 256 bit AES (Advanced Encryption Standard) encryption at the physical storage level, protecting the data from unauthorized access to the physical drives. Documents that are archived in an Encrypted Disk Group can only be opened and viewed using the OnBase interface, ensuring that the security controls imposed by OnBase are respected at all times.

For complete details, see the **Encrypted Disk Groups** appendix in this module reference guide.

Export and Publishing

The Export and Publishing modules provide the ability to write OnBase files or systems to CD or DVD media.

- The Export module allows an OnBase user to create a database with only selected documents and all of their associated system information. This information may then be imported into another OnBase system, giving the other system access to the exported documents.
- The Publishing module produces the same export files and database, but adds a runtime Client to the collection of exported files. This allows the user receiving the published documents to view and retrieve those documents without having to import data, or even have access to an OnBase system at all. The published Client supports all of the document retrieval, double-click cross-referencing, text searching, printing to local printer, custom query, and enveloping functionality of the full Client module. It does not support full-text indexing, any type of document input option, or any of the administrative functions available in the full Client module, ensuring the integrity of your documents.
- The Encrypted Publishing module provides all of the functionality of the Publishing module, with the added feature of providing the ability to produce a CD or DVD with encrypted contents. This eliminates the ability for someone to casually browse the document files or database.

The following module reference guides are available for details on the suite of export and publishing modules:

- Automated CD and DVD Publishing
- Encrypted CD and DVD Publishing
- Export and Publishing

Storage Integration for EMC Centera

EMC Centera is a magnetic disk-based WORM storage system that offers added security and data integrity. Centera's software and hardware architecture produces unique identifiers for the data it stores. Specifically, Centera uses Content Addressing. Rather than accessing content from a standard file system, a 64-character identifier is used to save and retrieve documents. In that way, only the application can get access to the content. OnBase is able to use Centera for any Disk Group copy other than the first mass storage copy.

For complete details, see the separate **Storage Integration for EMC Centera** module reference guide.

Storage Integration for IBM Tivoli

IBM Tivoli is a software solution designed to allow network workstations to perform automatic and manual backups to virtual storage media. The virtual storage media is managed by a network server, Tivoli Storage Manager (TSM), and utilizes TCP/IP communications with the client software. This virtual storage media can be configured to create redundant copies of data files on any type of media. It also provides a file retention system. OnBase is able to use Tivoli for any Disk Group copy other than the first mass storage copy.

For complete details, see the separate **Storage Integration for IBM Tivoli** module reference guide.

Integration for KOMpliance

Caution: As of Foundation EP1, KOMpliance is no longer supported by OnBase.

Though previously supported in earlier versions of OnBase, KOMpliance servers are no longer supported as of Foundation EP1. If KOMpliance support is required, updating to this or later versions of OnBase is not possible.

Windows User Account Control Statement

Hyland Software is dedicated to ensuring that OnBase is compatible with Windows User Account Control (UAC). UAC is a feature of Windows operating systems that was introduced with Windows Vista. It limits the ability of standard users to make global system changes to a workstation and prevents malicious software from making unauthorized changes to protected areas.

For details on UAC, refer to your Microsoft support information or see [http://technet.microsoft.com/en-us/library/cc709691\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc709691(WS.10).aspx).

You may encounter UAC in OnBase when:

- Installing or uninstalling OnBase, OnBase modules, or OnBase ActiveX controls.
- Copying, moving, or saving files to the Program Files directory, Windows directory, or another protected location.
- Modifying system-wide settings, such as the registry.
- Re-indexing a document or opening a scanned batch using published Internet Explorer from a Remote Desktop Server.

If Windows UAC is enabled, the above operations may prompt for administrator privileges or credentials, even if an administrator is currently logged on.

Licensing

Most Platter Management is done from the OnBase Client, which requires a valid Client license.

Disk Group Configuration requires a valid Configuration license.

Exporting platters requires an Export license, and writing platters to CD or DVD requires additional valid licensing. Please see the Export and Publishing manual for the variety of export, publishing, and authoring licenses that are available, and how they are used.

To use Encrypted Disk Groups, a valid Encrypted Disk Groups database license is required.

Moving platters to EMC Centera or IBM Tivoli requires additional licensing for those storage solutions.

You can check your current licensing status in OnBase Configuration by selecting **Product Licensing** from the **Utils** menu.



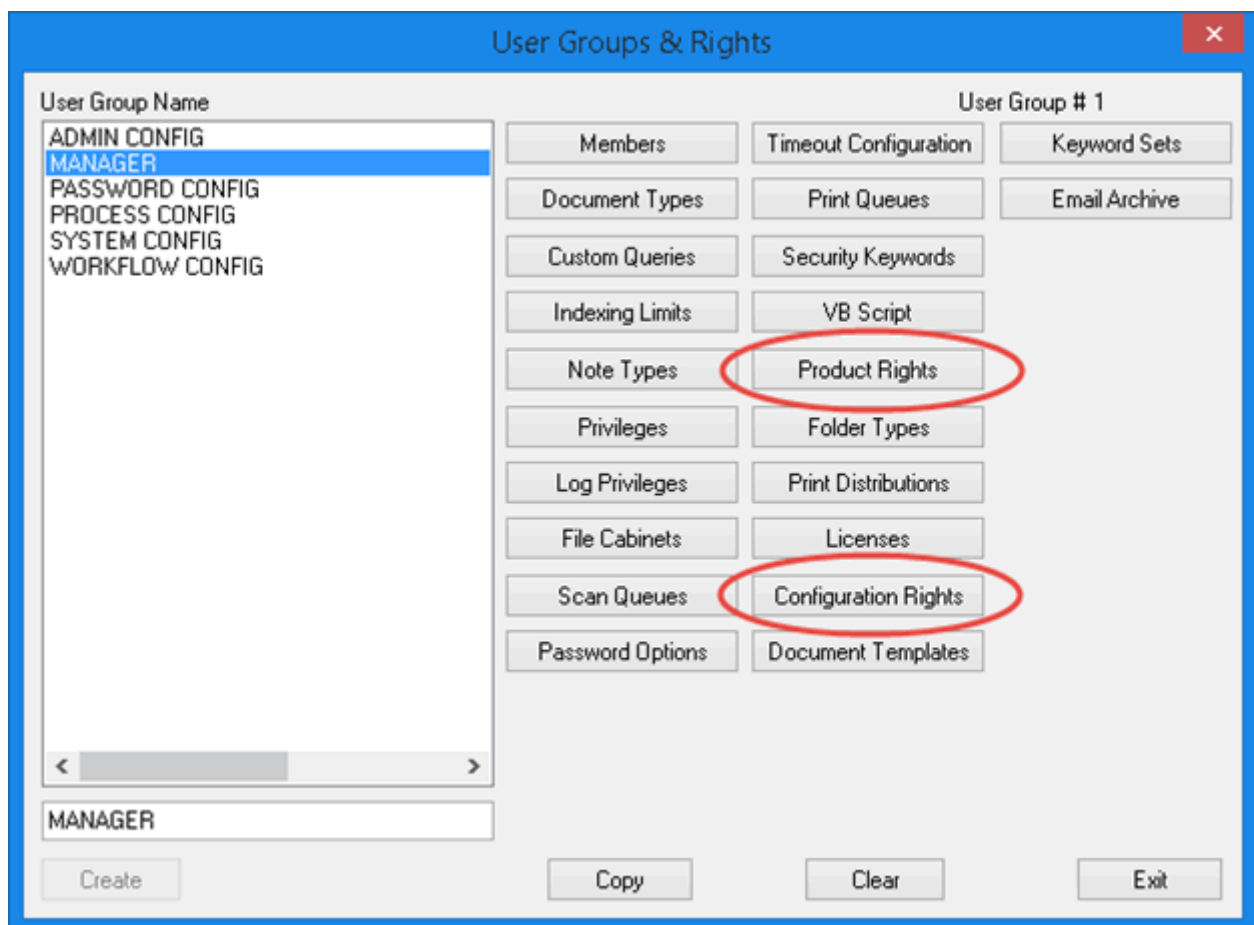
Platter Management

Administration Guide

User Groups and Rights

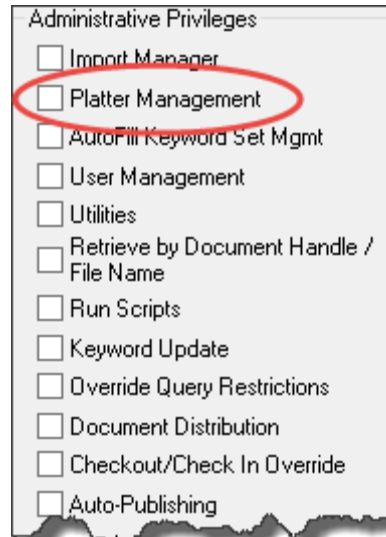
In order to perform Platter Management operations, User Groups need Product Rights to **Platter Management**. To configure Disk Groups, User Groups need **Disk Group Configuration** rights.

The **User Groups & Rights** dialog box is displayed in Configuration by selecting **Users | User Groups/Rights** from the menu bar.



Product Rights

Highlight the User Group and click on the **Product Rights** button. To allow User Groups to access Platter Management functions, for the purpose of performing either a **Backup** or **Copy** operation, select the **Platter Management** option listed under **Administrative Privileges**.



Configuration Rights

To access **Disk Mgmt** in the Configuration module, highlight the user group name, click the **Configuration Rights** button and select **Disk Group Configuration** under the **General Settings** tab.



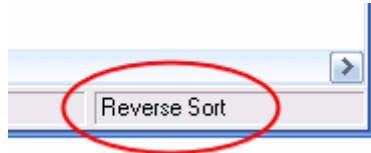
Global Client Settings

There are several Platter Management options available in the **Global Client Settings** dialog box. To configure these settings, select **User | Global Client Settings** in the Configuration module.

The options for Platter Management are located on the **Platter Management** tab of the **Global Client Settings** dialog.

Note: Depending on your licensing, some options may not be available.

Option	Description
Automatically analyze all backups	When this option is selected, immediately after they are completed, backups will be automatically analyzed.

Option	Description
Enable WORM compatibility	<p>Makes the OnBase.ID file writable, so that it does not trigger the WORM document retention. By default, this file is read only.</p> <p>You must re-launch Configuration prior to creating or promoting Disk Groups for this setting to take effect.</p>
Reverse sort Platter Management window volumes	<p>Reverses the order of the volumes listed in the Client Platter Management dialog, such that volumes are listed from the highest to lowest volume number.</p> <p>This also creates the Reverse Sort option in the bottom right-hand corner of the Platter Management dialog:</p>  <p>Double-click it to reverse the current sort order of volumes in the Platter Management dialog.</p>
Enable generation of deleted file reports (for 3rd party backup systems)	<p>This setting enables the Deleted Disk Group Files report under the Report menu in the OnBase Configuration module.</p> <p>Select this option to create a report containing the full paths to all copies of all files deleted from the Disk Groups. The report is stored in OnBase as Deleted Files under the SYS - Platter Management Reports Document Type.</p>
Enable multi-threaded Centera backups	<p>Enables multi-threaded backups when OnBase is writing a backup copy to a Centera device. This results in an improvement in write performance.</p> <hr/> <p>Note: This option requires the Storage Integration for EMC Centera license.</p> <hr/>

Disk Group Configuration

Disk Groups can be configured or modified in the OnBase Configuration module, through the **Disk Group Configuration** dialog, accessed from the **Disk Mgmt | Disk Groups** menu option.

Disk Group Folders Share/NTFS Permissions

In order for users to be able to access the Disk Groups from OnBase, the Disk Group folders must be set with certain share/NTFS permissions, depending on a user's level of access. It is a best practice to give users or User Groups the minimum level of access required to perform the OnBase functions expected of them. In this way, if a user is able to access the Disk Group folders outside of OnBase, that user may be prevented from manually performing actions not granted in OnBase, such as editing documents.

Caution: Documents should not be edited, moved, copied, deleted, or otherwise managed in the physical Disk Group folder without using the OnBase interfaces. The OnBase clients and Configuration module provide the ability to fully manage documents stored in OnBase, as well as providing additional security, disk management, and backup benefits.

Note: Refer to the **Encrypted Disk Groups** or **Distributed Disk Services** documentation for information on how to better secure files accessed outside of OnBase.

Client document retrieval only

- Share permissions: **Read**.
- NTFS permissions: **Read & Execute** (which includes **List Folder Contents** and **Read**).

Client document retrieval, with import and/or processing

- Share permissions: **Change**.
- NTFS permissions: **Modify** (which includes **Read & Execute**, **List Folder Contents**, **Read**, and **Write**).

Application Server

The Application Server domain account configured to access the Disk Group requires the following permissions.

- Share permissions: **Change**.
- NTFS permissions: **Modify**.

If impersonation is enabled on the Application Server, then the impersonation account requires these permissions. If impersonation is not enabled, then the identity account running the Application Server's application pool requires these permissions.

Creating and Editing Disk Groups

A **Disk Group** is a logical storage area for documents and data. All data that is added to OnBase must be referenced from a Disk Group. This allows OnBase to track, categorize, and perform specialized maintenance functions on the data.

When Disk Groups are created, the number of copies of the data that will be maintained for the Disk Group, as well as a size of the volumes, is configured. When the configured size of a volume is reached, a new volume is created for the Disk Group.

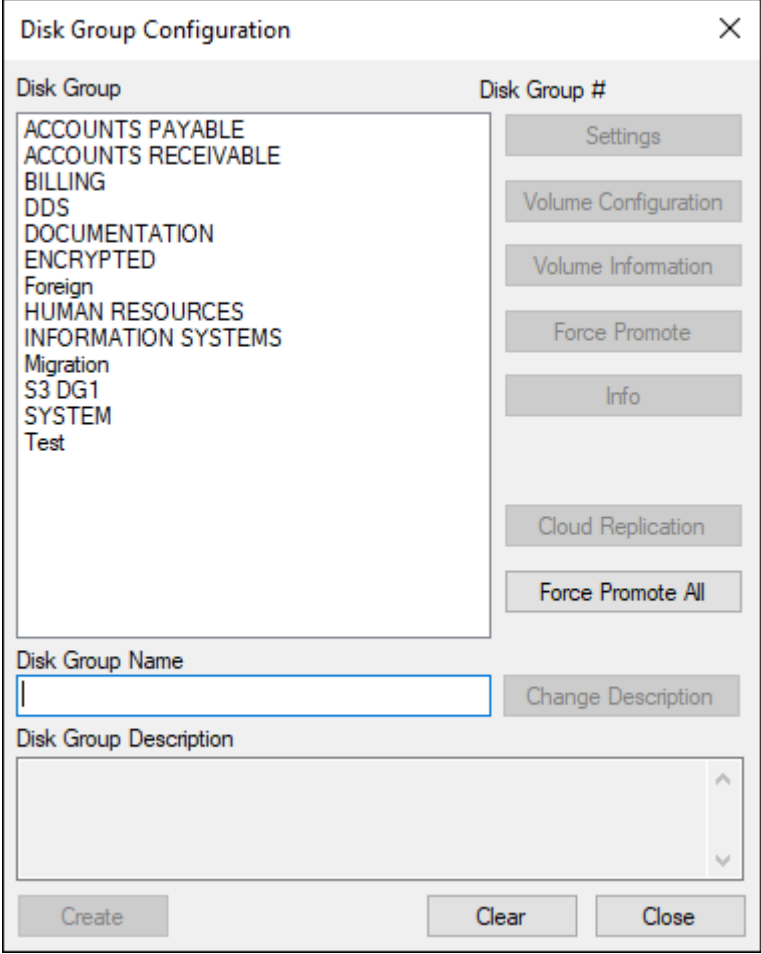
A **Volume** is the logical division for all of the copies associated with a Disk Group. The process of creating a new volume is referred to as **promoting** the volume. Volumes can also be promoted manually, using the **Platter Management** functionality.

A **Platter** refers to the physical location of the files, which can be anywhere on the network. It is recommended that you configure each Disk Group with at least two copies stored on different platters, each in a different location, to protect against data loss.

Note: When editing disk groups, the disk group may need to be locked. This prevents other users of the Client and Configuration from importing additional files to the disk group. However, users of the Unity Client can still import files to the disk group.

To Create a Disk Group:

1. In the Configuration module, select **Disk Mgmt | Disk Groups**. The **Disk Group Configuration** dialog box displays.



The **Disk Group Configuration** dialog box is shown. It features a list of disk groups on the left and a series of configuration buttons on the right. The list includes: ACCOUNTS PAYABLE, ACCOUNTS RECEIVABLE, BILLING, DDS, DOCUMENTATION, ENCRYPTED, Foreign, HUMAN RESOURCES, INFORMATION SYSTEMS, Migration, S3 DG1, SYSTEM, and Test. The buttons on the right are: Settings, Volume Configuration, Volume Information, Force Promote, Info, Cloud Replication, Force Promote All, Change Description, and a large text area for the Disk Group Description. At the bottom are buttons for Create, Clear, and Close.

Disk Group	Disk Group #
ACCOUNTS PAYABLE	
ACCOUNTS RECEIVABLE	
BILLING	
DDS	
DOCUMENTATION	
ENCRYPTED	
Foreign	
HUMAN RESOURCES	
INFORMATION SYSTEMS	
Migration	
S3 DG1	
SYSTEM	
Test	

Buttons: Settings, Volume Configuration, Volume Information, Force Promote, Info, Cloud Replication, Force Promote All, Change Description

Fields: Disk Group Name, Disk Group Description

Buttons: Create, Clear, Close

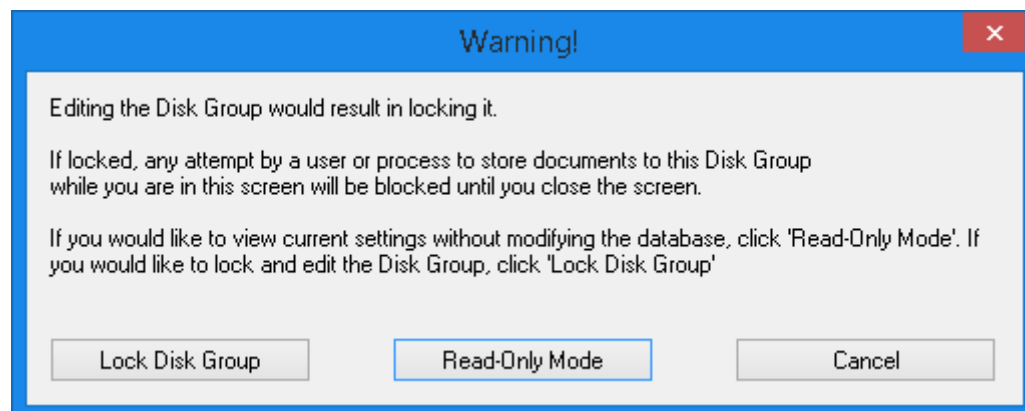
2. If creating a new Disk Group, type the name of the new Disk Group in the **Disk Group Name** field and click **Create**. The **Disk Group Type** dialog box is displayed. Select the type of Disk Group you are creating and click **Next**. The **Settings** dialog box for that type of Disk Group is displayed.

If editing an existing Disk Group, select an existing Disk Group from the **Disk Group** field.

3. Configure settings for the Disk Group using the parameters accessed via the **Settings**, **Volume Configuration**, **Volume Information**, and **Force Promote** buttons.

To rename an existing Disk Group, double click the name of the desired Disk Group.

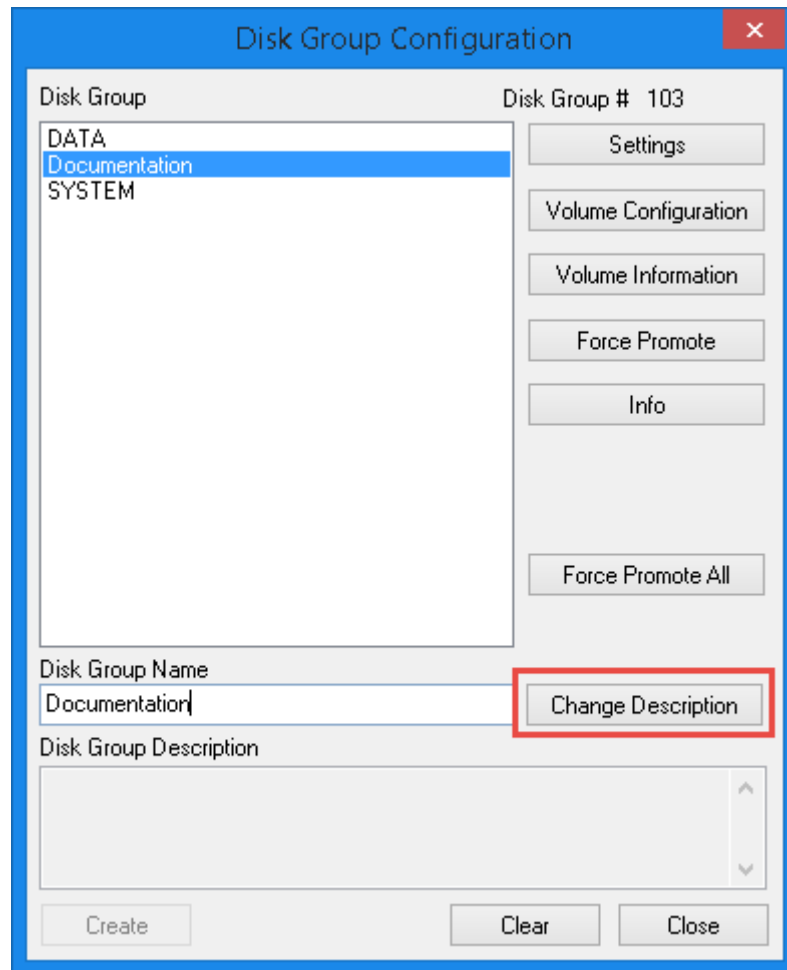
When any of these buttons are clicked after the Disk Group has already been created, the following warning is displayed:



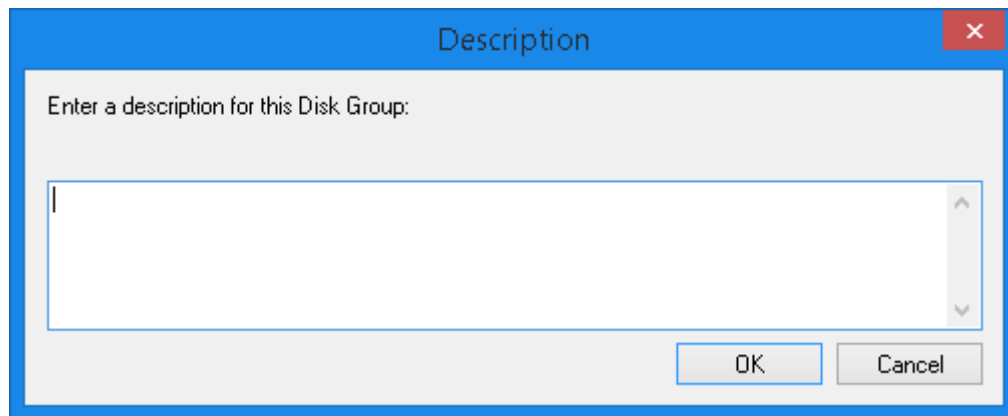
If you want to make changes to the Disk Group, select **Lock Disk Group**.

If you want to view Disk Group settings without making changes, click **Read-Only Mode**. This allows you to view Disk Group information, but no changes can be saved.

4. If you would like to change or add a description for the Disk Group, click the **Change Description** button on the **Disk Group Configuration** dialog box:



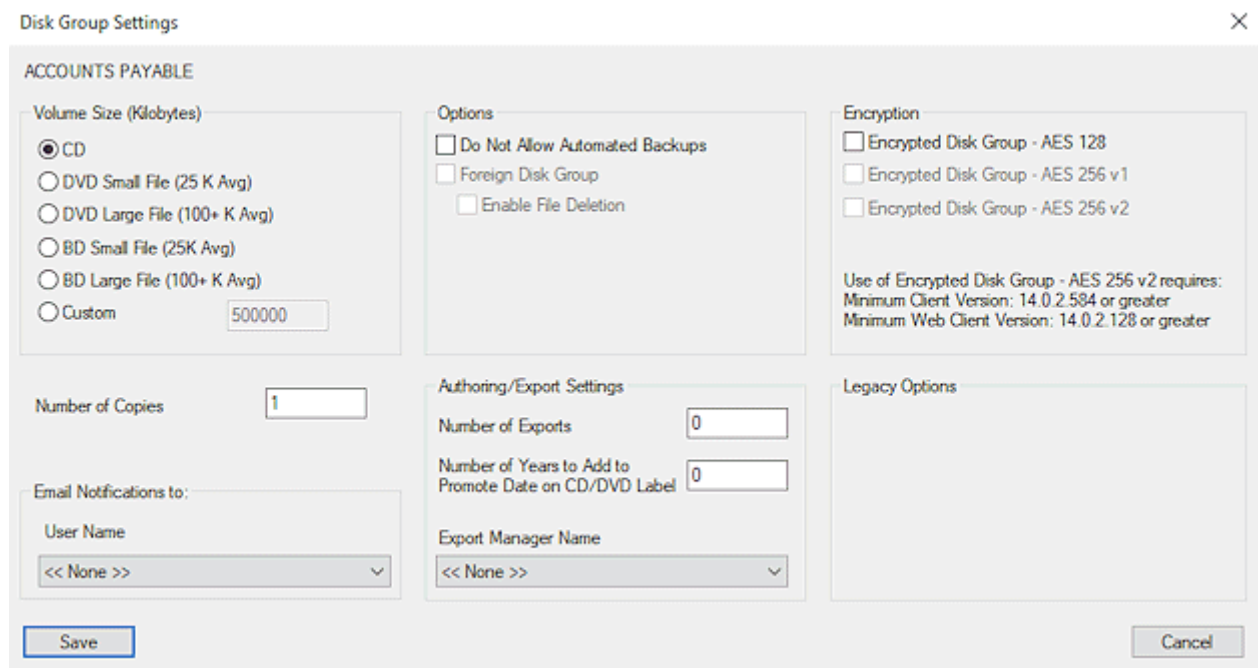
5. The **Description** dialog box opens:

A dialog box titled "Description" with a blue header bar and a red close button. The main area is light gray and contains the text "Enter a description for this Disk Group:" above a large, empty text input field. At the bottom right are "OK" and "Cancel" buttons.

Enter any comments or descriptions and click **OK** to apply the changes and to close the **Description** dialog box. The description is updated in the **Disk Group Configuration** dialog box.

Configuring Disk Group Settings

The **Disk Group Settings** dialog box lets you specify the size of the volume and the number of copies of data to maintain for each volume and can be accessed by selecting **Disk Mgmt | Disk Groups** in the Configuration module and clicking **Settings**. Settings specific to Export, Foreign, and Externally Filled copies are also configured at this dialog box.

A complex dialog box titled "Disk Group Settings" with a close button. It is divided into several sections. The "ACCOUNTS PAYABLE" section at the top left contains a "Volume Size (Kilobytes)" group with radio buttons for "CD", "DVD Small File (25 K Avg)", "DVD Large File (100+ K Avg)", "BD Small File (25K Avg)", "BD Large File (100+ K Avg)", and "Custom" (with a text input field showing "500000"). Below this is a "Number of Copies" text input field showing "1". The "Options" section in the middle left has checkboxes for "Do Not Allow Automated Backups", "Foreign Disk Group", and "Enable File Deletion". The "Encryption" section in the middle right has checkboxes for "Encrypted Disk Group - AES 128", "Encrypted Disk Group - AES 256 v1", and "Encrypted Disk Group - AES 256 v2", with a note below stating "Use of Encrypted Disk Group - AES 256 v2 requires: Minimum Client Version: 14.0.2.584 or greater, Minimum Web Client Version: 14.0.2.128 or greater". The "Authoring/Export Settings" section in the bottom middle has text input fields for "Number of Exports" (showing "0") and "Number of Years to Add to Promote Date on CD/DVD Label" (showing "0"), and a dropdown for "Export Manager Name" (showing "<< None >>"). The "Email Notifications to:" section in the bottom left has a dropdown for "User Name" (showing "<< None >>"). A "Legacy Options" section is empty on the bottom right. "Save" and "Cancel" buttons are at the bottom.

To specify settings for the Disk Group:

1. Select the size to be reserved for the volume in the **Volume Size (kilobytes)** section. The **Volume Size (kilobytes)** should equal the size of the smallest media that will be used for data files in the Disk Group and can be one of the following sizes:
 - **CD:** Select **CD** if you will be using CDs to back up the volumes of this Disk Group. This automatically sets the size of the volume to 500,000 kilobytes.
 - **DVD Small File (25 K Avg):** Select **DVD Small File** if you will be using DVDs to back up the volumes of this Disk Group. This setting assumes an average file size of 25 kilobytes and presets the total size of the volume to 3.8 gigabytes. The total volume size is preset by the system and cannot be modified.
 - **DVD Large File (100+ K Avg):** Select **DVD Large File** if you will be using DVDs to back up the volumes of this Disk Group. This setting assumes an average file size of 100 kilobytes or more and presets the total size of the volume to 4.0 gigabytes. The total volume size is preset by the system and cannot be modified.
 - **BD Small File (25 K Avg):** Select **BD Small File** if you will be using Blu-Ray Discs to back up the volumes of this Disk Group. This setting assumes an average file size of 25 kilobytes and presets the total size of the volume to 22.6 gigabytes. The total volume size is preset by the system and cannot be modified.
 - **BD Large File (100+ K Avg):** Select **BD Large File** if you will be using Blu-Ray Discs to back up the volumes of this Disk Group. This setting assumes an average file size of 100 kilobytes or more and presets the total size of the volume to 24.0 gigabytes. The total volume size is preset by the system and cannot be modified.
 - **Custom:** Select **Custom** to enter a specific total volume size, then enter the size in kilobytes in the data entry field. When configuring a custom size, the general rule for Disk Group volume size is to take the maximum amount of space on the media and subtract enough space to account for file-system overhead. The amount of space to reserve for overhead varies based on the media. For example, a 640 MB CD should be configured for a custom volume size of **500000** (500,000 kilobytes).

Caution: It is critical that the absolute limit of the media is not used for the volume size. Keep in mind that space is required on the media for the file allocation table. If the media has a set block size, multiple small files could actually take up more space. This could cause issues when going from one block-size media to another. Scanning also poses special considerations when computing volume size. Scanning always finishes a batch in whatever volume it started in, regardless of the volume size.

2. Enter the **Number of Copies** (physical platters) of data to maintain for each volume. Every Disk Group must have at least one copy, and that copy must be Mass Storage. Mass Storage uses online storage, such as a hard drive or RAID.
With the exception of a Foreign Disk Group, the remaining number of copies can be assigned in any combination of Mass Storage, Removable Media, Backup, or Externally Filled copies. Foreign Disk Groups are restricted to Backup copies only. The Disk Group type is configured later in this process.

3. Select a user from the **User Name** drop-down list under **Email Notifications to:**. The user selected will be sent email notifications concerning Disk Groups, such as Disk Group volume promotion.

Note: Ensure that the user you select is assigned an email address in the **User Settings** dialog box. In addition, in order for this feature to be functional, E-mail and Fax Distribution Service must be installed.

4. If your workstation has a license for **Automated CD Authoring** or **Automated DVD Authoring**, any copy that appears in the Backup Queue or Export Queue will be automatically backed up or exported to the configured CD-R or DVD-R. If you do not want a platter automatically backed up, select the **Do Not Allow Automated Backups** check box.
5. The **Foreign Disk Group** check box is used when referencing files in a storage area not created by OnBase. Instead of processing these files and moving them into a Disk Group, only the index information and a simple reference to the file location is stored. This allows access to the files, without actually having to move them to a Disk Group location.
6. Select the **Enable File Deletion** check box to allow OnBase to delete the physical files stored in Foreign Disk Groups as needed. This option is only selectable after the Foreign Disk Group has been created. All batches associated with the Disk Group must be committed before enabling deletion.

Note: All batches in the Foreign Disk Group must be committed before file deletion can be enabled for that Disk Group.

Caution: Enabling file deletion for a Foreign Disk Group will prevent new files from being imported. This setting cannot be disabled once it is saved.

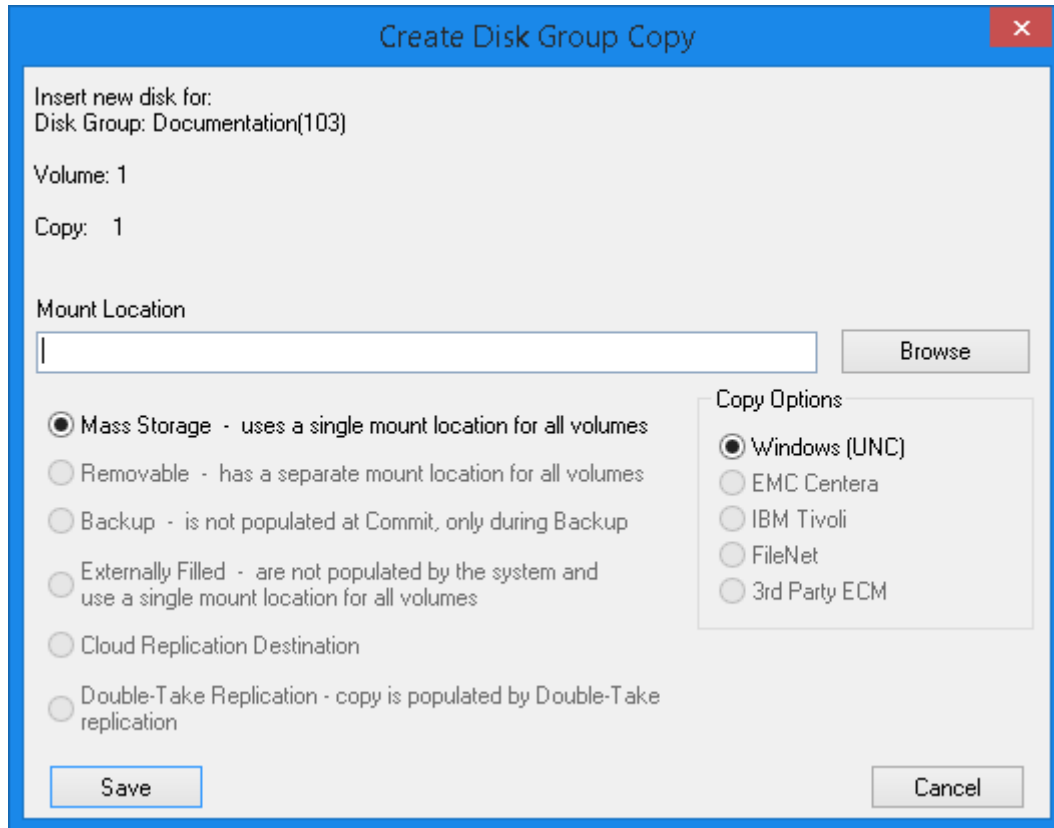
7. The **Encrypted Disk Group** options are only available if the database is licensed for Encrypted Disk Groups. See the **Encrypted Disk Groups** chapter in the **Platter Management** module reference guide for complete details regarding this option.
8. The **Number of Exports** designates the number of copies that will be made of the volume when it is exported from the **Platter Management** window in OnBase (Export module required). If an Export copy is specified for a Disk Group, filled volumes will automatically appear in the **Export Queue** of the **Platter Management** window, and you can perform the exports directly from this queue.
If you will not be exporting the data directly from the Disk Groups, then set this value to **0**. Although Export copies will not be created in Platter Management, documents can still be exported on an individual basis from the **Document Retrieval** dialog box.
9. The **Number of Years to Add to Promote Date on CD/DVD Label** is used to calculate the disposition date of the backup copy, for use with merge fields in Automated CD/DVD Authoring. If you will not be using this functionality, then this value can be set to **0**.

10. If your workstation has a license for **Automated CD Authoring** or **Automated DVD Authoring**, any copy that appears in the Backup Queue or Export Queue will be automatically backed up or exported to the configured CD-R or DVD-R. For export functions, the manner in which export will proceed is determined by the **Export Manager Name** specified. The **Export Manager Name** references an **Export Format** (that in turn identifies the predefined file system foldering structure that has been created for the exported data).

Note: Currently, automated backups and exports can only be performed with a Rimage™ Unit.

11. Click **Save**. The new Disk Group is added to the **Disk Group** list.

With the exception of Foreign Disk Groups, the **Create Disk Group Copy** dialog box is displayed and allows you to specify the path and copy type for each copy of the Disk Group. If a Foreign Disk Group was created, the **Alias ID File Name** must be entered manually at the **Volume Information** dialog box.



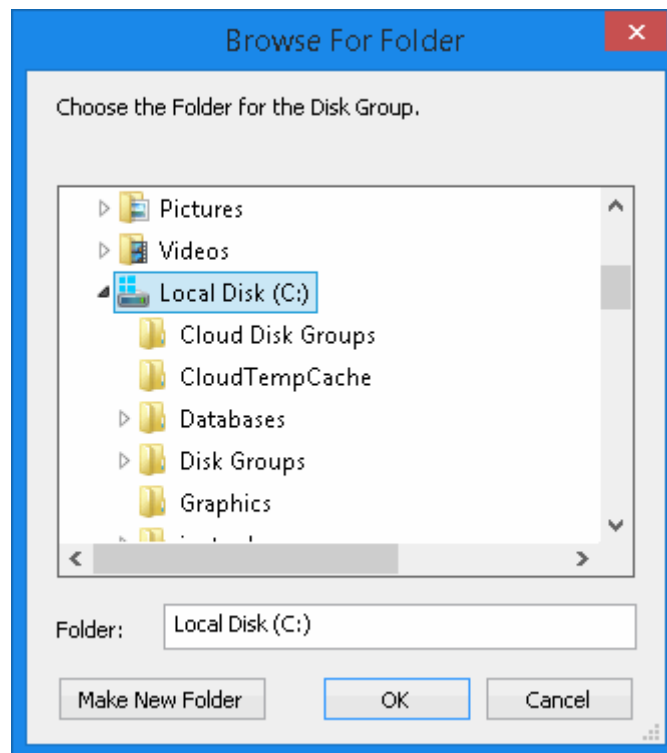
Note: The **Create Disk Group Copy** dialog box is displayed once for each copy and must be completed each time to configure each copy. It is often helpful to create your backup copies last so that they always appear as a group after all of the other copies.

This dialog box also contains information on the Disk Group name, the unique system-generated Disk Group ID number (in parentheses after the Disk Group name), the volume number, and the copy number. The system-generated Disk Group ID number is also displayed above **Settings** in the **Disk Group Configuration** dialog box.

12. Enter the path to the copy in the **Mount Location** data entry field, or click **Browse** and navigate to the location.

Note: Backup copies do not require a path. Select **Backup** as the copy type to complete the configuration.

If **Browse** is clicked, the **Browse for Folder** dialog box is displayed. Navigate to the location for the Disk Group then click **OK**. To create a new folder for the Disk Group, click **Make New Folder** and enter a folder name.



Mount Location Format	Description
Drive Letter e.g., F:\central\data\hr	Specifies a drive letter location for the data file storage. This drive letter must be valid and mapped to the same location for everyone using the system. Users without the appropriate mapping will be unable to retrieve the information.

Mount Location Format	Description
UNC Path e.g., \\server1\central\data\hr	<p>UNC is the preferred method of assigning the path to the Disk Group copy because it is valid for all users and does not necessitate the assigning of drive letters.</p> <p>If you do not want users to know the path to the Disk Group, you must use a hidden share. This is accomplished by creating a share with a share name ending with a \$ character. The hidden share must directly follow the computer name. In configuration, you must specify the \$ in the share path.</p> <p>Example: \\computername\share\$diskgroup1.</p> <p>In OnBase, when a user accesses the properties of a document, the computer name and share name are replaced with \\UNCSHARE.</p> <p>Example: \\UNCSHARE\diskgroup1\V1\1\9264.img</p>
FTP e.g., \\FTP:\marvin:delvin\\ftpserver\:21	<p>Allows for the specification of an FTP location and the login and password to gain access to the location. The login and password are stored internally, so that the system can provide them when processing or retrieving. When using an FTP location, the system will connect to the location and cache the retrieved files locally. When OnBase is exited, the files are removed.</p> <p>The FTP location must be in the following format: \\FTP:\username:password\\servername\:port \\pathelement1\pathelement2\pathelement3...</p> <p>After creating the Disk Group copy location, the system will replace the password with <pwd> whenever the location displays. See also, Core Access to Disk Groups Using FTP on page 25.</p> <hr/> <p>Note: When using Kofax or TWAIN interfaces to bring documents into OnBase, an FTP path cannot be used for a first copy in a Disk Group.</p> <hr/>

Mount Location Format	Description
Ascent™	<p>This option is used in conjunction with an Ascent server. Enter \\ASC: in the Path to Disk Group field. The system automatically requests information from the Ascent server and retrieves it. This Ascent location can only be used with a Foreign copy from a Foreign Disk Group. The system can only read files from this copy. It cannot process to it. This copy also requires the Ascent Client be installed on the machine as well as the Ascent Storage API configuration utility. Additionally, all workstations accessing the information must have the ascentget.dll file installed on the PC.</p> <hr/> <p>Note: When using Kofax or TWAIN interfaces to bring documents into OnBase, and Ascent path cannot be used for a first copy in a Disk Group.</p> <hr/>

Note: Documents should not be edited, moved, copied, deleted, or otherwise managed in the physical Disk Group folder without using the OnBase interfaces. The OnBase clients and Configuration module provide the ability to fully manage documents stored in OnBase, as well as providing additional security, disk management, and backup benefits.

13. Select the type for each copy.

Note: The first copy must always be a **Mass Storage** copy. If you attempt to assign a different type, an error message is displayed. Secondary copies can be designated as any of the available types. It is often helpful to create your backup copies last so that they always appear as a group after all of the other copies.

Device Type	Description
Mass Storage	If the location of this platter is a mass storage device, such as a hard drive, type the path to the correct location for this copy in the Path to Disk Group field and click Mass Storage . If you are unsure of the exact location for the copy, click Browse and use the standard Windows Open dialog box to locate the drive. Click OK in the Open dialog box to enter the mass storage location path.
Removable	When saving to Removable media (i.e. WORM), you should create a label for the removable media cover with the Disk Group name, Disk Group number, volume number and copy number information that is on the Insert New Disk dialog box. Of these values, only the volume number will change as new volumes will be created when the previous volume fills to capacity. Insert the formatted media into the drive and type the correct path to the removable media into the Path to Disk Group field. Click Removable .
Backup	<p>When you are designating a backup copy, click Backup without entering a path location into the Path to Disk Group field. When you back up the volume, you will enter the location for the backup copy.</p> <hr/> <p>Note: For systems using Automated Backup with Rimage, you can configure an automated backup that creates multiple copies from one configured backup using the [Rimage] onbase32.ini setting BackupCopies. Configure just one backup copy in Disk Group Settings Configuration, and set the onbase32.ini file setting BackupCopies=[number of desired copies].</p> <hr/> <p>For example, if you want to create 3 copies of the same backup file, change the onbase32.ini setting as follows:</p> <p>[Rimage] BackupCopies=3</p>

Device Type	Description
Externally Filled	<p>An Externally Filled copy is reserved for use by a system administrator. Data redundancy will not be managed for this copy by Platter Management. Specifically, data processed into the Mass Storage copy of the Disk Group will not be placed into the Externally Filled copy upon commit. Data can only be placed in the Externally Filled copy by manually copying the desired data files via the tools available from the file system (Explorer, etc.).</p> <hr/> <p>Note: Externally filling a copy should only be performed when the selective copying of data cannot be readily performed using the Platter Management functions available through OnBase. To ensure that the manual copying of data does not exclude any committed (critical) data, externally filling a copy is recommended only after promoting the volume that contains the data to be externally filled.</p> <hr/>

Note: If two or more Disk Group copies are configured, then committing documents copies the files to each of the Disk Group copies configured as Mass Storage or Removable. Files are not copied to secondary Disk Group copies that are configured as Backup or Externally Filled copies when a commit is performed, but are copied to Backup Disk Group copies when a backup is performed.

14. Select the **Copy Option** that corresponds to device configured in the Mount Location. **Windows (UNC)** is selected by default and is typically the option that is required. Depending on the configuration of your system, some Copy Options may not be available.
The only valid **Copy Option** for the first Mass Storage copy is **Windows (UNC)**. When the copy type is changed, the **Copy Option** is reset to the default value.
15. Click **Save** at the **Create Disk Group Copy** dialog box.

Note: The **Create Disk Group Copy** dialog box is displayed once for each copy and must be completed each time to configure each copy.

Core Access to Disk Groups Using FTP

Only the OnBase Client can access Disk Groups using FTP. In order to allow the OnBase Core (which includes the OnBase Web Client and Unity Client) to access FTP Disk Groups, an alias must be set up in the Application Server's web.config file.

To create an alias for the Core to access FTP Disk Groups:

1. Open the Application Server's **web.config** file in a plain-text editor, such as Notepad. In a default installation, this file is located at **C:\inetpub\wwwroot\AppServer**.

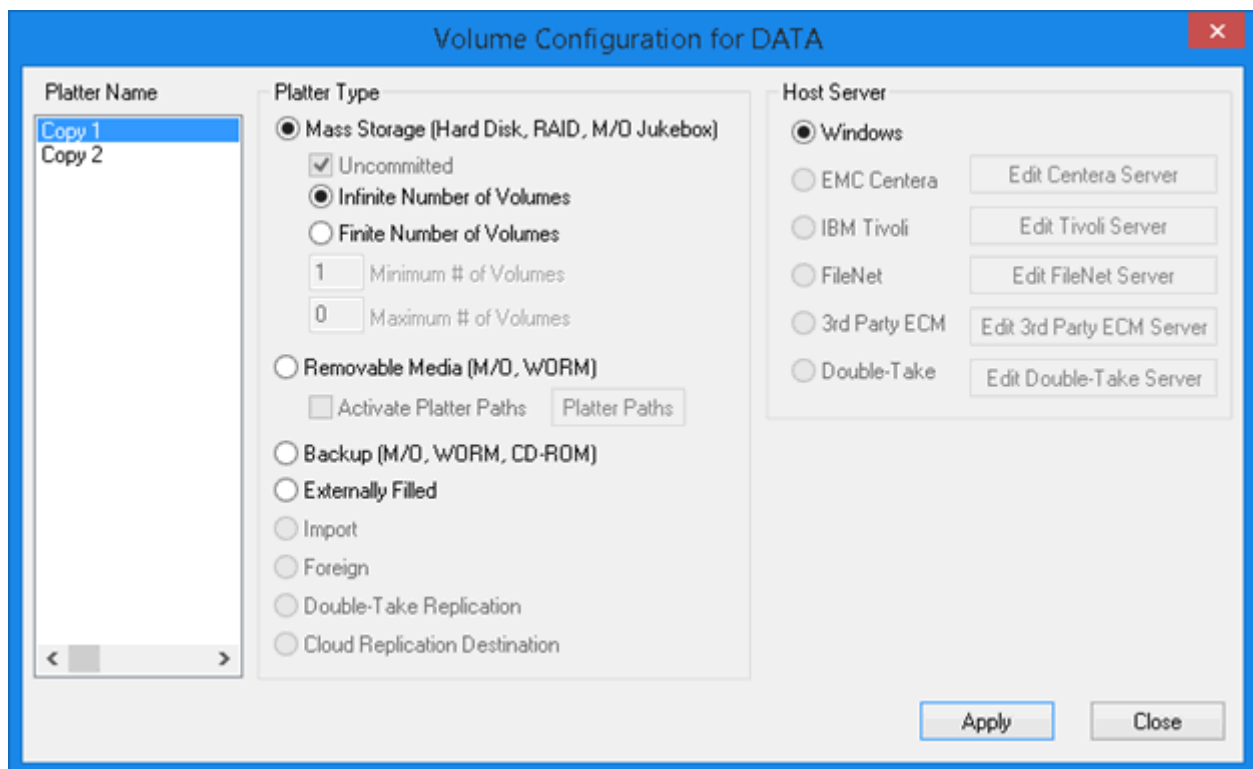
Note: When UAC is enabled, administrators must open the text editor by right-clicking it and selecting **Run as administrator**, otherwise the config file cannot be modified and saved.

2. Locate the **<Hyland.PlatterManagement><DiskgroupAlias>** element.
3. Update the attributes of the **<Alias>** element in the **<DiskgroupAlias>** element as follows:
 - **oldname:** This is the full FTP platter path used by the Client, as entered for the **Mount Location** in the **Create Disk Group Copy** dialog.
 - **newname:** This is the full UNC path to the physical location of the Disk Groups.
 - **type:** Set the type to **unc** or **unix**, as appropriate to your system.
4. Remove the comment coding around the **<Alias>** element. The comment coding is the **<!--** line directly before the **<Alias>** element and the **-->** line directly after the **<Alias>** element.
5. Save and close the Application Server's web.config file.

Configuring Disk Group Volume

The **Volume Configuration** dialog box allows you to view and modify the current configuration of the different copies or platters of a Disk Group.

To open the Volume Configuration dialog box, click **Volume Configuration** on the **Disk Group Configuration** dialog box.



Platter Name

The **Platter Name** list box contains each of the configured copies for this Disk Group. When you select a copy, its configuration settings are displayed in the Platter Type section.

Note: Any changes you make on this dialog box will only affect this copy on the next volume of this Disk Group. It will not change any volumes that have already been created. To make the changes immediate, the Disk Group must be promoted (using **Force Promote** at the **Disk Group Settings** dialog box).

Platter Type

The configuration information is broken down by the platter (copy) type. The button that is selected will indicate which platter type applies to this copy. If you make any changes in this dialog box, you must click **Apply** to permanently store your changes before selecting a different copy or closing the dialog box.

Mass Storage indicates that the platter is on a type of media that remains mounted and available at any time. The **Mass Storage** fields allow you to set several configuration choices for a mass storage platter copy. The mass storage copies use the same mounted folder for the next volume of documents as the last volume.

Note: The **Copy 1** mass storage platter cannot have its type altered; it must always be a **Mass Storage** copy. An error message is displayed if you attempt to change the copy type.

Mass Storage Platter Characteristics	Description
Uncommitted	Indicates that this copy will receive all documents before they are committed into the Disk Group. This option should only be available for selection for Copy 1 and not available for any other mass storage copies in the Disk Group.
Infinite Number of Volumes	<p>Allows the mass storage copy to continuously promote, regardless of how much space is available on the physical drive where the copy is stored. Volumes with this setting are not added to the Delete queue. When creating a new Disk Group, this option is selected by default.</p> <hr/> <p>Note: If you set the copy to allow an infinite number of volumes, you must maintain a proper schedule of platter administration to ensure that you do not run out of space in the middle of your daily document processing.</p> <hr/>
Finite Number of Volumes	Helps maintain available space for mass storage volumes. Setting finite volumes allows entry of Minimum # of Volumes and Maximum # of Volumes for the Disk Group.

Mass Storage Platter Characteristics	Description
Minimum # of Volumes	<p>Available only if Finite Number of Volumes is enabled.</p> <p>Minimum # of Volumes sets a low watermark for how many volumes must be kept online for a Disk Group copy. Ideally an installation would relate the minimum number of volumes to the time in days, weeks, or months worth of data that should be kept on the storage device associated with this Disk Group copy. The system will not allow volumes to be deleted if the result of that deletion causes less than the Minimum # of Volumes to exist online. The Minimum # of Volumes thus protects an organization against excessive delete behavior that could cause retrievals from the next Disk Group copy that is possibly on slower media.</p>
Maximum # of Volumes	<hr/> <p>Note: The Minimum # of Volumes cannot be equal to the Maximum # of Volumes.</p> <hr/> <p>Available only if Finite Number of Volumes is enabled.</p> <p>Maximum # of Volumes sets the high watermark for how many volumes can be kept online for a Disk Group copy. Ideally the Maximum # of Volumes is set to a sufficient number of volumes greater than the Minimum # of Volumes to allow a predictable window of time for an administrator to perform routine delete operations. The closer the Maximum # of Volumes is set to the Minimum # of Volumes, the more frequently an administrator will need to delete older volumes. The Maximum # of Volumes must be at least one volume less than the actual maximum quantity of filled volumes that will fit into the space allocated on the device for this Disk Group copy.</p> <hr/> <p>Note: This setting is not considered during ad hoc importing. If the number of volumes exceeds the maximum number of volumes specified during an ad hoc import, the setting is not respected and a new volume is created.</p> <hr/>

Example: Assume that the **Mass Storage** drive has been designated to store 4 gigabytes of documents and you have configured your volume size to 500000 kilobytes. The largest maximum value you should configure is 7, because the most you could store is 8 volumes and you should enter 1 less than the maximum.

The reason for using one less is that if you process documents into your system using COLD, DIP or any other batch process, then it is possible to begin a batch with the maximum number of volumes on line and will need to promote in the middle of the job. If this occurs, the system will promote the last volume and complete the job on the next volume. At this point, you will have more than your configured maximum number of volumes on line. After this job is completed, however, you cannot add more documents to the Disk Group until the oldest volume is deleted.

A copy selected for **Removable Media** indicates that a platter can be mounted or dismounted at any time. If a platter is not mounted when a document on that platter is accessed, then the **Mount Disk** dialog box is displayed, which prompts you for the location of the platter.

You can change a removable copy type to either a **Mass Storage** or **Backup** copy.

After the first copy of a volume has been committed, the removable copy will have documents added to it. The system does not promote removable copies and will use the same folder as the previous volume. Instead, the system will automatically ask for the new path for the documents when a volume is promoted.

It is best to pre-configure the paths for each volume before the volume is created. You can enter the paths to each new volume for this copy by selecting the **Activate Platter Paths** box. By default, this option is selected when the copy is of the **Removable Media** type. It will activate the **Platter Paths** button. Click **Platter Paths** to open the Platter Paths dialog box and type the paths for each new volume.



Backup platters are specifically created during a Platter Administration backup process. The backup copy is created, but will not appear in the backup queue until the volume is full. No documents are written to the backup copy until the backup process has been completed.

You can change a backup copy to either a **Mass Storage** or **Removable** copy type.

Note: Only created backup copies can be changed to a **Mass Storage** copy type.

Import copies only exist in an Import Disk Group, which is automatically created when an Import process is initiated via **Import Manager**. When data is imported into the Import Disk Group, the files remain on their original distribution media, usually a CD.

Note: Import copies cannot be changed to any other type and no copy can be changed to be an **Import** type. It is important that only imported platters be identified as import copies.

A **Foreign** copy references files in a storage area that was not created by OnBase. Instead of processing these files and moving them into a Disk Group, only the index information and a simple reference to the file location is stored. This allows access to the files without actually having to move them to a Disk Group location. Foreign Disk Groups are populated by a **Self Configuring DIP Process**.

An **Externally Filled** copy is a valid logical placeholder in the Disk Group that is recognized by the database. The data management system will not place any data in that copy. The responsibility of copying data into the **Externally Filled** copy is the responsibility of the system administrator.

Platter Paths

Activating the **Platter Paths** check box for removable media platters in Volume 1 allows you to predefine paths for subsequent volumes in your Disk Group. This option is primarily used with CD Jukebox storage.

After a volume has been promoted, the system will use the predefined platter paths as the location of removable media paths in the new volume, instead of continually prompting you for the new location. Clicking Platter Paths opens the **Platter Paths** dialog box, allowing you to set up the platter paths for removable media.

The first default volume number displayed in the **Volume** field is **2**. Since you are currently working in Volume 1, Volume 2 is the next possible configurable volume. Be sure that this is the volume number that you want for the platter paths. If you want to configure platter paths for a different volume number, delete the number 2, and type the new volume number in the **Volume** field.

Type the path for the removable media platters for this volume in the **Path for Platter** field. To add this new path to the **Volume/ Paths for Platter** box, click **Add**.

If you need to modify an existing volume path, select the path from the **Volume/ Path for Platter** box and then make the necessary changes in the fields. You can delete a path from the box by selecting that path and clicking **Remove**. When you are finished predefining platter paths, click **Close**.

Host Server

Select the type of storage device to use for the volume. The external storage devices listed in this pane require additional licensing. See the corresponding module reference guides for details.

Configuring Disk Group Volume Information

The **Volume Information** dialog box gives details of each Disk Group volume and allows you to modify the current configuration of the platters.

Volume Information for SYSTEM Disk Group

Volume

Volume 1

Platters

Platter	Space Used	Type	Platter Path
1	0	M U-N-- C---	\\doc-024787\Disk Groups\OnBaseLocalSQL151\SYSTEM\Copy 1
2	0	M ---- C---	\\doc-024787\Disk Groups\OnBaseLocalSQL151\SYSTEM\Copy 2

Platter Path

\\doc-024787\Disk Groups\OnBaseLocalSQL151\SYSTEM\Copy 1

Search Order

Up Down

Physical Platter Information

Platter Type

☒ Mass Storage (Hard Disk, RAID, M/D Jukebox)

☒ Uncommitted

☐ Removable Media (M/D, WORM)

☐ Backup (M/D, WORM, CD-ROM)

☐ Externally Filled

☐ Import

Disk Alias

☐ Foreign

Alias ID File Name

☐ Double-Take Replication

☐ Cloud Replication Destination

Platter State

☒ Created

☐ In Backup Queue (To Create)

☐ In Delete Queue (To Remove)

☐ Deleted (Removed)

Media Information

☐ EMC Centera ☐ FileNet

☐ IBM Tivoli ☐ Double-Take

☐ KDMpliance ☐ 3rd Party ECM

Go To

Apply Close

It displays the following information:

- **Volume:** Lists each of the created volumes for the Disk Group. When you select a volume, the platter copies for that volume are listed in the **Platters** box in the top right corner of the dialog box. When a different volume is selected in the **Volume** section, the information in the **Platters** section will change to show the copies for that volume.
- **Platters:** Shows the volumes (**Platters**) and their current size in KB (**Used**).

The **Platter Information** section displays platter configuration settings that can be edited, with certain restrictions imposed according to the platter type. These settings include:

- **Search Order: Up** and **Down** can be used to move the order of the platter (copy) in the volume.

Note: The first copy, the uncommitted mass storage copy, will always remain first in the search list. Its order cannot be modified, nor can its type.

- **Platter Path:** This field is used to specify where the data in the volume is stored on the network. The path can be edited if moved. If the platter is a backup that has not yet been created, the path is listed as **Not Created**.

Note: Documents should not be edited, moved, copied, deleted, or otherwise managed in the physical Disk Group folder without using the OnBase interfaces. The OnBase clients and Configuration module provide the ability to fully manage documents stored in OnBase, as well as providing additional security, disk management, and backup benefits.

- **Platter Type:** Sets the storage medium for the platter. This setting is reflected in the Platters section, using a string of several characters. The first character in the string indicates the overall platter type. More than one Secondary Character can be used.

Platter Type (1st Character)	Description
M	Mass Storage
R	Removable
B	Backup
I	Import
F	Foreign
E	Externally Filled

Platter Type (Secondary Characters)	Description
U	Uncommitted
A	Auto Delete
N	Not Movable
D	Dedicated
W	WORM

Note: The **Uncommitted** option is not available for selection. Only the first copy will be marked as **Uncommitted**.

- **Alias ID File Name:** No path is specified for a Foreign copy when it is created. The path to the copy is entered manually in **Alias ID File Name**. OnBase checks for the existence of this file when performing Disk Group functions, but does not read the file.
- **Disk Alias:** The **Disk Alias** bar will show the **Import** label identification of an import platter. This bar will be unavailable for any other type of platter.

- **Platter State:** Sets the availability of the platter for Disk Management and configuration functions. The current state of the platter is reflected in the Platters section, using a single-character indicator.

Platter State	Description
C	Created
B	Backup Queue
D	Delete Queue
R	Deleted ("R": Removed)
F	Full Text

Codes for failed backup copies are also indicated by a single-character indicator.

Backup Failure	Description
S	Missing Files
	Too Large
N	Not Mounted
I	Image Server Error
P	Production Server Error
?	Undefined

- **Media Information:** Indicates if a volume is managed by an external storage device. The external storage devices listed in this pane require additional licensing. See the corresponding module reference guide for details.

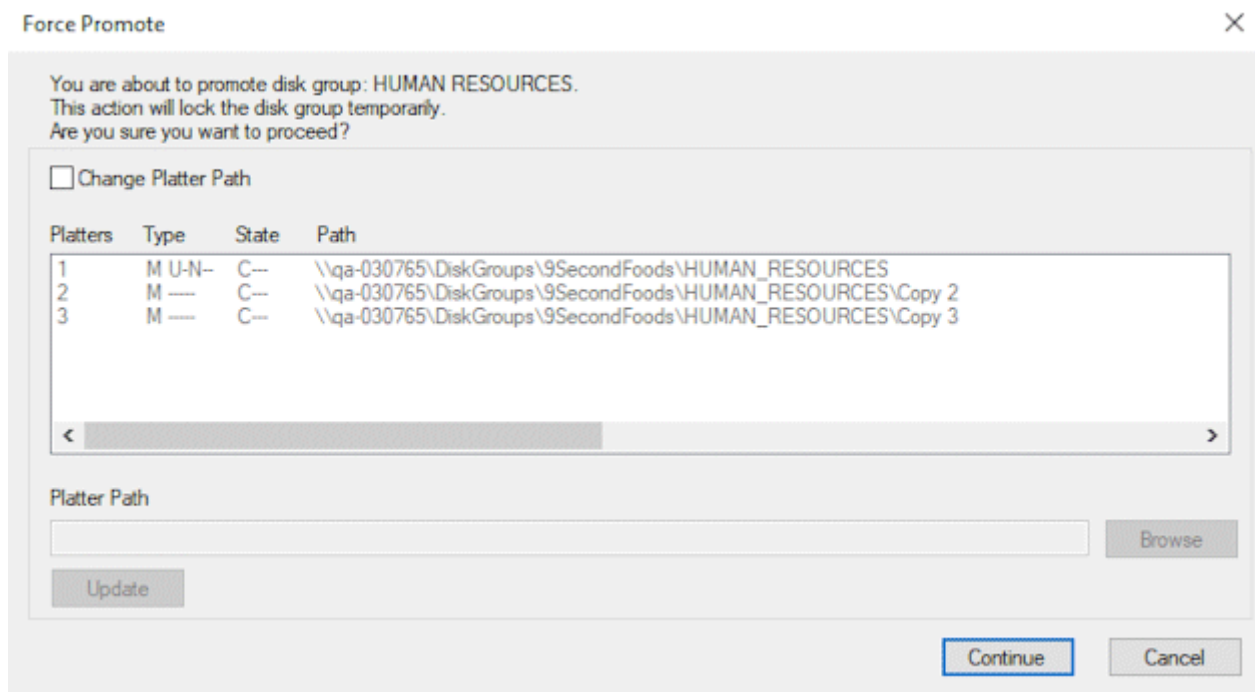
Configuring Disk Group Force Promote

Promoting a Disk Group ends the current volume and begins the next volume. The system will automatically promote a Disk Group when the current volume is full. This is achieved when the current volume reaches the number of kilobytes (KB) that were specified in the **Volume Size** field during Disk Group configuration.

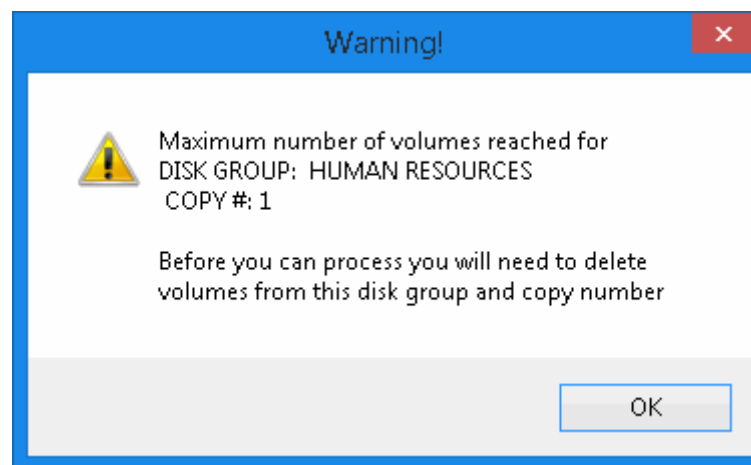
You can force a Disk Group to begin a new volume at any time. Imported Disk Groups can only be force promoted using the Import Manager with the **Use existing Disk Group** option. All force promotions are logged in the **SYS Platter Management Reports** log.

To force promote a Disk Group:

1. Click **Force Promote** on the **Disk Group Configuration** dialog box. The **Force Promote** dialog box is displayed.



If you have reached the maximum number of volumes designated for the Disk Group, a warning message is displayed instead.



Caution: You cannot recover a deleted volume. Before deleting volumes from any Disk Group, ensure they have been properly backed up according to your solution's requirements.

2. If you need to change the platter path of the promoted copies, select **Change Platter Path**.
 - a. Select the platter path to change in the **Platters** pane. The current path is displayed in the **Platter Path** field.

Note: Platter paths must be UNC paths at the time of promotion. Changing paths for backup or removable copies is not allowed.

- b. Edit the path in the **Platter Path** field, or click **Browse** to select a new location for the promoted copies.
 - c. Click **Update** to save your changes to the platter path.

Note: You cannot promote a volume to a location already used by another Disk Group.

3. Click **Continue** to promote the volume and create a new volume to continue storing data.

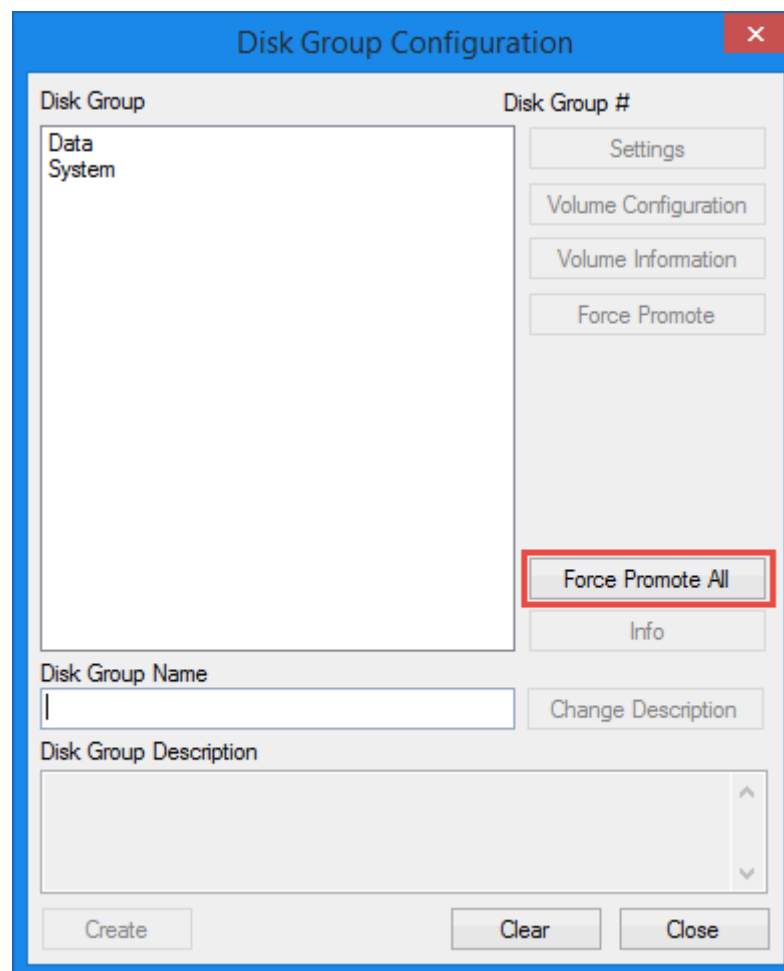
Note: If you **Force Promote** a volume, causing the minimum number of volumes to be met, copies that would enter the delete queue during an automatic promote do not enter the delete queue, even if all backup copies have been created.

Force Promoting All Disk Groups

In some circumstances it may be useful to force volume promotion in all Disk Groups at once so that there is a clear "break point," i.e. a clearly-visible demarcation for data in the disk groups. Such circumstances might occur when there is a major system event, for example if you are upgrading or restoring a database.

To force promote all Disk Groups:

1. Open Configuration and click on **Disk Mgmt | Disk Groups**. The **Disk Group Configuration** dialogue box is displayed.



2. Click on **Force Promote All**. A **Warning** dialogue box is displayed with the text, **You are about to promote <number of Disk Groups> Disk Groups. This action will temporarily lock each Disk Group. Are you sure you want to proceed?**

Note: Force promoting all Disk Groups will temporarily lock each Disk Group affected. This will affect any users in the system, so it is recommended to perform this action during down time.

Click **Yes** to proceed with volume promotion.

Click **No** to cancel the process.

Note: When force promoting all Disk Groups, you cannot change the platter path of any of the promoted copies.

If you have reached the maximum number of volumes designated for any of the Disk Groups, a warning message is displayed with the text **Maximum number of volumes reached for DISK GROUP: <your Disk Group> COPY #: <your Copy #>. Before you can process you will need to delete volumes from this disk group and copy number**

In order to force promote any Disk Groups that have reached their configured maximum number of volumes, you will need to either increase the maximum number of volumes allowed for the affected Disk Groups, or delete volumes from the affected Disk Groups.

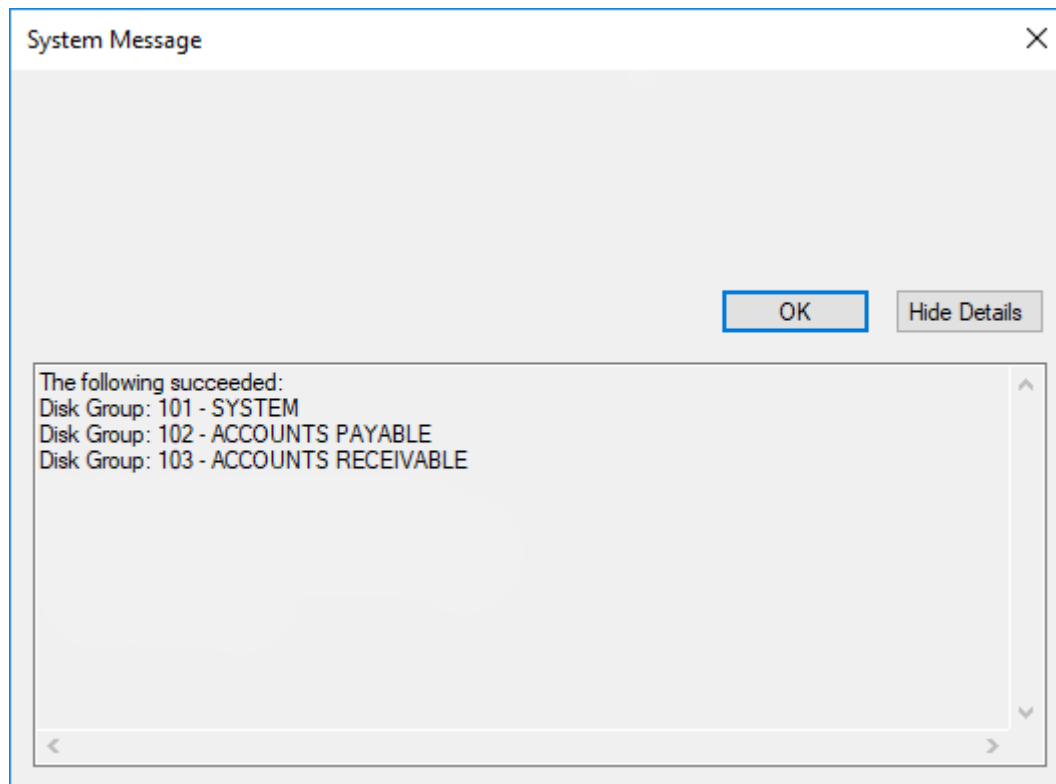
Caution: You cannot recover a deleted volume. Before deleting volumes from any Disk Group, ensure they have been properly backed up according to your solution's requirements.

Click **OK** to continue. A dialogue box is displayed with the text **Would you like to continue to promote the other Disk Groups?**

Click **Yes** to continue.

Click **No** to cancel the process.

3. If you clicked **Yes**, a **System Message** dialogue box is displayed, listing all the Disk Groups which have been successfully promoted.



4. Click **OK** to close the message.

Configuration Information Tree

The Configuration Tree provides a representation of system components and their relationship to other configured system modules and elements. For example, the Configuration Tree displays information for each Keyword Type such as the AutoFill Keyword Sets, Custom Queries, Document Types, Folder Types, and Keyword Type Groups in which the Keyword Type is used.

The Configuration Tree provides information about the following:

- Disk Groups
- Keyword Types
- Document Types
- User Names & Passwords

In the Configuration module, access the **Configuration Tree** from the following dialog boxes by clicking the **Info** button:

- **Disk Group Configuration** dialog box (dialog box accessed by selecting **Disk Mgmt | Disk Groups**). Provides information specific to Disk Groups.

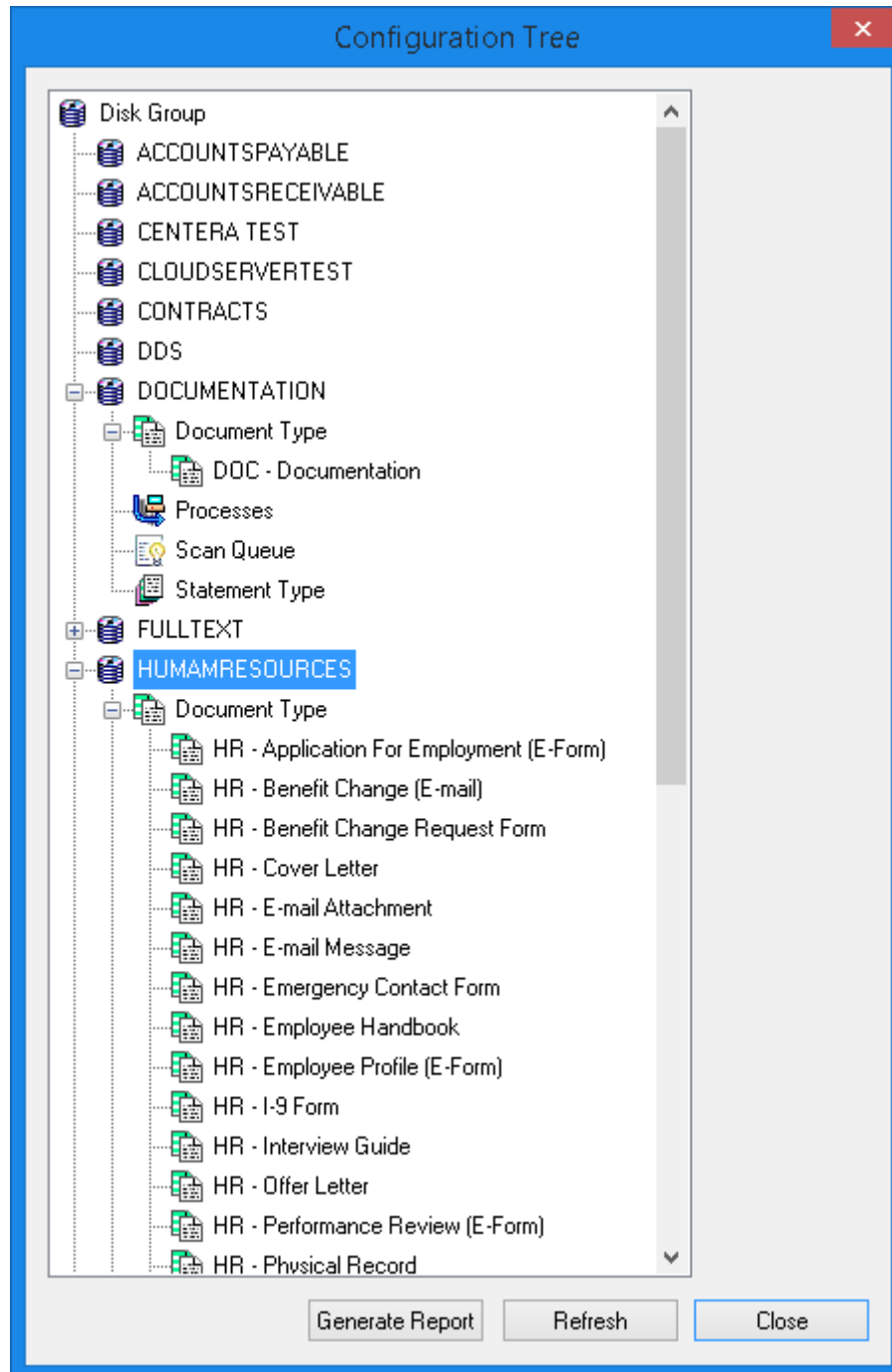
- **Keyword Type Configuration** dialog box (dialog box accessed by selecting **Keyword | Keyword Types**). Provides information specific to Keyword Types.
- **Document Types** dialog box (dialog box accessed by selecting **Document | Document Types**). Provides information specific to Document Types.
- **User Names & Passwords** dialog box (dialog box accessed by selecting **Users | User Names & Passwords**). Provides information specific to User Names & Passwords.

Note: From the **User Names & Passwords** dialog box, **Info** is only available to the MANAGER and ADMIN users.

Inclusive configuration information for all of the above components can be accessed by selecting **Utils | Configuration Tree**.

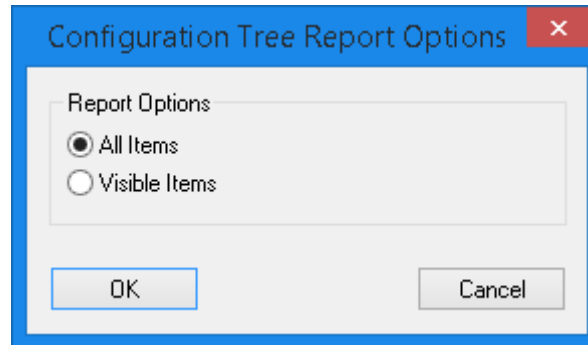
Configuration Tree Dialog Box

The **Configuration Tree** dialog box lists configuration information for items within the specified configuration category (Disk Group, Document Type, Keyword Type, user name). Select an item to view items on the subsequent level. Items that have additional information available are displayed with a plus sign (+).



The **Configuration Tree** dialog box can remain open while configuring other components of OnBase to allow easy access to configuration information. Click **Refresh** to update any configuration performed while the Configuration Tree is open.

You can create a text-based report displaying the hierarchy of tree items by clicking **Generate Report**. When the **Configuration Tree Report Options** dialog box displays, choose to run the report for **All Items** or for only the **Visible Items** within the tree.



When you run a report for **All Items**, every level of the tree automatically expands. When you run a report for **Visible Items**, the report displays only the currently expanded tree levels. The report is stored in the **SYS - Configuration Reports** Document Type.




Note: Generating a report for **All Items** may take a long time.



Component Information

The following tables describe the information displayed based on the dialog box from which you access the Configuration Tree.








Note: If you access the **Configuration Tree** dialog box from multiple dialog boxes within a session, information from all of the dialog boxes where the Configuration Tree was accessed will display.


Disk Group Configuration

Icon	Information Type	Description
	Disk Group Name	Name of Disk Group.
	Document Type	Lists Document Types configured to use the Disk Group by default.
	Processes	Lists all import processes configured to process documents into the Disk Group.













Icon	Information Type	Description
	Scan Queue	Lists all scan queues configured to scan documents into the Disk Group.
	Statement Type	Lists all statement types that are configured to use the Disk Group as the Archived Statement Disk Group .



User Names & Passwords

Icon	Information Type	Description
	User Name	Name of the user. The following elements relate to the user listed.
	Custom Query	Lists Custom Queries.
	Document Type	Lists Document Types. Right-click a Document Type and select Document Privileges to view a user's privileges for that Document Type.
	File Cabinet	Lists file cabinets.
	Folder Name	Lists folder types.
	Life Cycle	Lists Workflow life cycles.
	Note Type	List note types.
	Print Queue	Lists print queues.
	Scan Queue	Lists scan queues.
	User Group	Lists user groups.








Icon	Information Type	Description
	VB Script	Lists VB Scripts.

Document Types

Icon	Information Type	Description
	Document Type Name	Name of Document Type.
	Advanced Exception Report	Lists the names of advanced exception reports configured for the Document Type.
	Basic Exception Report	Lists the names of basic exception reports configured for the Document Type.
	Cross-Reference	Lists all Document Types that are cross-referenced from the current Document Type.
	Custom Query	Lists the Custom Queries that search the selected Document Type.
	Document Template	Lists the document templates associated with the Document Type.
	Document Type Overrides	Lists all overrides associated with the Document Type.
	Folder Type	Lists the dynamic Folder Types associated with the Document Type.
	Index Extraction	Lists all index extraction formats associated with the Document Type.
	Print Distribution	Lists all print distributions associated with the Document Type.
	Processes	Lists all import processes associated with the Document Type.
	Statement Type	Lists all statement types associated with the Document Type.

Icon	Information Type	Description
	Workflow Action	Lists all Workflow actions associated with the Document Type.
	Workflow Rule	Lists all Workflow rules associated with the Document Type.

Keyword Type Configuration

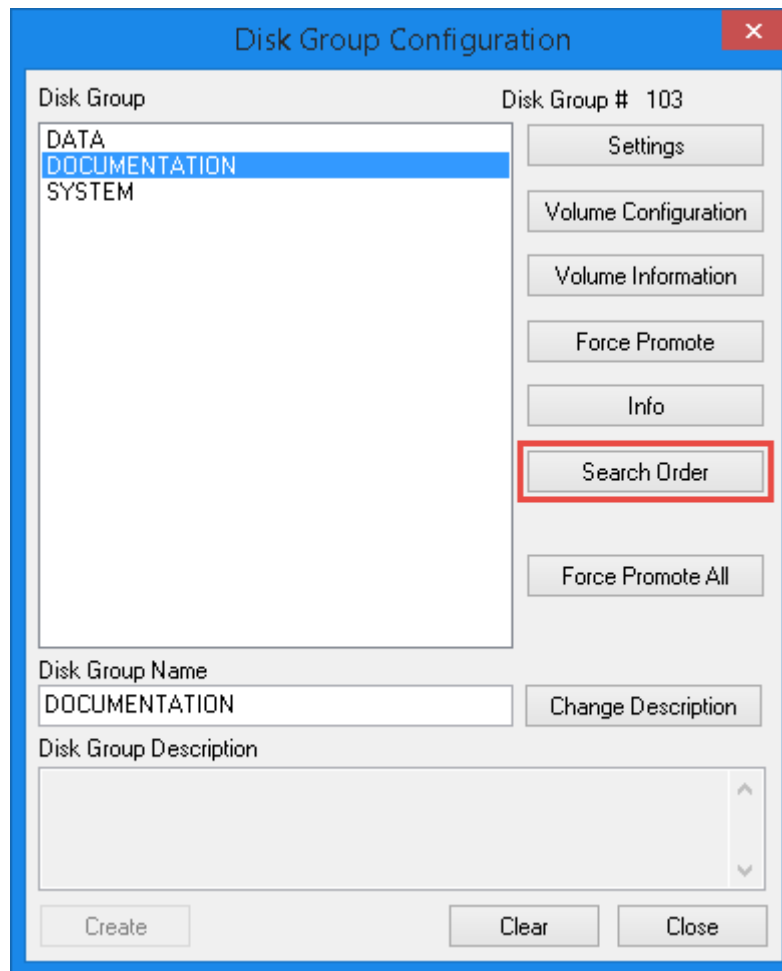
Icon	Information Type	Description
	Keyword Type Name	Name of Keyword Type.
	AutoFill Keyset	Lists AutoFill Keyword Sets that the Keyword Type belongs to.
	Custom Query	Lists Custom Queries that use the Keyword Type to search for documents.
	Document Distribution	Lists document distributions that use the Keyword Type as a process ID keyword.
	Document Type	Lists Document Types that use the Keyword Type for indexing and retrieval.
	Folder Type	Lists the Folder Types that use the Keyword Type for retrieval.
	Keyword Group	Lists Keyword Type Groups that the Keyword Type belongs to.

Changing the Platter Search Order Across a Range of Volumes

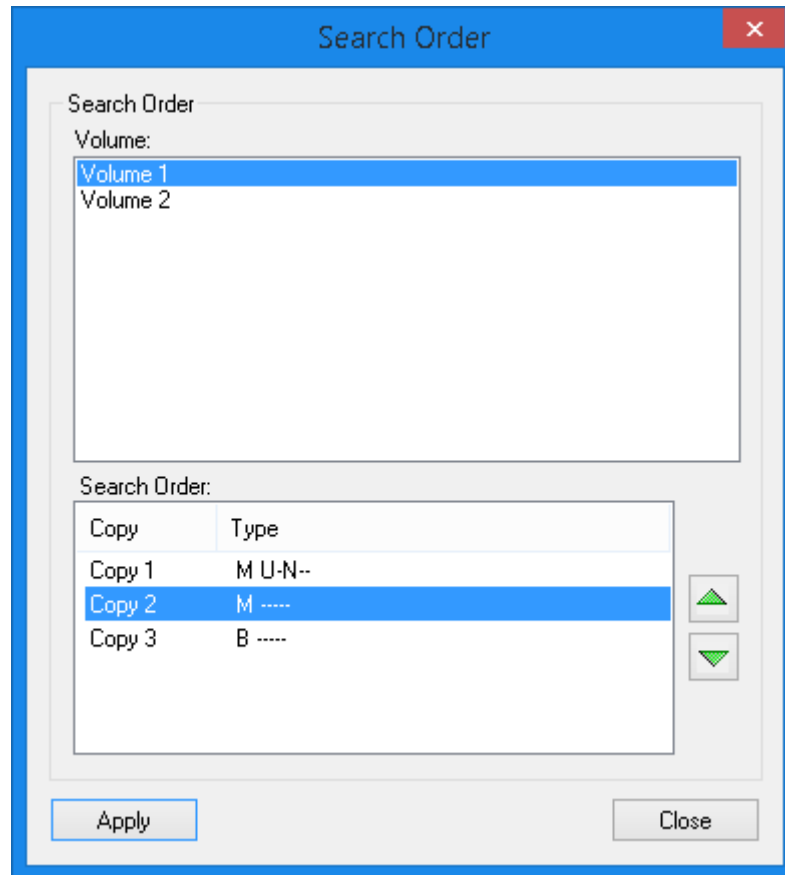
Sometimes it is necessary to change the order in which platters (copies) are searched across a range of volumes. The search order of copies for a specific volume can be changed from the **Volume Information** dialog box, but changing the search order across a range of volumes can only be done from the **Search Order** dialog box. To access this dialog, you must first apply the **-ROMANZO** switch to the Configuration module.

Caution: Before using features enabled by the -ROMANZO switch, ensure that you understand the feature and implications of any changes to your system. Contact your service provider with any questions regarding these features. Features enabled by the -ROMANZO switch should not be made available to the casual user. Remove the -ROMANZO switch after completing necessary actions.

To change the search order of copies across a range of volumes, select **Disk Mgmt | Disk Groups** in Configuration. The **Disk Group Configuration** dialog is displayed.



1. Select the Disk Group of which to change the search order, then click **Search Order**. The **Search Order** dialog is displayed.
2. In the **Volume** pane, select the volumes for which you would like to change the copy search order. The changes you make are applied to each volume selected. To select the volumes, hold down the **CTRL** key and select each volume, or hold down the **SHIFT** key and select the first and last volumes in the range desired.



In order to successfully change the search order, the volumes selected must meet certain requirements:

- You can only select sequential volumes (e.g., 5 through 9, not 5, 6, and 9)
- The volumes selected must be matched, meaning they must each contain the same number of copies.

For example, if you select volumes 1 through 3, and volumes 1 and 2 have four copies, but volume 3 has five copies, volume 3 does not match, so its search order cannot be changed in this way (its search order can still be changed separately).

3. In the **Search Order** pane, select the copy you want to move.

Note: Copy 1 cannot be moved because it is the uncommitted copy, and no copy can be moved to a position before Copy 1.

4. Click the up or down arrows to move the selected copy to the desired place in the search order.
5. If you need to change the search order of other copies, select the next copy to move and use the arrows to reorder it accordingly.
6. Click **Apply** to commit the changes.
7. Click **Close** to exit the Search Order dialog.

Convert Existing Disk Groups to Centera or Tivoli

If your system is configured with Storage Integration for Centera or Tivoli, platters can be converted to these storage devices. To move platters to Centera or Tivoli:

1. In the Configuration module, select **Disk Mgmt | Disk Groups**.
2. Select the appropriate Disk Group.
3. Click **Volume Configuration**.
4. Select **Copy 2** or any other copy.

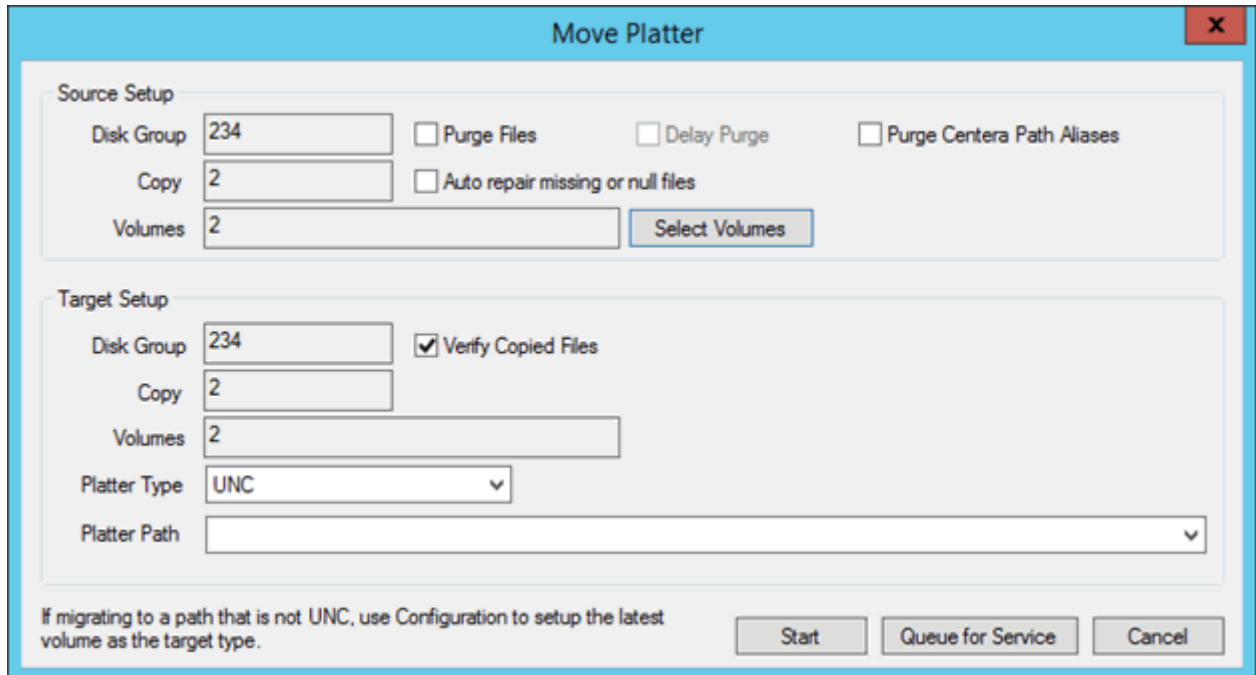
Note: Copy 1 cannot be moved to Centera or Tivoli.

5. Select **EMC Centera** or **IBM Tivoli** in the **Host Server** settings.
6. Enter the appropriate information into the **Server Settings** dialog box.
7. Click **Save**.
8. Apply the **-ROMANZO** switch to the OnBase Client module's shortcut and open the Client.

Caution: Before using features enabled by the -ROMANZO switch, ensure that you understand the feature and implications of any changes to your system. Contact your service provider with any questions regarding these features. Features enabled by the -ROMANZO switch should not be made available to the casual user. Remove the -ROMANZO switch after completing necessary actions.

9. In the OnBase Client, select **Admin | Platter Management**.
10. Select the appropriate Disk Group.
11. Double-click on the appropriate volume.

12. Right-click on the appropriate copy and select **Move**. The **Move Platter** dialog box is displayed.



The **Move Platter** dialog box is shown with the following settings:

Source Setup

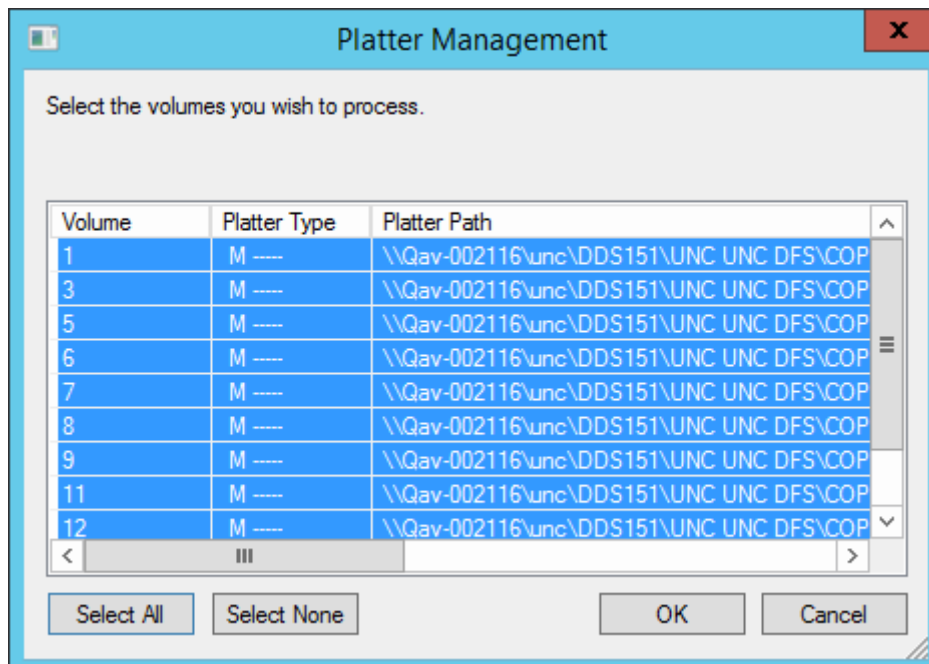
- Disk Group: 234
- Copy: 2
- Volumes: 2
- ☐ Purge Files
- ☐ Delay Purge
- ☐ Purge Centera Path Aliases
- ☐ Auto repair missing or null files
- Select Volumes** button

Target Setup

- Disk Group: 234
- Copy: 2
- Volumes: 2
- Platter Type: UNC
- Platter Path: (empty field)
- ☒ Verify Copied Files

At the bottom, there is a note: "If migrating to a path that is not UNC, use Configuration to setup the latest volume as the target type." and three buttons: **Start**, **Queue for Service**, and **Cancel**.

13. In the **Platter Type** drop-down, select the **EMC Centera** or **IBM Tivoli** option, depending on your system.
14. If you want to move multiple volumes, click **Select Volumes**. If not, skip to step 18.
15. The **Platter Management** dialog box is displayed.



The **Platter Management** dialog box is shown with the title "Select the volumes you wish to process."

Volume	Platter Type	Platter Path
1	M ----	\\Qav-002116\unc\DDS151\UNC UNC DFS\COP
3	M ----	\\Qav-002116\unc\DDS151\UNC UNC DFS\COP
5	M ----	\\Qav-002116\unc\DDS151\UNC UNC DFS\COP
6	M ----	\\Qav-002116\unc\DDS151\UNC UNC DFS\COP
7	M ----	\\Qav-002116\unc\DDS151\UNC UNC DFS\COP
8	M ----	\\Qav-002116\unc\DDS151\UNC UNC DFS\COP
9	M ----	\\Qav-002116\unc\DDS151\UNC UNC DFS\COP
11	M ----	\\Qav-002116\unc\DDS151\UNC UNC DFS\COP
12	M ----	\\Qav-002116\unc\DDS151\UNC UNC DFS\COP

At the bottom, there are buttons: **Select All**, **Select None**, **OK**, and **Cancel**.

16. You can click **Select All** to select all available volumes or control-click to select the desired volumes.

Note: The process will halt if it encounters a volume that has already been moved to Centera or Tivoli.

Click **Select None** to deselect all volumes.

17. Click **OK** to return to the **Move Platter** dialog.

18. Select **Purge Files** to delete the existing copies of the files once the files have been successfully moved.

If you want to keep the files in the old location after the move, deselect the **Purge Files** check box.

Note: If the **Purge Files** option is deselected, the old files are not deleted and are no longer controlled by OnBase. Deletion of these files must be done manually outside of OnBase.

19. Click **Start**.

S3 Disk Groups allow for the use of S3 cloud storage as a Disk Group within OnBase. S3 disk groups work with an S3 provider to store data in containers called buckets on a cloud based server. To use an S3 Disk Group, you need to work with a third-party S3 provider. A URL for the S3 Disk Group and keys should be provided by the third-party provider for configuration of the S3 Disk Group.

S3 Considerations

Before implementing S3 disk groups, several issues need to be considered, including:

- S3 Disk Groups appear in the **Platter Management** window in the OnBase Client similar to other Disk Groups. However, the only right-click function available for these disk groups in this window is **Compute Volume Size**.
- Documents, images, and files can be imported into S3 disk groups from the OnBase Client, but cannot be retrieved using the OnBase Client. The Unity Client, Web Client, or any method using the Application Server must be used for retrieval.
- The only System Document Types that should be used with S3 are Reports and Logs. All other System Document Types should remain stored on a traditional Disk Group.
- Import processors such as DIP and COLD are supported by S3 Disk Groups, but require the use of an Upload Cache. For more information on the Upload Cache, see [Configuring S3 Upload Cache Processing on page 62](#).
- If using a cloud based S3 provider, retrieving files from an S3 Disk Group may take more time than retrieving items from a traditional disk group.
- Scrubbing files during deletion is not supported on S3 Disk Groups.

Migrating to an S3 Disk Group

If you are planning on using an S3 Disk Group to replace a previously in use Disk Group, you must use Disk Group Migration to migrate the files from the older Disk Group to the S3 Disk Group. Prior to attempting migration, ensure that the S3 Disk Group has been properly configured. For more information on Disk Group Migration, see [Disk Group Migration on page 100](#). For more information on configuration, see [Configuring an S3 Disk Group on page 53](#).

Configuring an S3 Disk Group

S3 Disk Groups require different configuration steps from other disk groups. Prior to configuring an S3 Disk Group, an S3 Provider must be configured for use. For information on configuring S3 Providers, see [Configuring an S3 Provider on page 56](#). Additionally, if the S3 Disk Group is going to be used for any import processing, such as DIP or COLD, you must have an S3 Upload Cache Processing task configured. For more information on this task, see [S3 Upload Cache Processing on page 114](#).

To create an S3 Disk Group in the Configuration module:

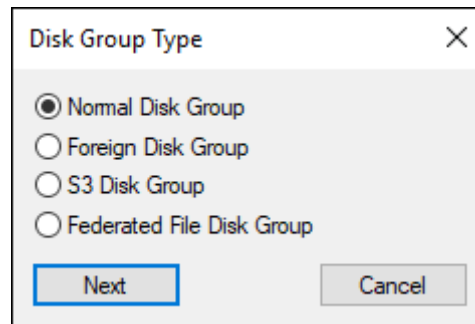
1. Select **Disk Groups** under **Disk Mgmt**. The **Disk Group Configuration** dialog box is displayed.

The screenshot shows the 'Disk Group Configuration' dialog box. It features a list of existing disk groups on the left, including 'ACCOUNTS PAYABLE', 'ACCOUNTS RECEIVABLE', 'BILLING', 'DDS', 'DOCUMENTATION', 'ENCRYPTED', 'Foreign', 'HUMAN RESOURCES', 'INFORMATION SYSTEMS', 'Migration', 'S3 DG1', 'SYSTEM', and 'Test'. To the right of this list are several action buttons: 'Settings', 'Volume Configuration', 'Volume Information', 'Force Promote', 'Info', 'Cloud Replication', and 'Force Promote All'. Below the list is a text field for 'Disk Group Name' and a text area for 'Disk Group Description'. A 'Change Description' button is positioned to the right of the name field. At the bottom of the dialog are three buttons: 'Create', 'Clear', and 'Close'.

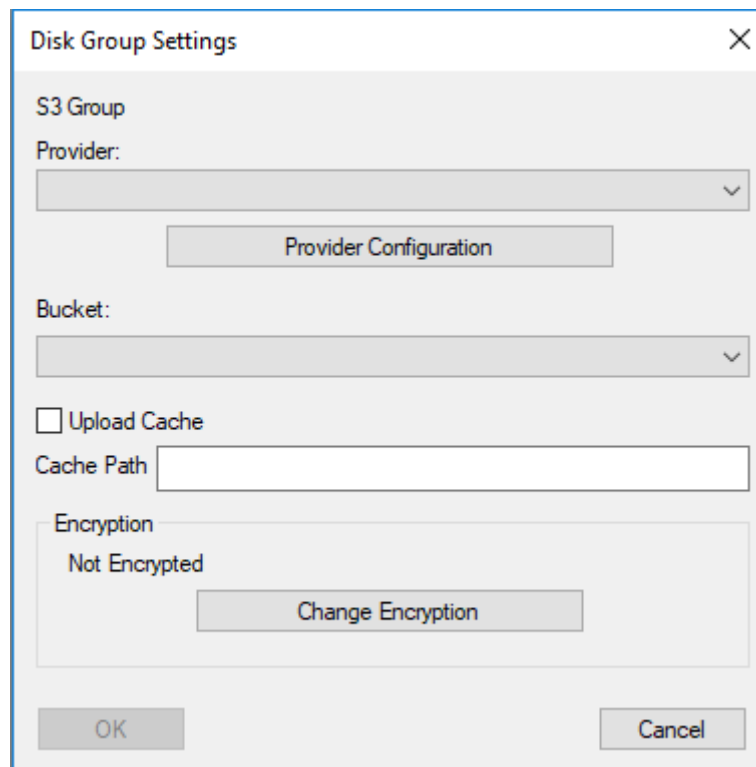
2. Type the name of the new S3 Disk Group in the **Disk Group Name** field.

Note: S3 Disk Groups must have unique names compared to other Disk Groups. An S3 Disk Group cannot have the same name as any other Disk Group, S3 or otherwise.

- Click **Create**. The **Disk Group Type** dialog box is displayed



- Select **S3 Disk Group** and click **Next**. The **Disk Group Settings** dialog box is displayed.



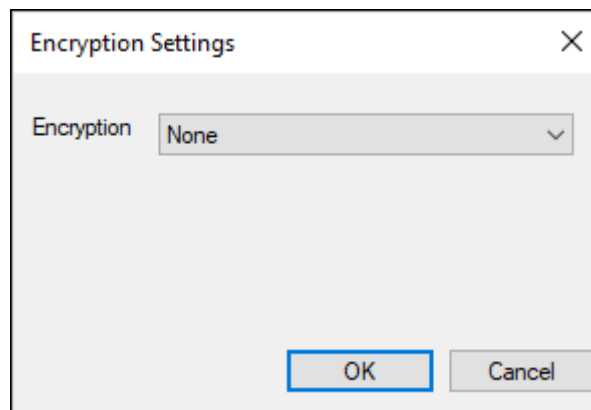
- Select an S3 provider for the Disk Group from the **Provider** drop-down list. If the provider is not listed, click **Provider Configuration** to configure the provider. For more information on configuring providers, see [Configuring an S3 Provider on page 56](#).
- Select a bucket from the **Bucket** drop-down list. If the bucket you need is not included in this list, ensure that you have the proper S3 provider selected. If the bucket is still not available, contact your first line of support to have the bucket created.

Note: Buckets cannot be created within OnBase. New buckets must be created directly with your S3 provider. Changing the bucket in an already active Disk Group forces the promotion of the Disk Group. Each bucket can only be used by one provider and a single implementation of OnBase.

7. Select the **Upload Cache** option to enable the Upload Cache for use with the S3 Disk Group. The Upload Cache is required for any Disk Group that uses any form of processing in the OnBase Client such as COLD, Check Images, etc. For more information on the Upload Cache, see [Configuring S3 Upload Cache Processing on page 62](#).

Note: Prior to enabling an Upload Cache, you must have an S3 Upload Cache Processing task configured in the Unity Scheduler module. For more information on the Upload Cache Processor task, see [Configuring S3 Upload Cache Processing on page 62](#). Any change made to the Upload Cache setting once an S3 Disk Group is in use will force the promotion of the Disk Group before the change takes place. Once an S3 Disk Group is configured, changing the path for the S3 Upload Cache requires the use of the **-ROMANZO** switch and locking out the database.

8. Enter a UNC location into the **Cache Path** field. This is the location where files are locally stored in the Upload Cache before being uploaded to the S3 server.
9. Click **Change Encryption** to change the encryption on files both on the S3 server and within the Upload Cache. The **Encryption Settings** dialog box is displayed.



10. Select the desired encryption from the drop-down select menu and click **OK**. Options for encryption are **AES 128**, **AES 256 v2**, and **S3 KMS**. For more information on S3 KMS encryption, see [KMS Encryption on page 77](#).

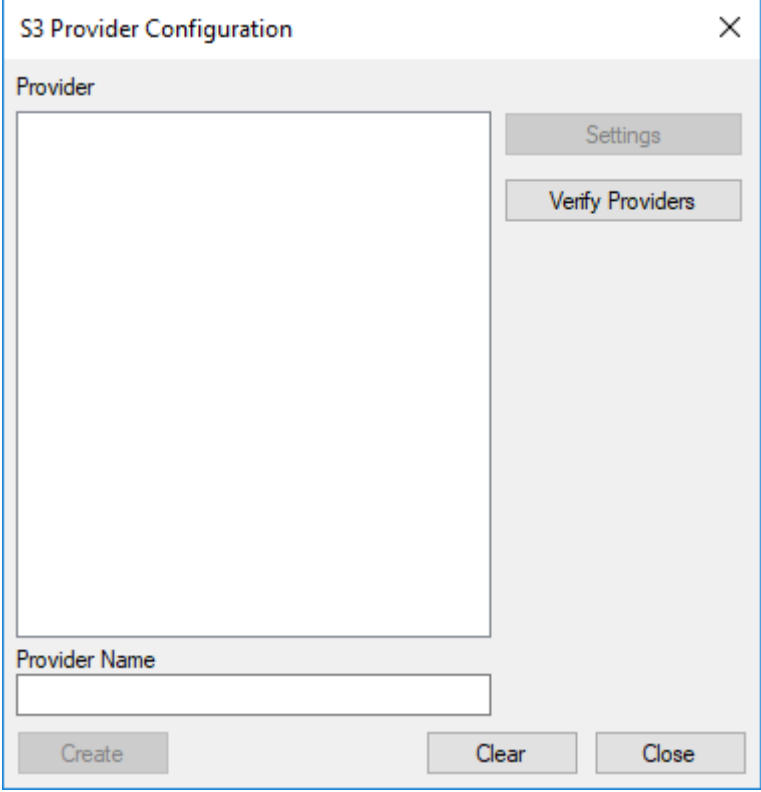
Note: AES 128 and AES 256 v2 can only be enabled during creation of a new S3 Disk Group. S3 KMS encryption can be enabled for an S3 Disk Group after configuration.

11. Click **OK** in the **Disk Group Settings** dialog box to complete creating a new S3 Disk Group.

If you want to migrate files from another Disk Group to the newly created S3 Disk Group, you must use the Disk Group Migration tool. For more information on this tool, see [Disk Group Migration on page 100](#).

Configuring an S3 Provider

S3 providers are configured in the **S3 Provider Configuration** dialog box, which can be accessed in the Configuration module by clicking **Provider Configuration** in the **Disk Group Settings** dialog box for an S3 Disk Group, or by clicking **S3 Provider Configuration** under **Disk Mgmt | S3 Disk Groups**.



The S3 Provider Configuration dialog box features a title bar with the text "S3 Provider Configuration" and a close button (X). The main area is divided into two sections. The top section, labeled "Provider", contains a large empty rectangular box for provider details and two buttons: "Settings" and "Verify Providers". The bottom section, labeled "Provider Name", contains a single-line text input field. At the bottom of the dialog are three buttons: "Create", "Clear", and "Close".

To create an S3 provider in the **S3 Provider Configuration** dialog box:

1. Type a name for the new S3 provider in the **Provider Name** field.
2. Click **Create**. The **S3 Provider Settings** dialog box is displayed.

3. Enter the **Provider URL**, **Access Key**, and **Secret Key** in the relevant fields. These should be provided to you by your S3 host or your systems administrator.
4. Select an **S3 Provider Type** from the list of available options. These options include:

Provider Type	Description
Basic Compatibility	The simplest version of an S3 provider. This type should only be selected if your S3 provider specifically does not support multi-part uploads, which allow for larger files to be uploaded in smaller pieces.
Moderate Compatibility	The recommended compatibility setting for most S3 providers. This setting supports multi-part uploads and most other S3 functions.

The provider type affects the expected APIs in use for the S3 provider, shown to the right of the selection under **Expected APIs**. **Moderate Compatibility** is the recommended setting and should be used unless you know in advance that your S3 provider does not support multi-part uploads.

5. Click **OK**. The **S3 Provider Settings** dialog box is closed.

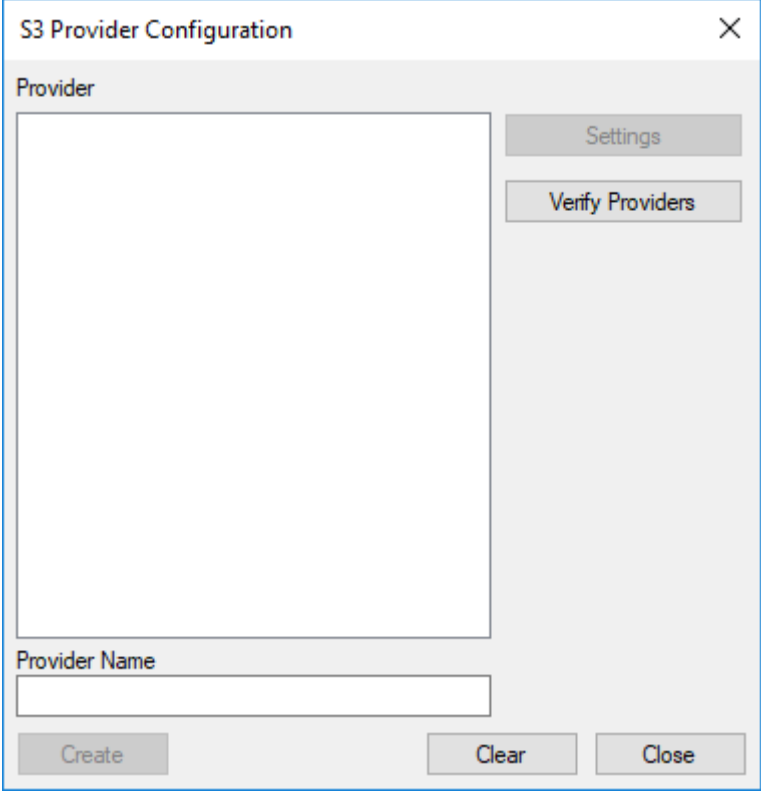
Once configured, the S3 provider appears in the drop-down list in the **Disk Group Settings** dialog box for the S3 Disk Group.

Verifying an S3 Provider

If you are having any problems connecting to an S3 provider, the Provider Status dialog box can be used to verify the status of the S3 provider.

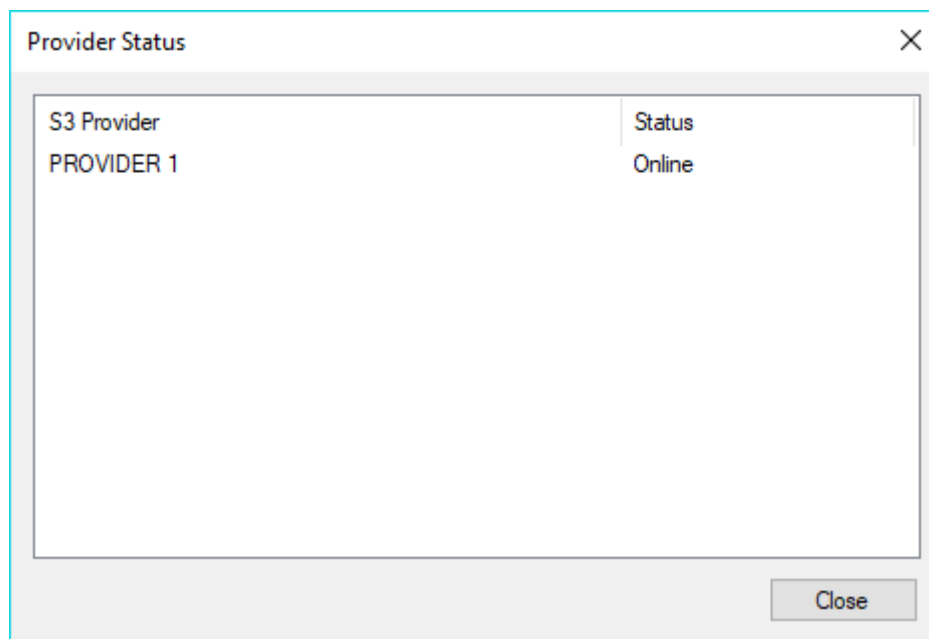
To verify the status of a provider in Configuration:

1. Click **S3 Provider Configuration** under **Disk Mgmt | S3 Disk Groups**. The **S3 Provider Configuration** dialog box is displayed.



The screenshot shows a dialog box titled "S3 Provider Configuration" with a close button (X) in the top right corner. The dialog is divided into two main sections. The top section, labeled "Provider", contains a large empty rectangular box on the left and two buttons on the right: "Settings" and "Verify Providers". The bottom section, labeled "Provider Name", contains a single-line text input field. At the very bottom of the dialog, there are three buttons: "Create", "Clear", and "Close".

2. Click **Verify Providers**. The **Provider Status** dialog box is displayed. The configured S3 providers are shown here with their status.



3. Ensure that the S3 provider you configured is shown as **Online** under **Status**.
4. Click **Close**. The **Provider Status** dialog box is closed.
5. In the **S3 Provider Configuration** dialog box, click **Close**. The dialog box is closed.

If an S3 provider's status is shown as **Offline** or **Invalid Credentials**, confirm that the S3 provider is properly configured. If all settings are correct, contact your S3 provider or system administrator to resolve the issue.

Viewing S3 Volume Information

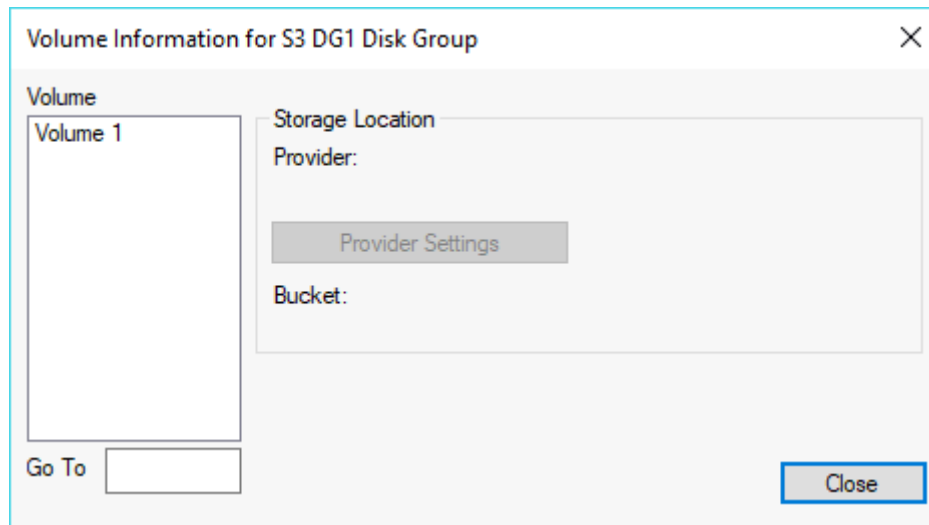
Information on S3 Disk Group Volumes is accessed from the **S3 Disk Group Configuration** dialog box. To access the Volume Information for an S3 Disk Group in OnBase Configuration:

1. Select **Disk Group Configuration** under **Disk Mgmt | S3 Disk Groups**. The **S3 Disk Group Configuration** dialog box is displayed.

The screenshot shows the 'S3 Disk Group Configuration' dialog box. It has a title bar with a close button (X). The main area is divided into two columns. The left column is titled 'Disk Group' and contains a list with one item, 'S3 DG1'. The right column is titled 'Disk Group #' and contains three buttons: 'Settings', 'Volume Information', and 'Info'. Below the list, there is a 'Disk Group Name' label and a text input field. To the right of the input field is a 'Change Description' button. Below the input field is a 'Disk Group Description' label and a large text area with a vertical scrollbar. At the bottom of the dialog, there are three buttons: 'Create', 'Clear', and 'Close'.

2. Select the desired S3 Disk Group from the list of available S3 Disk Groups.

- Click **Volume Information**. The **Volume Information** dialog box is displayed.



- Select the desired volume from the list of available volumes. The **Storage Location** box displays the S3 Provider and S3 Bucket for the selected volume. To view settings for the assigned S3 Provider, click the Provider Settings button. The S3 Provider Settings dialog box is displayed. For more information on S3 Providers, see [Configuring an S3 Provider on page 56](#).
- Once finished viewing the information on volumes, click **Close**.

Forcing the Promotion of S3 Disk Groups

S3 Disk Groups can be forced to promote in the **S3 Disk Group Configuration** dialog box in the Configuration module. The **Force Promote** and **Force Promote All** buttons will only appear in this dialog box when using the **-ROMANZO** switch.

To force the promotion of an S3 Disk Group:

- Apply the **-ROMANZO** switch to Configuration before launching the Configuration module.

Caution: Before using features enabled by the **-ROMANZO** switch, ensure that you understand the feature and implications of any changes to your system. Contact your service provider with any questions regarding these features. Features enabled by the **-ROMANZO** switch should not be made available to the casual user. Remove the **-ROMANZO** switch after completing necessary actions.

- Launch Configuration with the **-ROMANZO** switch applied.

3. Select **Disk Group Configuration** under **Disk Mgmt | S3 Disk Groups**. The **S3 Disk Group Configuration** dialog box is displayed with the **Force Promote** and **Force Promote All** buttons available.

The screenshot shows the 'S3 Disk Group Configuration' dialog box. It has a title bar with a close button (X). Inside, there's a table with two columns: 'Disk Group' and 'Disk Group #'. The first row contains 'S3 DG1'. To the right of the table are five buttons: 'Settings', 'Volume Information', 'Info', 'Force Promote', and 'Force Promote All'. Below the table, there's a 'Disk Group Name' text field and a 'Change Description' button. Below that is a 'Disk Group Description' text area. At the bottom are three buttons: 'Create', 'Clear', and 'Close'.

4. To promote a single S3 Disk Group, select the desired Disk Group and click **Force Promote**. To promote all S3 Disk Groups, click **Force Promote All**. A **Warning** dialog box is displayed to confirm you want to promote the Disk Group(s).
5. Click **Yes** to continue. Once the promotion is complete, a **System Message** window confirms the promotion was successful.
6. Click **OK**.

Configuring S3 Upload Cache Processing

The S3 upload cache is used to locally store files processed by the OnBase Client prior to uploading to the S3 servers. The upload cache is configured during the creation of an S3 Disk Group. For more information on configuring the upload cache, see [Configuring an S3 Disk Group on page 53](#).

The upload cache stores files in a UNC accessible storage location and uploads the files to the S3 provider whenever the **S3 Upload Cache Processing** task is run by the Unity Scheduler. When the **S3 Upload Cache Processing** task is executed, all of the files in the S3 upload cache are uploaded to the S3 Provider. When the task is completed, any empty folders created in the cache are deleted.

The **S3 Upload Cache Processing** task is available as a preconfigured system task. The **S3 Upload Cache Processing** system task is automatically configured when the Unity Management Console is initially launched.

Note: System tasks automatically run at 2:00 AM local time. The timing of a system task can be changed in Unity Scheduler. For more information on modifying the schedule of system tasks, see the **Unity Scheduler** module reference guide.

Alternatively, the **S3 Upload Cache Processing** task can be manually created in the Unity Management Console. Manually created tasks can be used to upload the cache multiple times a day, or to manually upload the cache after a significant number of files have been added. For information on manually creating a Unity Scheduler task, see [Creating a Task on page 110](#).

Note: Manually created tasks must have a schedule assigned to the task before they can execute. For information on creating and assigning schedules, see the **Unity Scheduler** module reference guide.

During the execution of an **S3 Upload Cache Processing** task, if an upload fails 20 times, the execution of the task is suspended and the remaining files are not uploaded. The task attempts to run again when scheduled but will fail if the issue causing the failure has not been addressed.

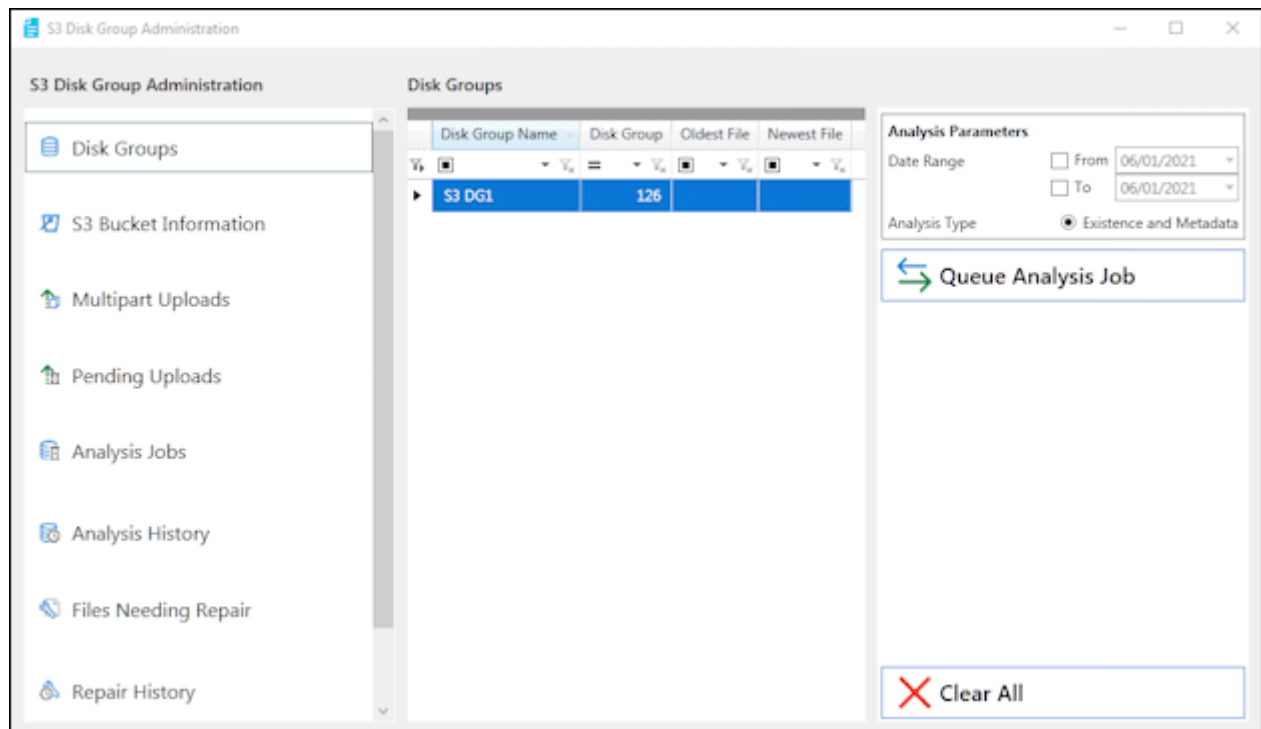
S3 Disk Group Administration

S3 Disk Group Administration is a tool for monitoring S3 Disk Groups once they have been configured. S3 Disk Group Administration is accessed in the OnBase Client by navigating to **Admin | S3 Disk Group Administration**. S3 Disk Group Administration is divided into a number of separate tabs including **S3 Bucket Information**, **Multipart Uploads**, and **Pending Uploads**. The **S3 Disk Group Administration** window includes tabs for:

- [Viewing S3 Disk Groups on page 64](#)
- [Viewing the Status of S3 Buckets on page 64](#)
- [Viewing the Status of Multipart Uploads on page 66](#)
- [Viewing Pending Uploads on page 68](#)
- [Viewing Analysis Jobs on page 70](#)
- [Viewing Completed Analysis Jobs on page 71](#)
- [Viewing Files Needing Repair on page 72](#)
- [Viewing Repaired Files on page 73](#)

Viewing S3 Disk Groups

The **Disk Group** tab of the **S3 Disk Group Administration** window. Analysis jobs that have been configured for a Disk Group can be queued in this window.



To queue an analysis job:

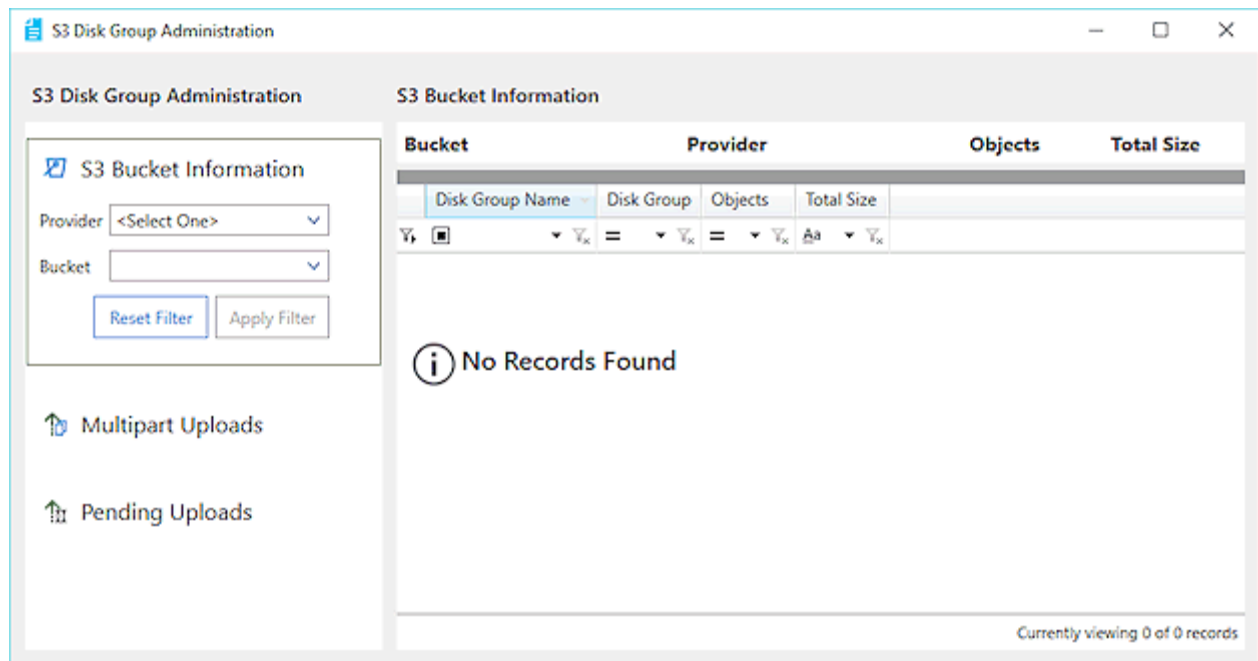
1. Select a Disk Group that an S3 Disk Group Analysis Rule had been configured for previously. For more information on configuring these rules, see [S3 Disk Group Analysis Rules on page 79](#).
2. To limit the range for the analysis click either the **From** or **To** checkboxes and select a date from the drop down menu. Limiting the date range is optional.
3. Click **Queue Analysis Job**. The job is then queued to run at the next scheduled time. Queued jobs are added to the **Analysis Jobs** tab of the **S3 Disk Group Administration** window.

Viewing the Status of S3 Buckets

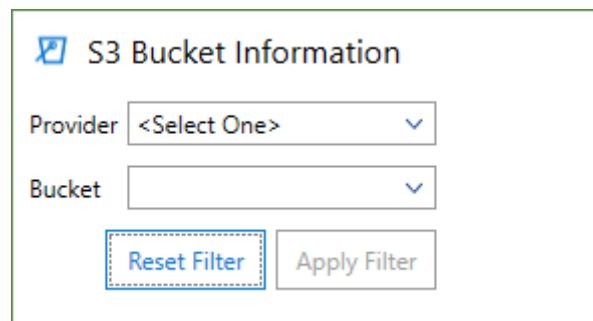
The **S3 Bucket Information** tab displays information about an S3 bucket in use, including the name of the Disk Groups in use on the bucket, the Disk Group number, the number of objects stored in the bucket, and the total size of all files stored on the bucket.

To view the status of S3 buckets in use in **S3 Disk Group Administration**:

1. Click **S3 Bucket Information**. The **S3 Bucket Information** tab is displayed on the right with no buckets listed. The S3 Bucket Information filter options are displayed on the left.



2. Select the filter options to determine the jobs displayed in the queue.



The S3 Bucket Information filter has the following options:

Filter Option	Description
Provider	Select an S3 provider from this drop-down list of configured S3 providers. For more information on configuring S3 Providers, see Configuring an S3 Provider on page 56 .
Bucket	Select a bucket from this drop-down list of configured buckets. Buckets are configured during the initial configuration of an S3 Disk Group. For information on configuring buckets, see Configuring an S3 Disk Group on page 53 .

3. Once the desired filter options are selected, click **Apply Filter** to show all buckets that meet the filter options selected. If you want to clear all options, click **Reset Filter**.

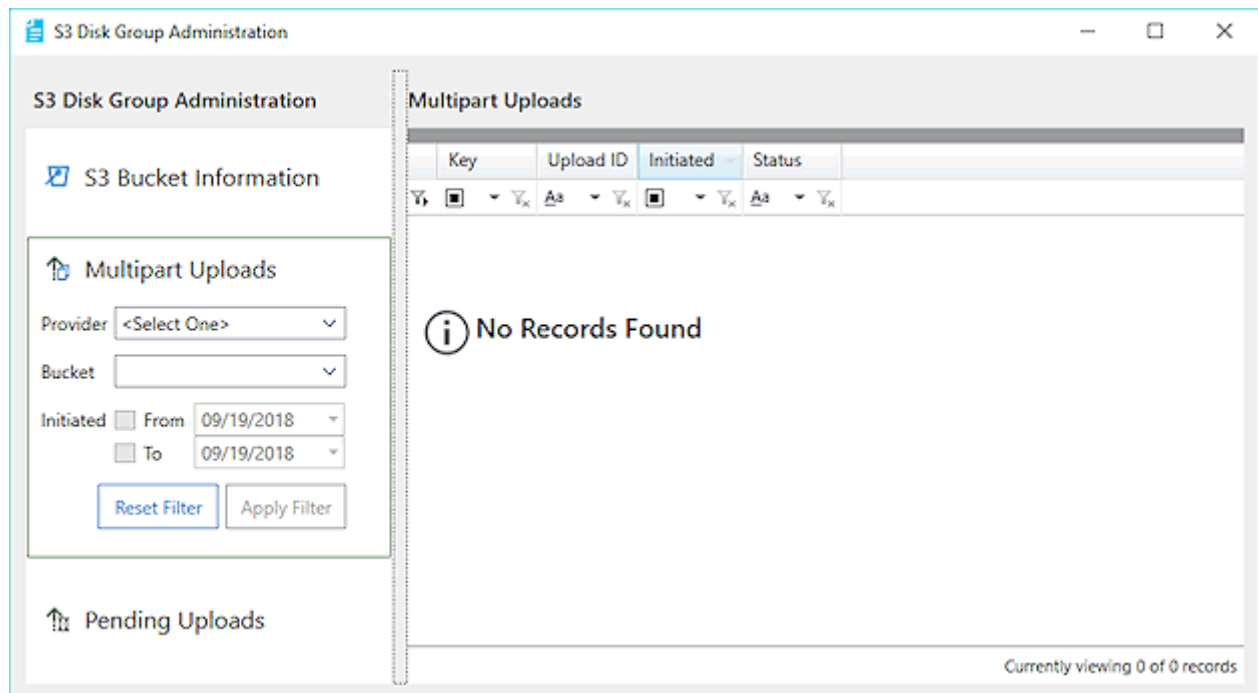
Once a filter has been applied, you can right-click in the list of buckets and select **Refresh** to update the list.

Viewing the Status of Multipart Uploads

The **Multipart Uploads** tab displays information about any multipart uploads for a selected S3 provider and bucket. This information includes a key number for the upload, an upload ID, the date and time the upload was initiated, and the status of the upload. For more information on multipart uploads, see [Multipart Uploads on page 74](#). Once a multipart upload is successfully completed, it does not appear in this tab.

To view the status of multipart uploads in use in **S3 Disk Group Administration**:

1. Click **Multipart Uploads**. The **Multipart Uploads** tab is displayed on the right with no uploads listed. The Multipart Upload filter options are displayed on the left.



2. Select the filter options to determine the jobs displayed in the queue.

The Multipart Uploads filter has the following options:

Filter Option	Description
Provider	Select an S3 provider from this drop-down list of configured S3 providers. For more information on configuring S3 Providers, see Configuring an S3 Provider on page 56 .
Bucket	Select a bucket from this drop-down list of configured buckets. For information on configuring buckets, see Configuring an S3 Disk Group on page 53 .
Initiated	Enable the From and To options to limit the multipart uploads to those started within that date range. Select the date or each From and To from the respective drop-down lists. The date for From and To defaults to today.

3. Once the desired filter options are selected, click **Apply Filter** to show all buckets that meet the filter options selected. If you want to clear all options, click **Reset Filter**.

Once a filter has been applied, you can right-click in the list of uploads and select **Refresh** to update the list.

Multipart Upload Statuses

Multipart uploads shown in the **Multipart Upload** tabs can have several statuses that have different meanings. These statuses include:

Status	Description
In Progress	The multipart upload is in the process of being uploaded to the S3 Provider or is less than 24 hours old.

Status	Description
Orphaned	The multipart upload has been awaiting upload for more than 24 hours without being able to be uploaded. For information on canceling these uploads, see Abandoning Orphaned Files on page 68 .
Indeterminate	The multipart upload was unable to be uploaded due to an error in the S3 configuration. Possible issues include an incorrectly formatted key or an issue on the part of the S3 Provider.

Abandoning Orphaned Files

If a multipart upload has the Orphaned status, it can be canceled in the **Multipart Uploads** tab of the S3 Disk Group Administration window.

To cancel a multipart upload in the **Multipart Uploads** tab:

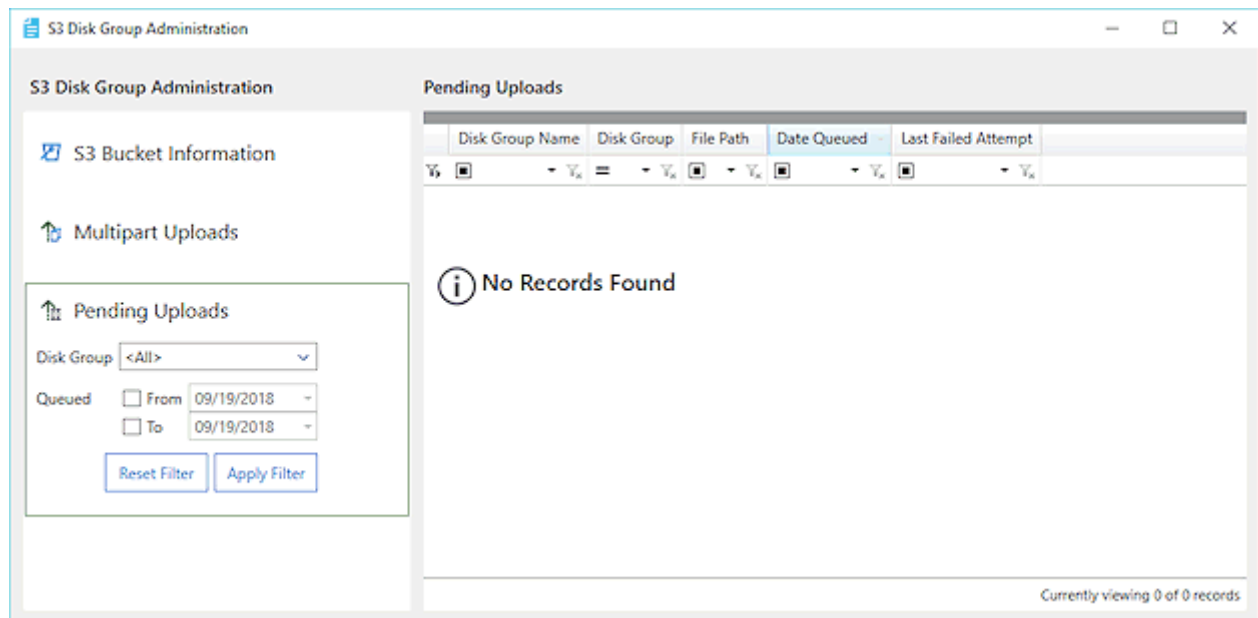
1. Select the multipart upload with the **Orphaned** status in the tab that you wish to cancel.
2. Right-click on the multipart upload.
3. Click **Abort** to cancel the multipart upload.
4. Click **OK** to confirm the cancellation. The multipart upload is removed from the tab.

Viewing Pending Uploads

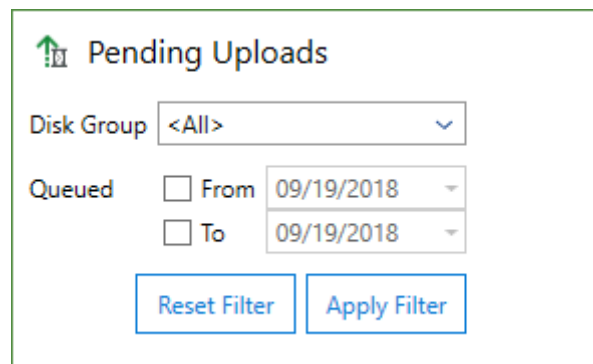
The **Pending Uploads** tab displays information about any uploads from the S3 Upload Cache that are scheduled for upload. These tasks will be uploaded when the next S3 Upload Cache Processing task is executed in the Unity Scheduler. For more information on the S3 Upload Cache, see [Configuring S3 Upload Cache Processing on page 62](#).

To view the status of pending uploads in use in **S3 Disk Group Administration**:

1. Click **Pending Uploads**. The **Pending Uploads** tab is displayed on the right with no uploads listed. The Pending Upload filter options are displayed on the left.



2. Select the filter options to determine the jobs displayed in the queue.



The Pending Uploads filter has the following options:

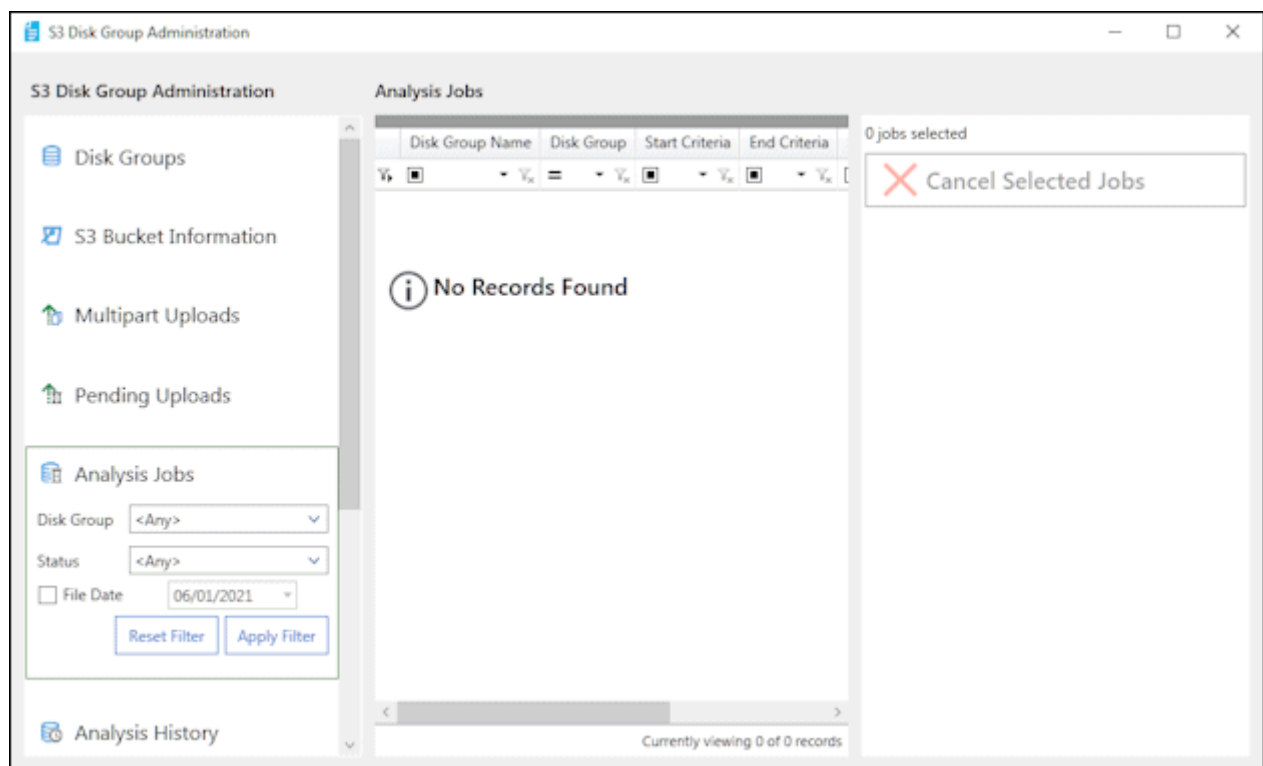
Filter Option	Description
Disk Group	Select an S3 Disk Group from the this drop-down list.
Queued	Enable the From and To options to limit the pending uploads to those queued within that date range. Select the date or each From and To from the respective drop-down lists. The date for From and To defaults to today.

- Once the desired filter options are selected, click **Apply Filter** to show all pending uploads that meet the filter options selected. If you want to clear all options, click **Reset Filter**.

Once a filter has been applied, you can right-click in the list of uploads and select **Refresh** to update the list.

Viewing Analysis Jobs

The **Analysis Jobs** tab displays analysis jobs that have been queued in the Disk Groups tab. For more information, see [Viewing S3 Disk Groups on page 64](#). These jobs will be completed when the next Disk Group Analysis Processing for S3 Disk Groups task is executed in the Unity Scheduler. For more information on configuring this task, see [Disk Group Analysis Processing for S3 Disk Groups on page 114](#).



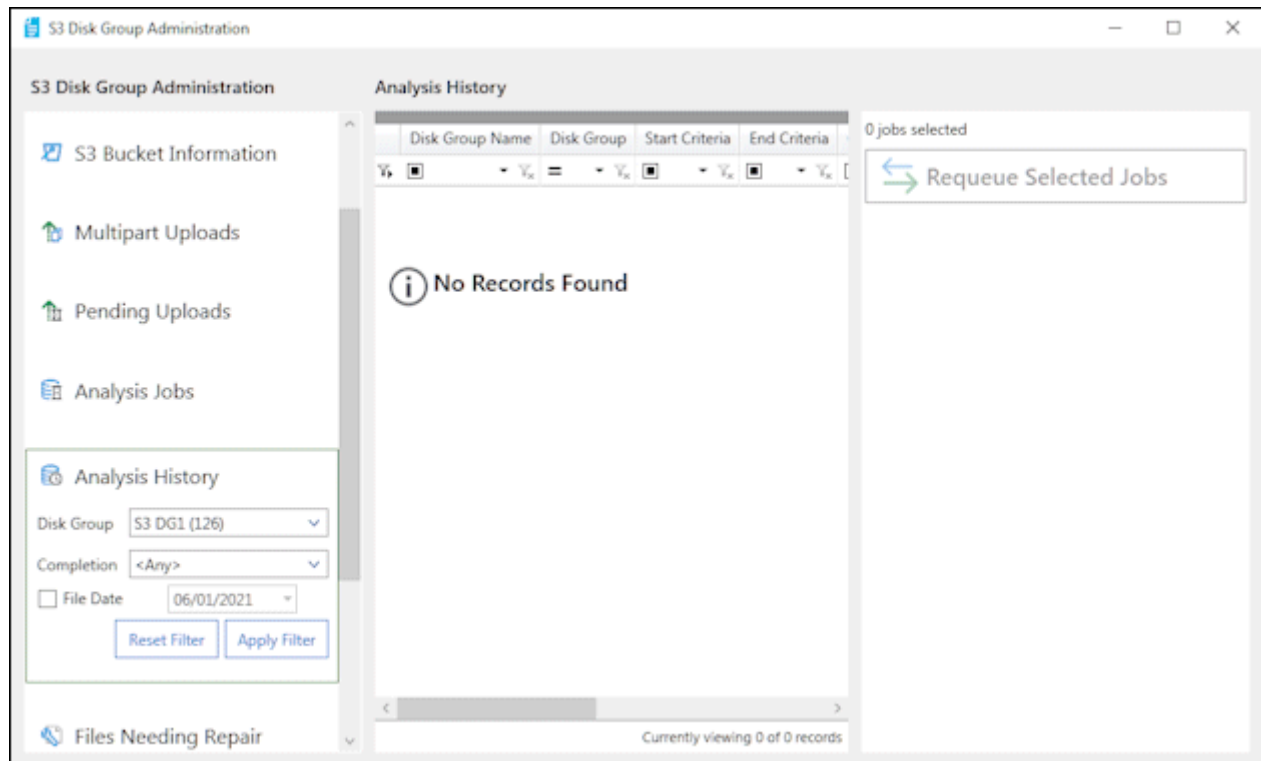
To view an analysis job or filter the view of analysis jobs:

- Select an S3 Disk Group from the **Disk Group** drop down menu.
- Select the status of the job from the **Status** drop down menu. Statuses include **Preparing**, **Pending**, **Processing**, and **Awaiting Cleanup**.
- To filter for jobs queued on a specific date, click the File Date checkbox and select a date from the drop down menu.
- Click **Apply Filter** to display analysis jobs that meet the selected requirements. To clear the selections, click **Reset Filter**.

Jobs can be canceled in this tab by selecting the job and clicking **Cancel Selected Jobs**.

Viewing Completed Analysis Jobs

The **Analysis History** tab displays analysis jobs that have been canceled or completed.



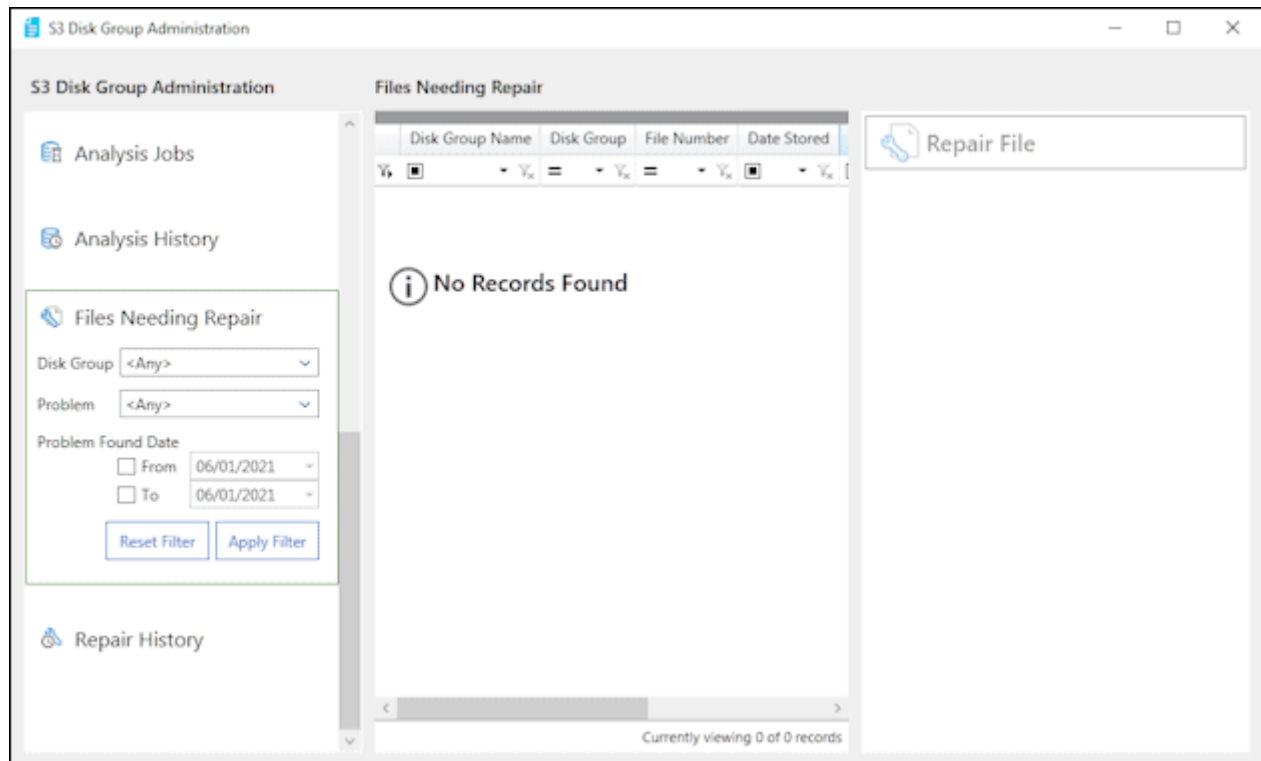
To view a completed/canceled analysis job or filter the view of completed/canceled analysis jobs:

1. Select an S3 Disk Group from the **Disk Group** drop down menu.
2. Select the status of the job from the **Completion** drop down menu. Statuses include **Completed** and **Canceled**.
3. To filter for jobs queued on a specific date, click the File Date checkbox and select a date from the drop down menu.
4. Click **Apply Filter** to display analysis jobs that meet the selected requirements. To clear the selections, click **Reset Filter**.

Jobs can be requeued in this tab by selecting the job and clicking **Requeue Selected Jobs**.

Viewing Files Needing Repair

The **Files Needing Repair** tab displays any files determined by analysis to need repairing.



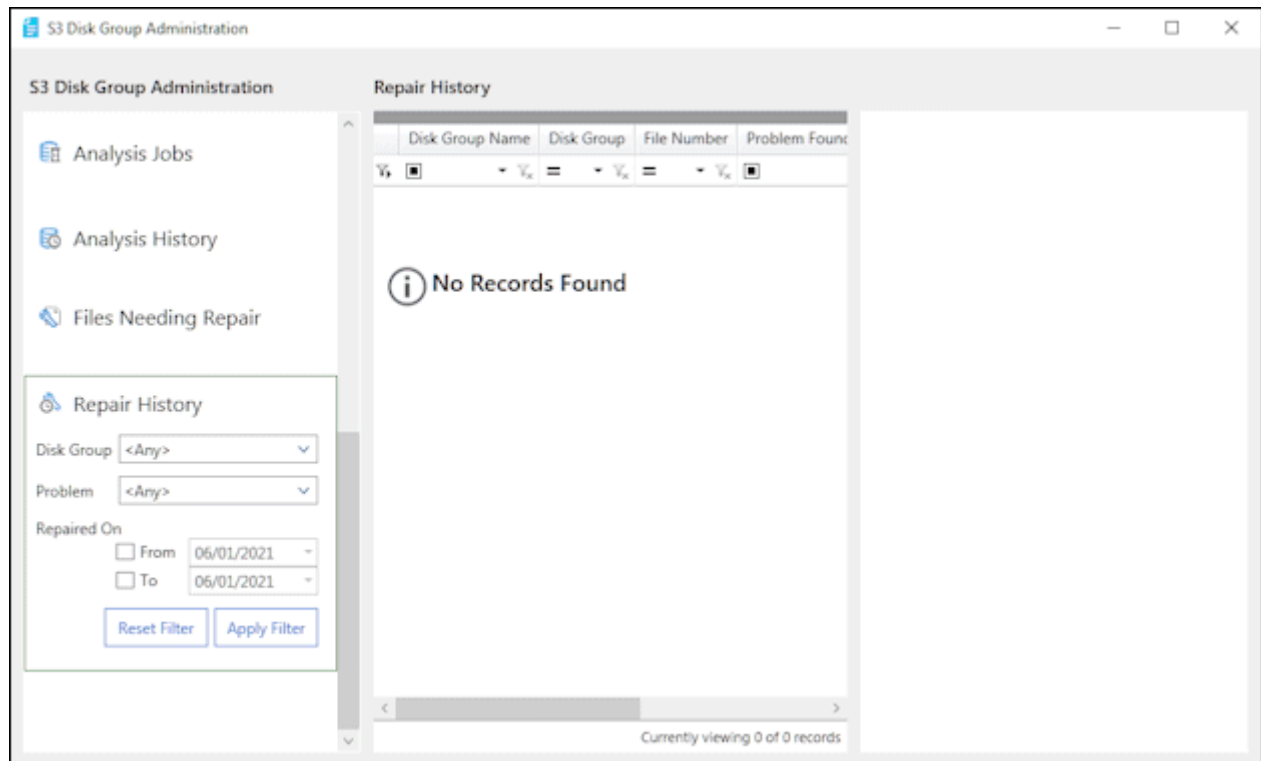
To view files needing repair or filter the view of files:

1. Select an S3 Disk Group from the **Disk Group** drop down menu.
2. Select an problem for the files from the **Problem** drop down menu. Problems include **Missing File**, **Error**, and **Incorrect Size**. If no problem is selected, all files that meet the other requirements are shown.
3. To filter for files for a specific date, click the **Problem Found Date** checkbox you wish to filter for. After clicking **From** or **To**, select a date from the drop down menu. If no date is selected, all files fitting the other requirements are shown.
4. Click **Apply Filter** to display analysis jobs that meet the selected requirements. To clear the selections, click **Reset Filter**.

Files can be repaired by selecting the desired file and clicking **Repair File**.

Viewing Repaired Files

The **Repair History** tab displays any analyzed files that have been repaired.



To view repaired files or filter the view of those files:

1. Select an S3 Disk Group from the **Disk Group** drop down menu.
2. Select an problem for the files from the **Problem** drop down menu. Problems include **Missing File**, **Error**, and **Incorrect Size**. If no problem is selected, all files that meet the other requirements are shown.
3. To filter for files for a specific date, click the **Repaired On** checkbox you wish to filter for. After clicking **From** or **To**, select a date from the drop down menu. If no date is selected, all files fitting the other requirements are shown.
4. Click **Apply Filter** to display analysis jobs that meet the selected requirements. To clear the selections, click **Reset Filter**.

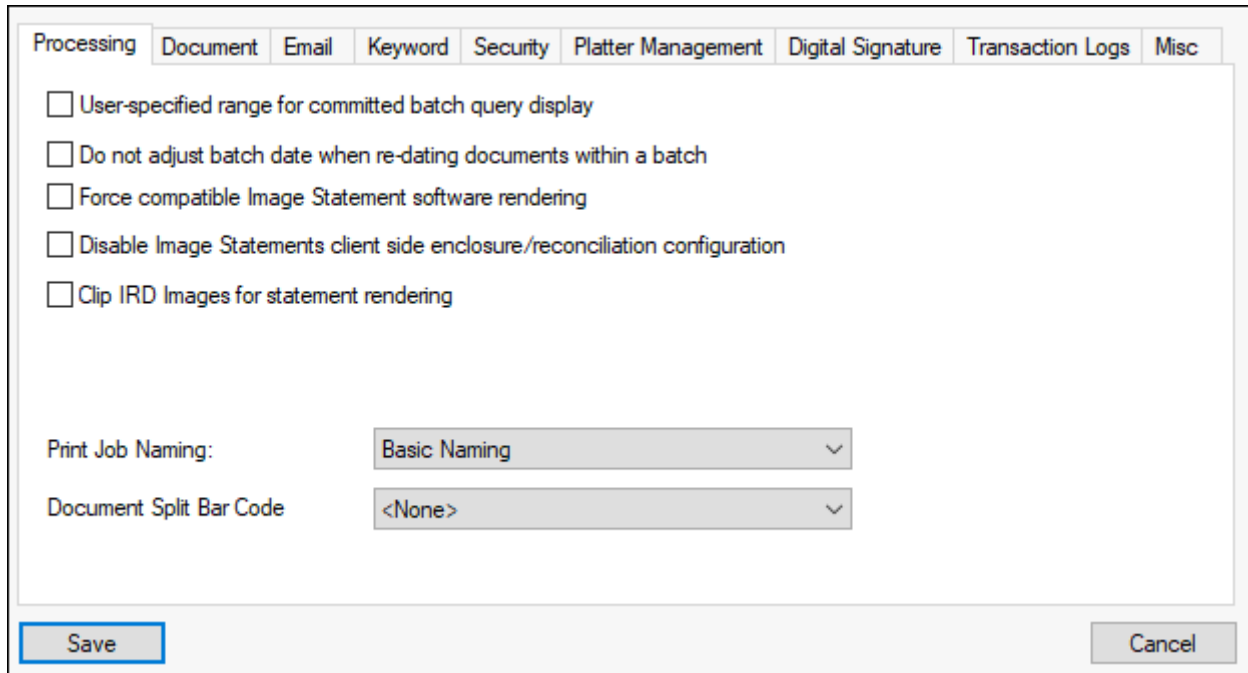
Multipart Uploads

When uploading files over a configured size limit to an S3 Provider, files are divided into multiple different parts for upload. By default, files larger than 100 MB are split into smaller parts for upload. As the smaller parts are uploaded, their progress can be tracked in the S3 Disk Group Administration window in the Client. For more information on this window, see [S3 Disk Group Administration on page 63](#). The size of these smaller parts is called the S3 multipart upload threshold and can be configured to different sizes. For more information this configuration, see [The file size at which a multipart upload is triggered is known as the S3 multipart upload threshold. This file size defaults to 100 MB but can be changed if needed. on page 74](#).

The file size at which a multipart upload is triggered is known as the S3 multipart upload threshold. This file size defaults to 100 MB but can be changed if needed.

To change the S3 Multipart Upload Threshold in Configuration:

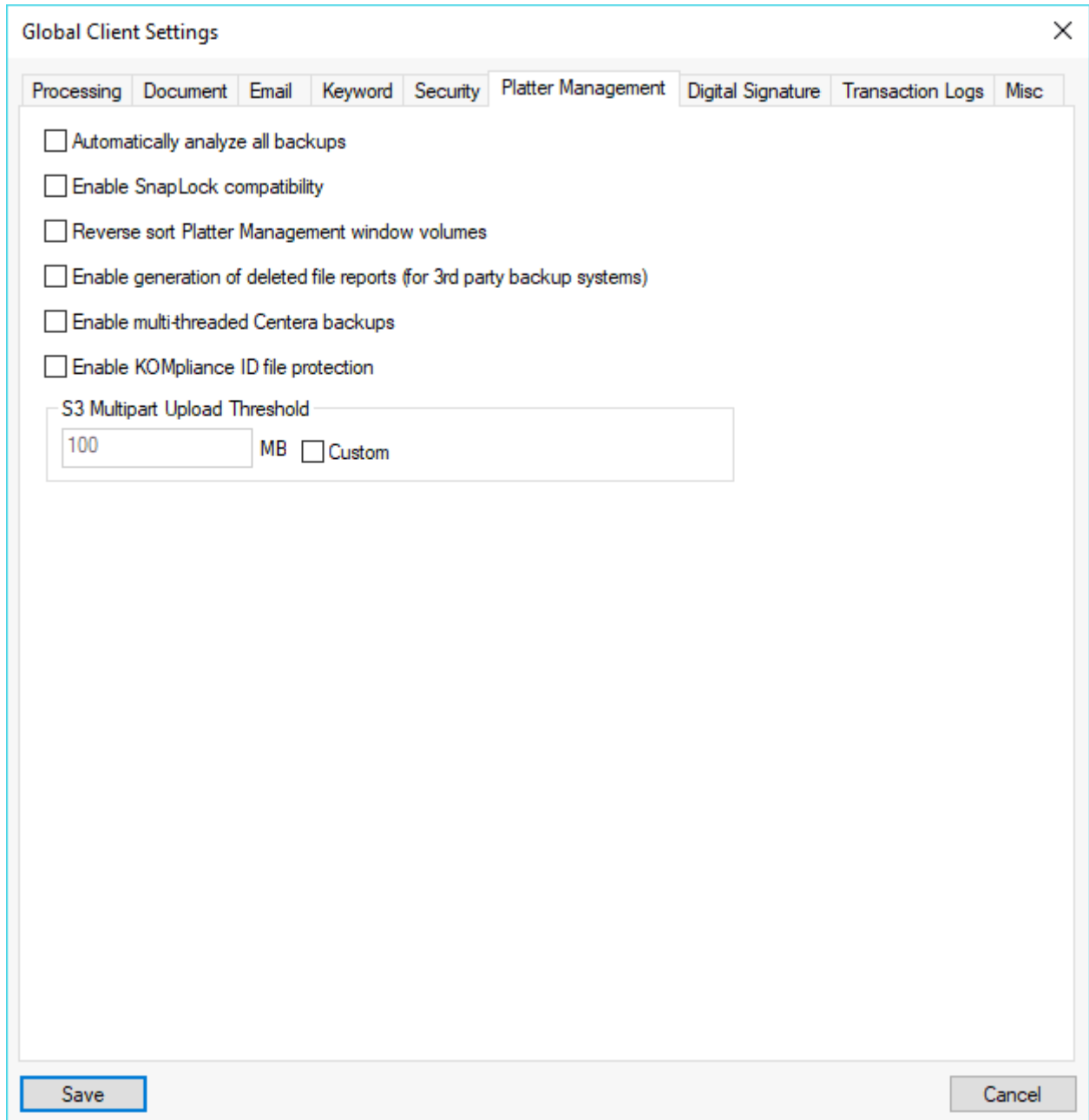
1. Select **Users | Global Client Settings**. The **Global Client Settings** window is displayed.



The image shows a software window titled "Global Client Settings". At the top, there is a horizontal tab bar with the following tabs: "Processing", "Document", "Email", "Keyword", "Security", "Platter Management", "Digital Signature", "Transaction Logs", and "Misc". The "Processing" tab is currently selected. Below the tabs, there is a list of five unchecked checkboxes with the following labels: "User-specified range for committed batch query display", "Do not adjust batch date when re-dating documents within a batch", "Force compatible Image Statement software rendering", "Disable Image Statements client side enclosure/reconciliation configuration", and "Clip IRD Images for statement rendering". Below these checkboxes, there are two rows of settings. The first row is labeled "Print Job Naming:" and has a dropdown menu showing "Basic Naming". The second row is labeled "Document Split Bar Code" and has a dropdown menu showing "<None>". At the bottom of the window, there are two buttons: "Save" on the left and "Cancel" on the right.

Processing	Document	Email	Keyword	Security	Platter Management	Digital Signature	Transaction Logs	Misc
<input type="checkbox"/> User-specified range for committed batch query display								
<input type="checkbox"/> Do not adjust batch date when re-dating documents within a batch								
<input type="checkbox"/> Force compatible Image Statement software rendering								
<input type="checkbox"/> Disable Image Statements client side enclosure/reconciliation configuration								
<input type="checkbox"/> Clip IRD Images for statement rendering								
Print Job Naming:				Basic Naming				
Document Split Bar Code				<None>				
Save				Cancel				

2. Click the **Platter Management** tab. The Platter Management settings are displayed.

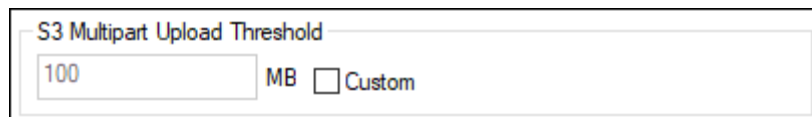


The image shows a 'Global Client Settings' dialog box with a close button (X) in the top right corner. The 'Platter Management' tab is selected among several tabs: Processing, Document, Email, Keyword, Security, Platter Management, Digital Signature, Transaction Logs, and Misc. The settings area contains several checkboxes and a threshold setting:

- ☐ Automatically analyze all backups
- ☐ Enable SnapLock compatibility
- ☐ Reverse sort Platter Management window volumes
- ☐ Enable generation of deleted file reports (for 3rd party backup systems)
- ☐ Enable multi-threaded Centera backups
- ☐ Enable KOMpliance ID file protection

The 'S3 Multipart Upload Threshold' section includes a text box with the value '100', the unit 'MB', and a checkbox for 'Custom' which is currently unchecked. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

3. Select the **Custom** option in the **S3 Multipart Upload Threshold** box.



This image is a close-up of the 'S3 Multipart Upload Threshold' section from the previous dialog. It shows a text box containing '100', followed by 'MB', and a checkbox labeled 'Custom' which is now checked.

4. Once the option is selected, the text field for the threshold size is available for editing. Type a numeric value into this field for the threshold size in MB. By default, this size is set to 100 MB.
5. Click **Save** to store the settings. The **Global Client Settings** window is closed.

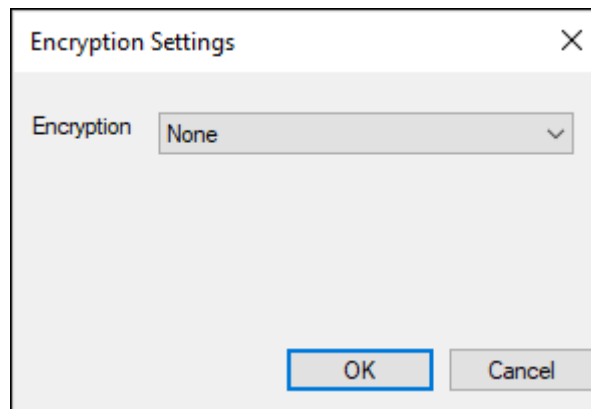
KMS Encryption

KMS encryption is available only for S3 Disk Groups and requires using a provider that supports the encryption. KMS encryption is primarily used with Amazon S3 storage, but may be supported by other providers. Contact your provider to ensure they support KMS encryption before attempting to use it. If supported, you should receive a KMS key from the provider.

Configuring KMS Encryption

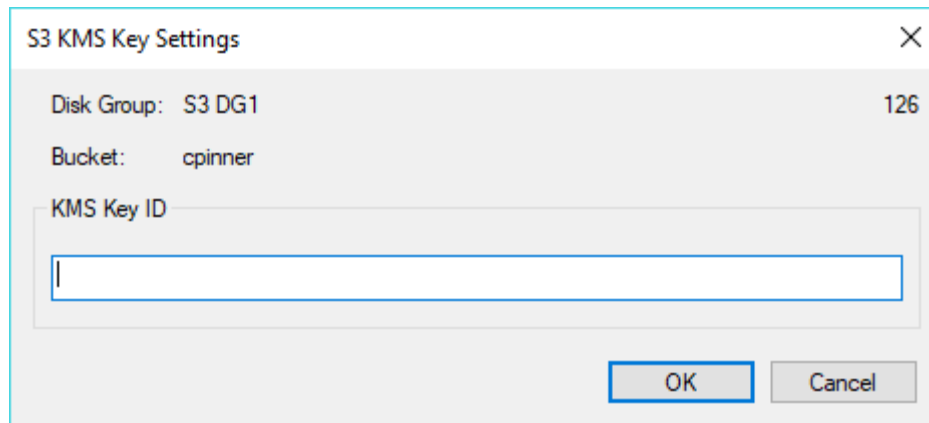
KMS encryption can be configured in the **Disk Group Settings** dialog box for S3 Disk Groups, which can be accessed in Configuration during S3 Disk Group creation or from the **S3 Disk Group Configuration** dialog box by clicking Settings. To configure KMS encryption in the **Disk Group Settings** dialog box:

1. Click **Change Encryption**. The Encryption Settings dialog box is displayed.



2. Select **S3 KMS** from the Encryption drop-down list.

- Click **OK**. The **S3 KMS Key Settings** dialog box is displayed.



- Type the KMS key provided by your S3 provider into the **KMS Key ID** field.

Note: The KMS key must match the region of the configured S3 Bucket.

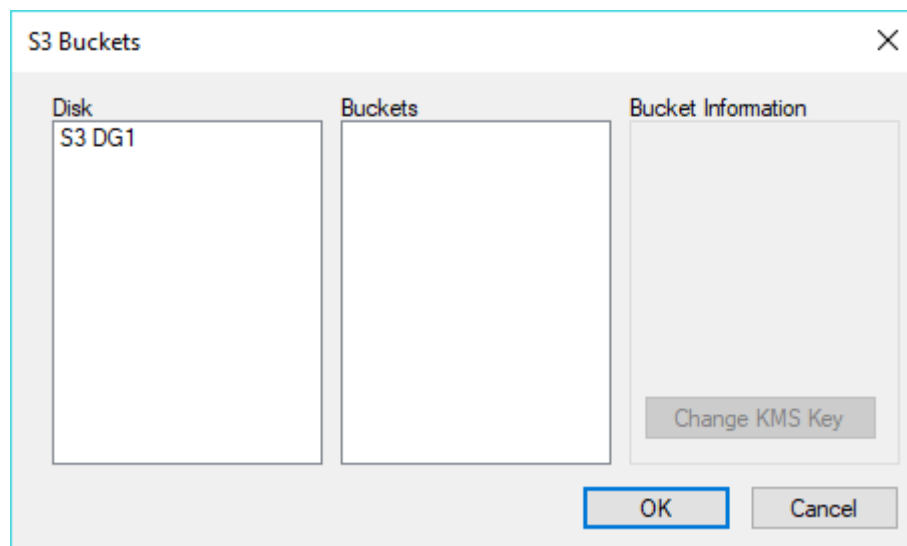
- Click **OK**. The **S3 KMS Key Settings** dialog box is closed.

Rotating the KMS Key

The KMS key can be rotated as needed for compliance or any other reason. A new key must be provided by your S3 provider when necessary.

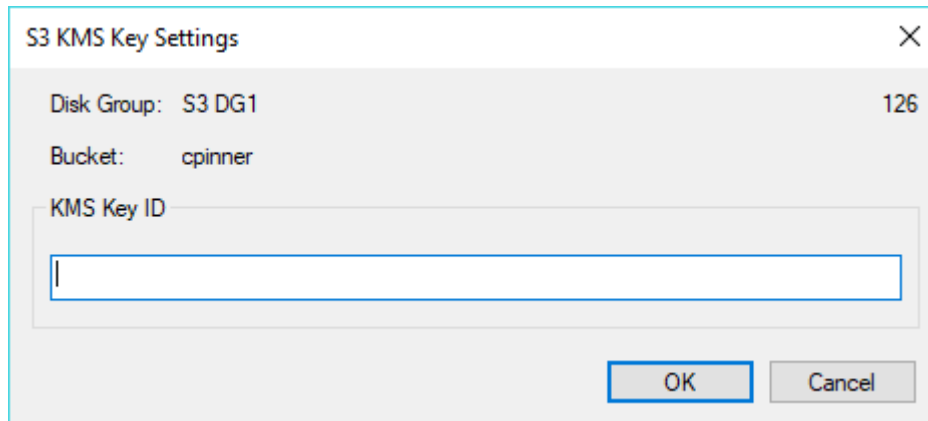
To change a KMS key in Configuration:

- Click on **Disk Mgmt | S3 Disk Groups | S3 Bucket Configuration**. The **S3 Buckets** dialog box is displayed.



- Select the Disk Group and Bucket to change the KMS key for. If KMS encryption is used on that Bucket, the **Change KMS Key** button will become enabled.

3. Click **Change KMS Key**. The **S3 KMS Key Settings** dialog box is displayed. If a key is already in use, it is displayed in the **KMS Key ID** field.

The image shows a dialog box titled "S3 KMS Key Settings" with a close button (X) in the top right corner. Inside the dialog, there are three fields: "Disk Group:" with the value "S3 DG1", "Bucket:" with the value "cpinner", and "KMS Key ID" which is an empty text box. To the right of the "Disk Group:" field is the number "126". At the bottom right of the dialog are two buttons: "OK" and "Cancel".

4. Replace the key in the **KMS Key ID** field with the new key.

Note: The KMS key must match the region of the configured S3 Bucket.

5. Click **OK**. The **S3 KMS Key Settings** dialog box closes. The key is validated to ensure that it properly functions with the S3 Provider as configured.
6. In the **S3 Buckets** dialog box, click **OK**.

S3 Disk Group Analysis

S3 Disk Group Analysis is performed using scheduled tasks in the **Unity Scheduler**. Rules must be created in the **S3 Disk Group Analysis Rules** dialog box in **Configuration** prior to the task being run. After the task has been completed, the results of analysis can be viewed in the **S3 Disk Group Administration** dialog box in the **Client**.

For more information on each part of the S3 Analysis process, see:

- [S3 Disk Group Analysis Rules on page 79](#)
- [Running Analysis Jobs on page 84](#)

S3 Disk Group Analysis Rules

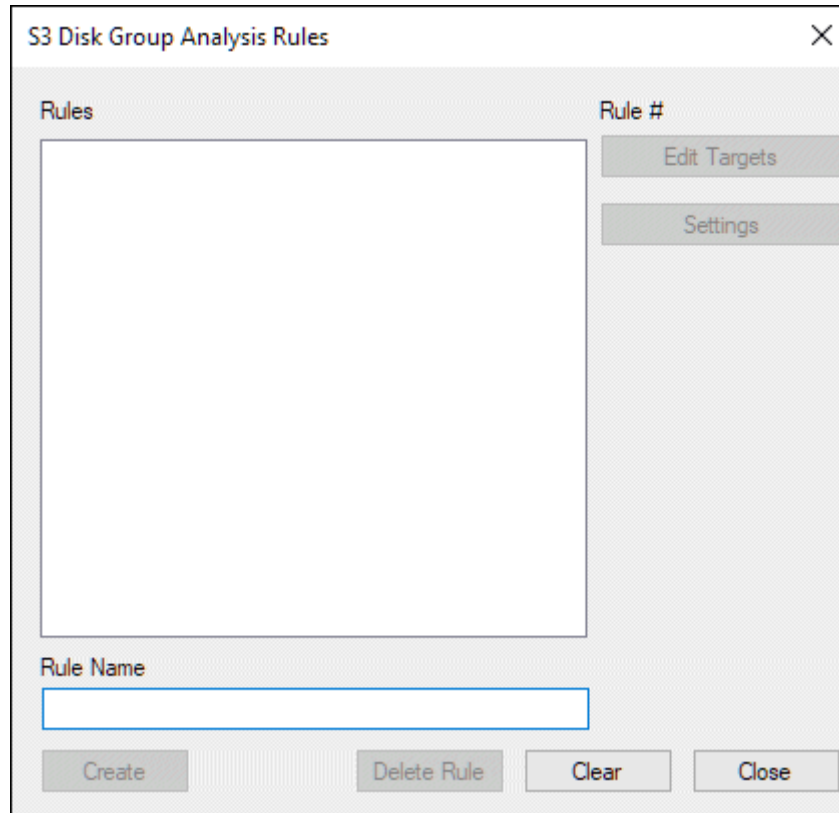
The rules used for S3 Disk Group Analysis are configured in Configuration. These rules determine what happens when the S3 Disk Group Analysis task is executed by the Unity Scheduler. For more information on S3 Disk Analysis Rules, see:

- [Creating an S3 Disk Group Analysis Rule on page 80](#)
- [Editing the Settings of an S3 Disk Group Analysis Rule on page 82](#)

Creating an S3 Disk Group Analysis Rule

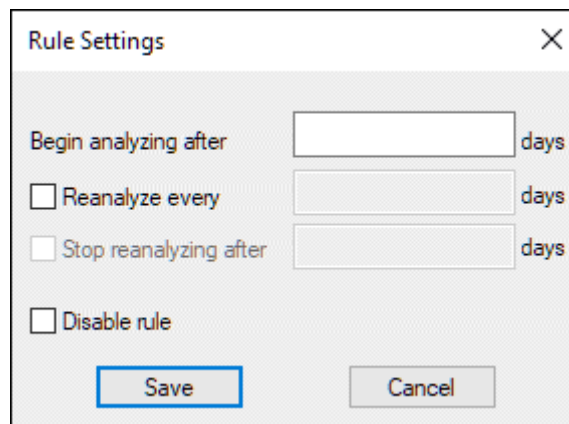
To create an S3 analysis rule in **Configuration**:

1. Select **S3 Analysis Rules** from the **Disk Mgmt** menu. The **S3 Disk Group Analysis Rules** dialog box is displayed.

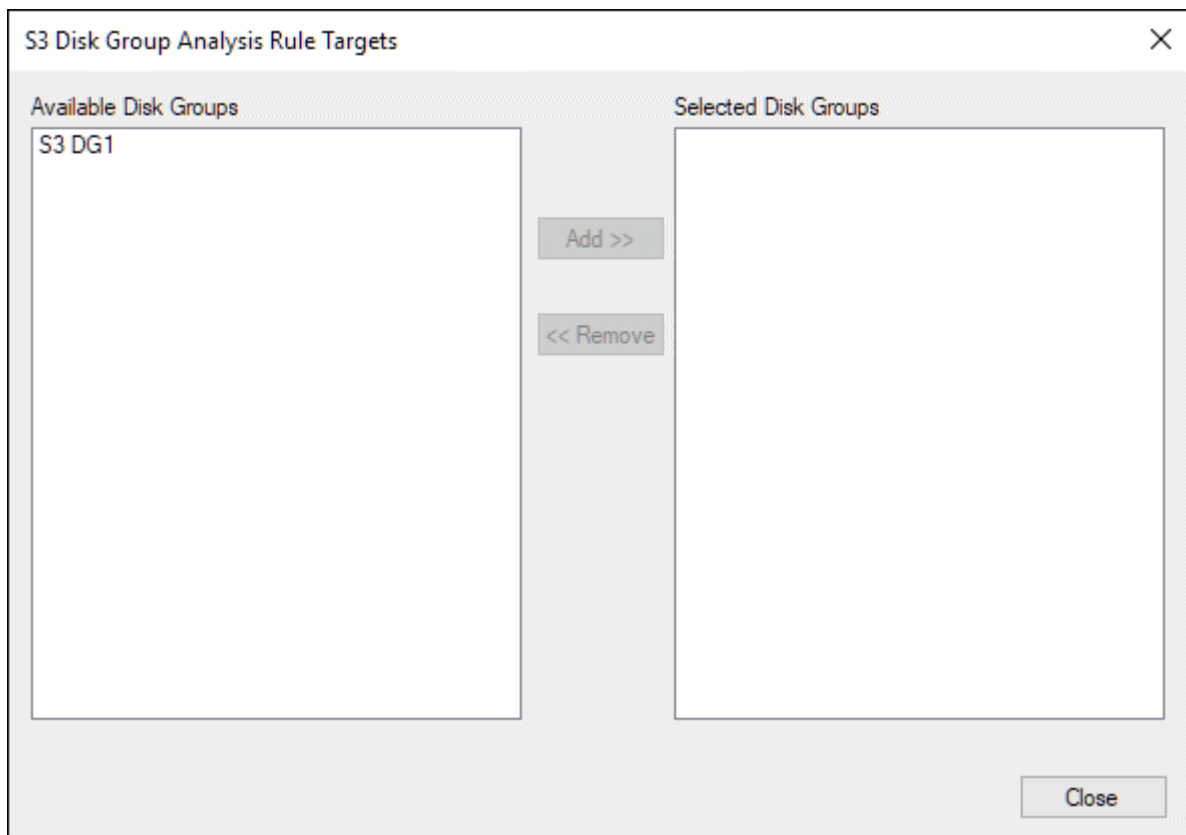
The screenshot shows a dialog box titled "S3 Disk Group Analysis Rules" with a close button (X) in the top right corner. The dialog is divided into two main sections. The left section, labeled "Rules", contains a large empty rectangular box for displaying a list of rules. The right section, labeled "Rule #", contains two buttons: "Edit Targets" and "Settings". Below the "Rules" list box is a text input field labeled "Rule Name". At the bottom of the dialog, there are four buttons: "Create", "Delete Rule", "Clear", and "Close".

Any previously configured S3 analysis rules are shown in the **Rules** list.

2. Type the name of the rule you wish to create into the **Rule Name** text box.
3. Click **Create**. The **Rule Settings** dialog box is displayed.

The screenshot shows a dialog box titled "Rule Settings" with a close button (X) in the top right corner. The dialog contains several settings: a text input field for "Begin analyzing after" followed by "days"; a checkbox labeled "Reanalyze every" followed by a text input field and "days"; a checkbox labeled "Stop reanalyzing after" followed by a text input field and "days"; and a checkbox labeled "Disable rule". At the bottom, there are two buttons: "Save" and "Cancel".

4. Enter the number of days that must pass before the **S3 Analysis** occurs in the Begin analyzing after text box.
5. To perform the analysis repeatedly, click the **Reanalyze every** check box and enter a number of days into the text box. This determines the number of days that pass between analyses being performed. If the **Reanalyze every** check box is enabled, the **Stop reanalyzing after** check box becomes available.
6. To stop reanalysis from occurring after a certain amount of time, click the **Stop reanalyzing after** check box and enter the total number of days that should pass before reanalysis stops.
7. To disable the rule, click the **Disable rule** checkbox. Any rule that is not disabled will be run by the Unity Scheduler once the appropriate task is run.
8. Click **Save** to save the rule settings. The newly created rule is added to the Rules list in the **S3 Disk Group Analysis Rules** dialog box.
9. Select the rule you created from the list of available rules and click the **Edit Targets** button to specify the S3 Disk Group to analyze. The **S3 Disk Group Analysis Rule Targets** dialog box is displayed.



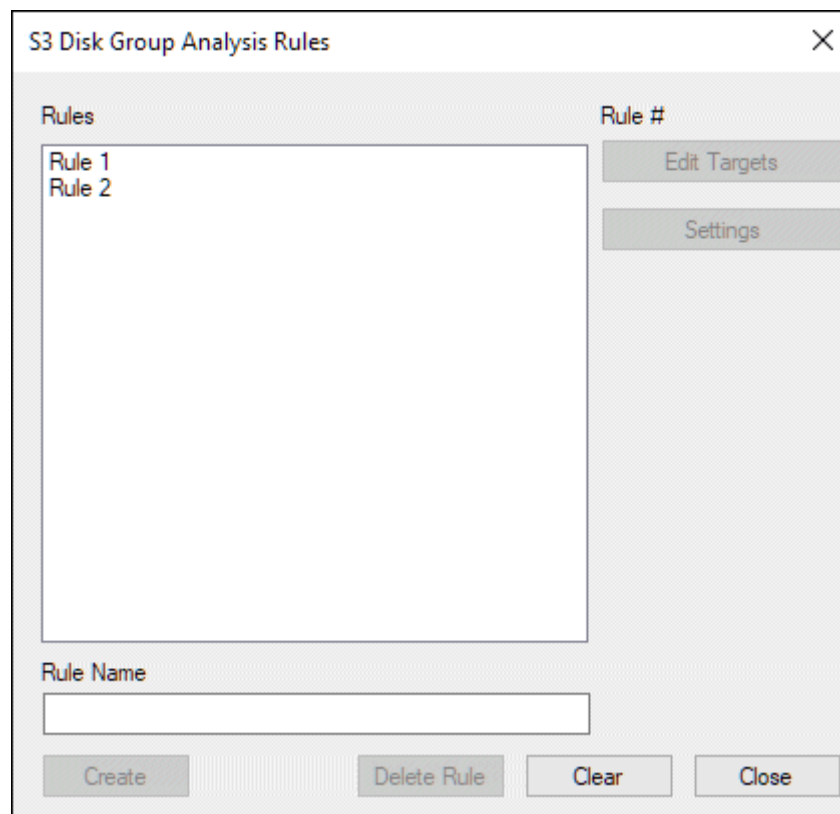
10. To add a Disk Group to analyze, select the Disk Group from the **Available Disk Groups** and click the **Add >>** button. The Disk Group is moved to the **Selected Disk Groups** list. Multiple Disk Groups can be added using this method.

11. To remove a Disk Group and prevent analysis, select the Disk Group from the **Selected Disk Groups** and click the **<< Remove** button. The Disk Group is moved to the **Available Disk Groups** list. Multiple Disk Groups can be removed using this method.
12. Once the Selected Disk Groups list includes all of the Disk Groups you want to analyze, click Close to close the **S3 Disk Group Analysis Rule Targets**.
13. Click **Close** in the **S3 Disk Group Analysis Rules** dialog box once all rules have been created.

Editing the Settings of an S3 Disk Group Analysis Rule

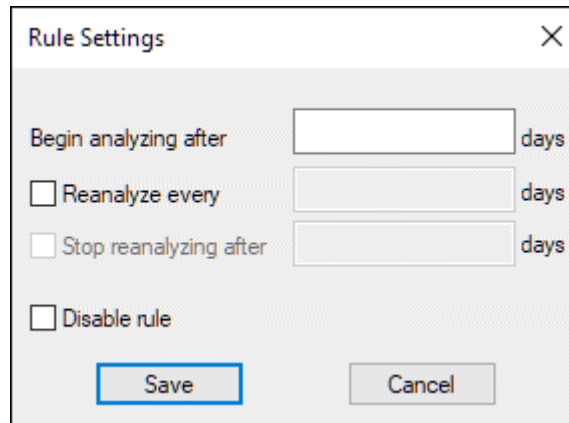
To edit an **S3 Analysis Rule** in the **Configuration** module:

1. Select **S3 Analysis Rules** from the **Disk Mgmt** menu. The **S3 Disk Group Analysis Rules** dialog box is displayed.



If no rules are displayed in the Rules list, you cannot edit any rules. for information on creating a rule, see [Creating an S3 Disk Group Analysis Rule on page 80](#).

2. To change the settings for a rule, select the rule from the **Rules** list and click **Settings**. The **Rule Settings** dialog box is displayed.

The image shows a 'Rule Settings' dialog box with a close button (X) in the top right corner. It contains four settings: 'Begin analyzing after' with a text input field and 'days' label; 'Reanalyze every' with a checkbox, a text input field, and 'days' label; 'Stop reanalyzing after' with a checkbox, a text input field, and 'days' label; and 'Disable rule' with a checkbox. At the bottom are 'Save' and 'Cancel' buttons. The 'Save' button is highlighted with a blue border.

Rule Settings

Begin analyzing after days

☐ Reanalyze every days

☐ Stop reanalyzing after days

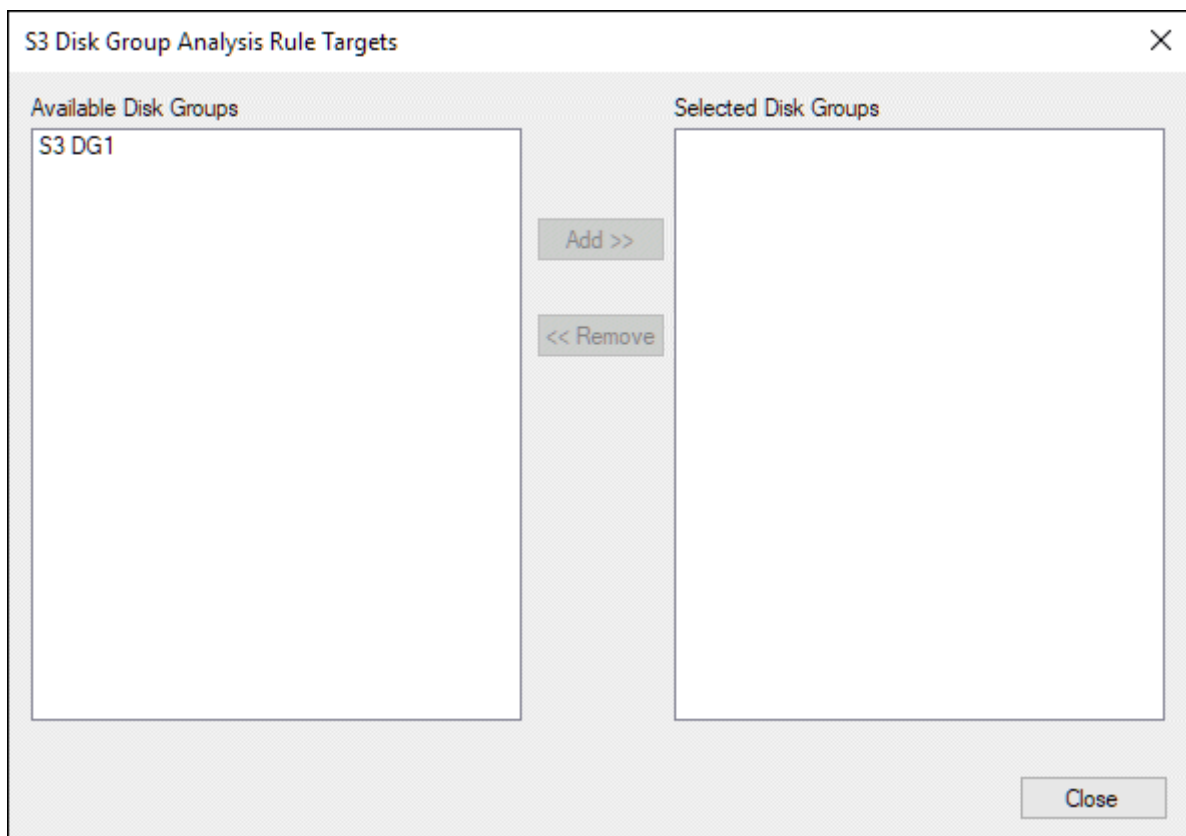
☐ Disable rule

Save Cancel

These settings include:

- **Begin analyzing after** is the number of days that pass before the S3 analysis is completed.
 - **Reanalyze every** includes the number of days that should pass between the analysis being run again once it is begun. Click the checkbox to enable this option.
 - **Stop reanalyzing after** is the number of days after which the analysis rule stops being repeated. This option is only available if **Reanalyze after** is enabled. Click the checkbox to enable this option
 - **Disable rule** allows you to prevent the rule from running if you want to run it at a later date.
3. Change the settings as desired and click **Save**. The **Rule Settings** dialog box is closed.

4. To change the targets for a rule, select the rule from the **Rules** list and click **Edit Targets**. The **S3 Disk Group Analysis Rule Targets** dialog box is displayed.



5. Select Disk Groups to target from the **Available Disk Groups** list and click **Add >>** to move the Disk Group to the **Selected Disk Groups** list. To remove a Disk Group from the **Selected Disk Groups** list, select the Disk Group and click **<< Remove**.
6. Click Close to save the target settings. the **S3 Disk Group Analysis Rule Targets** dialog box is closed.

Running Analysis Jobs

Once an analysis rule has been created, the rule is run by queuing an analysis job in the S3 Disk Group Administration window. For more information on this window and how to use it for S3 analysis, see [S3 Disk Group Administration on page 63](#). For information on creating rules, see [S3 Disk Group Analysis Rules on page 79](#).

Once a rule has been created and queued, a **Disk Group Analysis Processing for S3 Disk Group** task must be created and scheduled in the **Unity Scheduler**. For information on this task specifically, see [Disk Group Analysis Processing for S3 Disk Groups on page 114](#). For more information on creating and scheduling a task, see the **Unity Scheduler** module reference guide.

Best Practices for S3 Disk Groups

Several best practices are recommended when using S3 disk groups, including:

- Each bucket should have only one implementation of OnBase assigned to it.
- Files may be stored within a bucket that are not part of the database configured for that bucket, but this is not recommended.
- Several paths are reserved in S3 Disk Group buckets for OnBase specific files. These include OBID.file for all disk groups as well as folders labeled **DG#** (for 64 bit Disk Groups) and **#** (for 32 bit Disk Groups) where # is equal to the Disk Group's number.
- Usage of a data center as physically close as possible is recommended due to the potential for slowdown that occurs when using any cloud based service.
- Larger files are slower to transmit and manipulate using S3. If this is a concern, usage of S3 Disk Groups is discouraged.

Overview

The use of Encrypted Disk Groups helps organizations meet compliance regulations that surround the digital storage of documents, for example the processing, storing, and transmitting of sensitive financial information, such as credit card data.

The Encrypted Disk Groups module adds an additional layer of security to your OnBase solution that can be used separately or in conjunction with the other security practices implemented by your organization.

With Encrypted Disk Groups, the documents stored in OnBase are encrypted on the physical disks, protecting the data even in the event of access to the storage location of the OnBase Disk Groups. Documents that are archived in an Encrypted Disk Group can only be opened and viewed using OnBase, helping to ensure that the security controls configured in OnBase cannot be circumvented.

Documents can be migrated from unencrypted Disk Groups to Encrypted Disk Groups using **Disk Group Migration**. Additionally, already encrypted Disk Groups can be migrated to a different encryption or fully decrypted using **Disk Group Migration**. For more information on performing this migration, see [Disk Group Migration on page 100](#).

Requirements

All of the OnBase clients support Encrypted Disk Groups. The end-user experience is not impacted when documents are stored in, and retrieved from, Encrypted Disk Groups.

Licensing

Configuring Encrypted Disk Groups requires the **Encrypted Disk Groups** database license.

Disk Group Configuration requires a **Configuration** license.

You can check your current licensing status using the OnBase Configuration module, by selecting **Product Licensing** from the **Utils** menu.

Upgrading

Disk Groups configured to use the original implementation of **AES 256** should be migrated to the current **AES 256 v2** implementation. 256-bit AES encryption was introduced in OnBase 14 and renamed to **AES 256 v1** in OnBase 14 SP 2.

Caution: OnBase 13 and earlier clients cannot archive or read documents stored in a 256-bit AES encrypted Disk Group. Before configuring **AES 256 v2** make sure all clients and the OnBase Application Server are version 14 SP 2 or higher.

Note: To configure an **AES 256 v2** Encrypted Disk Group, the **Minimum Client Version** must be at least **14.0.2.584** and the **Minimum Web Client Version** must be at least **14.0.2.128**. To configure an **AES CFB** Encrypted Disk Group, the **Minimum Client Version** and **Minimum Web Client Version** must both be at least **18.0**. These values are set in the **Utils | Version Compatibility** dialog box.

Third Party Software

If you are using encrypted disk groups in a Windows 10 environment and have Microsoft Edge configured as your default PDF viewer, you must install the Adobe Acrobat Reader DC to properly access PDF files stored on the encrypted disk group through the OnBase Client.

System Interaction

Encrypted Disk Groups are supported by most OnBase modules, however, there are a few limitations described in this section that must be considered before configuring an Encrypted Disk Group. For complete details regarding the use and configuration of the specific modules mentioned in this section, refer to the help files and/or module reference guide for that module.

Distributed Disk Services

Distributed Disk Services supports new Encrypted Disk Groups but does not support the migration of existing Disk Groups to Encrypted Disk Groups.

Document Import Processor

Self Configuring DIP Import Index files cannot be used with Encrypted Disk Groups. The file paths in the Import Index file point to encrypted files in the Disk Group, which cannot be read by other OnBase systems.

Export and Publishing

Documents archived in Encrypted Disk Groups can be included in Export or Publishing processes in an encrypted or unencrypted state. In either case, the exported documents can still be viewed using the OnBase Client or stand-alone OnBase Runtime Client. Documents exported from Encrypted Disk Groups in an encrypted state can still be imported into another OnBase system using the Import Manager.

Externally Filled Disk Group Copies

Existing Disk Groups with externally filled copies cannot be migrated to Encrypted Disk Groups because externally filled Disk Group copies are not controlled by OnBase. New Encrypted Disk Groups can have externally filled copies and the files will be encrypted on all copies.

Caution: Storage Integration for Third Party ECM Systems can be used with Encrypted Disk Groups. However, copies of documents stored in the third-party systems are stored unencrypted.

Foreign Disk Groups

Foreign Disk Groups cannot be encrypted because they are not managed by OnBase.

Storage Integration for EMC Centera

Committed or backup copies archived using Storage Integration for EMC Centera are fully supported for use with Encrypted Disk Groups.

Storage Integration for FileNet

Storage Integration for FileNet is not supported because the FileNet storage device is not able to read OnBase encryption.

Storage Integration for IBM Tivoli

Storage Integration for IBM Tivoli supports new Encrypted Disk Groups but does not support the migration of existing Disk Groups to Encrypted Disk Groups.

Committed or backup copies archived using Storage Integration for IBM Tivoli are fully supported for use with Encrypted Disk Groups.

Storage Integration for Third Party ECM Systems

Storage Integration for Third Party ECM Systems can be used with Encrypted Disk Groups. However, copies of documents stored in the third-party systems are stored unencrypted.

Configuration

Caution: Encrypted Disk Groups should not be configured without having first developed a comprehensive storage plan. While an Encrypted Disk Group is simple to configure, the ramifications of this action must be clearly understood and considered before Encrypted Disk Groups are configured.

Encrypted Disk Groups can be created using several different methods. To create a new Disk Group as an Encrypted Disk Group, see [Configuring a New Disk Group as an Encrypted Disk Group on page 89](#). Encrypting an already created Disk Group to an Encrypted Disk Group, see [Disk Group Migration on page 100](#) or [Encryption Migration on page 74](#). Both methods can be used to perform the task, but Disk Group Migration is the preferred method for ease of use.

Configuring a New Disk Group as an Encrypted Disk Group

The following items should be kept in mind with regard to Encrypted Disk Groups:

- Your system must be licensed for **Encrypted Disk Groups** to configure Encrypted Disk Groups.
- Only the Disk Group being configured is affected. In other words, encrypting one Disk Group does not encrypt every Disk Group.
- Encrypted Disk Groups can only be converted to unencrypted disk groups using the Disk Group Migration process, not using Encryption Migration.
- The encryption status is applied to all copies of the Disk Group. In other words, you cannot choose to encrypt Copy 1 of a Disk Group but not encrypt Copy 2 or Copy 3.
- Storage Integration for IBM Tivoli supports new Encrypted Disk Groups but does not support the migration of existing Disk Groups to Encrypted Disk Groups.

Caution: Encrypted Disk Groups are not supported in all scenarios. Be sure to read and understand the [System Interaction](#) section in this chapter before configuring an Encrypted Disk Group (see [System Interaction on page 87](#)).

Note: This process for encrypting a disk group has been deprecated, and will be removed from future versions. Disk Group Migration should be used instead. For more information on this, see [Disk Group Migration on page 100](#).

To configure a new Disk Group as an Encrypted Disk Group:

1. Select **Disk Mgmt | Disk Groups** in the OnBase Configuration module. The **Disk Group Configuration** dialog box is displayed.
2. Select the Disk Group to configure from the **Disk Group** list in the left pane.
3. Click **Settings**. You are prompted to lock the Disk Group.
4. Click **Lock Disk Group**. The **Disk Group Settings** dialog box is displayed.

5. Click **Change Encryption** in the **Encryption** pane. A Warning! dialog box is displayed to recommend the use of Disk Group Migration for encryption. For more information, see [Disk Group Migration on page 100](#).
6. Click **Yes** to continue. The **Encryption Settings** dialog box is displayed.
7. Select the encryption algorithm to use from the **Encryption** drop-down list.

Disk Group Settings

DOCUMENTATION

Volume Size (Kilobytes)

☒ CD

☐ DVD Small File (25 K Avg)

☐ DVD Large File (100+ K Avg)

☐ BD Small File (25K Avg)

☐ BD Large File (100+ K Avg)

☐ Custom 500000

Options

☐ Do Not Allow Automated Backups

☐ Foreign Disk Group

☐ Enable File Deletion

Encryption

Not Encrypted

Change Encryption

Number of Copies 1

Email Notifications to:

User Name

<< None >>

Authoring/Export Settings

Number of Exports 0

Number of Years to Add to Promote Date on CD/DVD Label 0

Export Manager Name

<< None >>

Legacy Options

Save Cancel

Note: The exact algorithms available for encryption depend on the **Version Compatibility** and **Encryption Suite** settings configured. For example, if **FIPS 140-2** is configured as the Encryption Suite in the Cryptography Settings then **AES CFB** is the only encryption algorithm available.

- AES 128
- AES 256 v2
- AES CFB

Note: To configure an **AES 256 v2** Encrypted Disk Group, the **Minimum Client Version** must be at least **14.0.2.584** and the **Minimum Web Client Version** must be at least **14.0.2.128**. To configure an **AES CFB** Encrypted Disk Group, the **Minimum Client Version** and **Minimum Web Client Version** must both be at least **18.0**. These values are set in the **Utils | Version Compatibility** dialog box.

Minimum version information is displayed. Ensure the version requirements can be met before completing the configuration.

8. Click **OK**. The **Encryption Settings** dialog box is closed.

9. Click **Save** in the **Disk Group Settings** dialog box. You are prompted to confirm this action if an encryption algorithm is selected.

Caution: Once a Disk Group is saved as an Encrypted Disk Group it cannot be converted to a non-encrypted Disk Group and the files contained in that Disk Group can only be viewed using OnBase.

The remainder of the Disk Group settings are configured in the same way as non-encrypted Disk Groups. For complete details regarding Disk Group configuration, see the Disk Group configuration sections in the **System Administration** module reference guide.

Maintenance

The following sections describe items specific to maintaining Encrypted Disk Groups.

Backup Procedures

When using Encrypted Disk Groups as part of your overall solution you must include the OnBase executables as part of the overall backup strategy. This is because the encryption key used by OnBase is stored in two pieces: One piece is encrypted and stored in the OnBase database and the other piece is encrypted and stored in the OnBase Client and Configuration executables.

It is important to adopt backup procedures that reflect this dependency between the OnBase database, executables, and encrypted Keywords or Disk Groups. The OnBase executables that match a particular database must be backed up and stored with that database. Documents in Encrypted Disk Groups cannot be accessed without the matching database and executables.

Key Encryption Key Rotation

The Key Encryption Key (KEK) used by OnBase is stored in two pieces. One piece is encrypted and stored in the OnBase database. The other piece is encrypted and stored in the OnBase Client and Configuration executables.

For OnBase Core Services modules, which include the Web Client and modules dependent on the OnBase Application Server, the second piece is also encrypted and stored in **Hyland.Core.GrabIcon.dll**, which is included with the OnBase Core files.

Note: If OnBase Core Services modules are part of your OnBase solution, you cannot rotate the KEK without contacting your solution provider to obtain the **GrabIcon.NET.exe** file used in this process.

You can rotate, or change, the second piece of the KEK as a security measure against outside forces (e.g., separated employees, social engineering). The concept is similar to changing a password. When you rotate the KEK, OnBase changes the piece that is stored in the OnBase software, generates new Client and Configuration executables, and creates a new copy of **Hyland.Core.GrabIcon.dll**. These files contain the new KEK piece.

Rotating the Key Encryption Key

Note: Before rotating the Key Encryption Key (KEK), it is considered a best practice to backup your database.

Rotating the KEK entails modifying certain files in your OnBase solution. These files must then be pushed out, or deployed, to user workstations. After rotating the KEK, users cannot connect to OnBase with previous versions of the OnBase Client and Configuration executables, or by using Core Services with previous versions of **Hyland.Core.GrabIcon.dll**. They can only connect to OnBase using versions of the OnBase Client and Configuration executables containing the new KEK, or by using Core Services with the new **Hyland.Core.GrabIcon.dll**.

To rotate the KEK in the OnBase Configuration module:

Note: You only need to perform these steps on the workstation that will be used to deploy the KEK. After the KEK is rotated, the new files can be copied to other user workstations, as long as those workstations are using the same version of OnBase.

1. Lock your OnBase database and ensure that there are no users in the system.
For instructions on locking your OnBase database, see the System Administration documentation.
2. Stop all OnBase instances, processes, and services.
3. Stop the OnBase database. This ensures that all users are logged out of the system and all instances, processes, and services are stopped.
4. Restart the OnBase database.
5. Log on to the Configuration module as the user and/or workstation configured during system lockout.
6. Select **Utils | Rotate Database Password and KEK (key encryption key)**.

Note: This option is unavailable if the OnBase database has not been locked.

- The **Rotate Database Password and KEK (key encryption key)** dialog box is displayed:

Rotate Database Password and KEK (key encryption key)

Executable Files

Add Remove

Core KEK Rotation Parameters

☐ Generate Core dll

Core KEK Rotation Utility Path (GrabIcon.NET.exe) Browse Version

Passwords

☐ Change HSI Password HSI

☐ Change Core Password HSI CORE

☐ Change Viewer Password VIEWER

Comments

☐ Rotate KEK

User Entered String Format Formatted KEK Generate KEK

Comments

Update Cancel

- Click **Add**. Navigate to the folder containing your OnBase Client executable. Select the executable and click **Open**. The OnBase Client executable is added to the **Executable Files** list.

In a default installation, this file is located at **C:\Program Files\Hyland\OnBase Client** for 32-bit operating systems or **C:\Program Files(x86)\Hyland\OnBase Client** for 64-bit operating systems.

9. Click **Add**. Navigate to the folder containing your OnBase Configuration executable. Select the executable and click **Open**. The OnBase Configuration executable is added to the **Executable Files** list.
In a default installation, this file is located at **C:\Program Files\Hyland\OnBase Client** for 32-bit operating systems or **C:\Program Files(x86)\Hyland\OnBase Client** for 64-bit operating systems.
10. If you are using a legacy OnBase Core (released prior to OnBase 8.0), you will also need to add the **dmcore.dll** to the Executable Files list.
 - a. Click **Add**.
 - b. Navigate to the folder containing the OnBase Core files. In a default installation, this file is located at **c:\Program Files\Hyland\Core** for 32-bit operating systems or **C:\Program Files(x86)\Hyland\Core** for 64-bit operating systems.
 - c. Select the **dmcore.dll** file.
 - d. Click **Open**. The **dmcore.dll** is added to the **Executable Files** list.
11. If your OnBase version is older than OnBase 11.0 and includes the OnBase Core, you will also need to add the **OBCorePlatMgmt.dll** to the **Executable Files** list.
 - a. Click **Add**.
 - b. Navigate to the folder containing the OnBase Core files. In a default installation, this is located at **C:\Program Files\Hyland\Core** for 32-bit operating systems or **C:\Program Files(x86)\Hyland\Core** for 64-bit operating systems.
 - c. Select the **OBCorePlatMgmt.dll** file.
 - d. Click **Open**. **OBCorePlatMgmt.dll** is added to the **Executable Files** list.
12. If your solution includes an OnBase Application Server, select the **Generate Core dll** check box and complete the Core KEK Rotation Parameters:

Note: By selecting this option and performing the steps below, you are choosing to create a new version of **Hyland.Core.Grablcon.dll**. If you would like to back up the original version, place it another directory, or rename it to something else before completing the process.

- a. Enter the path to the **Grablcon.NET.exe** file in the **Core KEK Rotation Utility Path (Grablcon.NET.exe)** field, or select a path using the **Browse** button.

Note: This file is not included with your OnBase installation. Contact your first line of support to obtain the **Grablcon.NET.exe** executable.

- b. Enter the version of your OnBase Application Server in the **Version** field.
13. To change the **HSI**, **HSICORE**, and **HSINET** database passwords, select the respective **Change Password** check box. Type a new password in the corresponding text field.

14. To change the viewer account password, select the **Change Viewer Password** check box. The viewer account is a database account that allows only SQL SELECT statements to be executed. It is used by areas of OnBase that allow SQL statements to be run against the database. Type a new password in the **VIEWER** field to change the viewer account password.

Note: You do not need to change these database passwords in order to rotate the KEK. If you do need to change these database passwords, you should do so here if you are licensed for the Platter Management module.

Caution: If you change any of these database passwords, you are required to provide these passwords before you can upgrade your OnBase solution. Retain these passwords in a secure location.

15. Determine the type of KEK you want to use:
 - To use a random KEK, click **Generate KEK**.
 - To use a KEK based on your own string of text, type the string in the **User Entered String** field (i.e., **this is my new kek**), then click **Format**.

Note: The text in the **User Entered String** field must be exactly 16 characters. The User Entered String field can support letters, numbers, and symbols that are in a standard ANSI character set. Unicode is not supported for the User Entered String.

- To use a previous KEK, enter the previous KEK in the **Formatted KEK** field.

Note: The text in the **Formatted KEK** field must be greater than or equal to 24 characters.

16. If you chose to generate a KEK based on your own string of text or by clicking **Generate KEK**, a base64 string of text is displayed in the **Formatted KEK** field. This string represents the encrypted version of the text used to generate the KEK.

Note: You should retain the text displayed in the **Formatted KEK** field in a secure location. If you created a KEK based on your own string of text, retaining the string you typed in the **User Entered String** field is also sufficient. You can reuse the KEK when upgrading your OnBase solution.

17. To save any notes or comments about the KEK rotation, such as information on which files were modified and what environment the executables were set for, enter them in the **Comments** field. The text entered in this field is saved to a **readme** text file in the directory containing the new executables and DLL file.
18. Click **Update**.
19. OnBase rotates the KEK. Click **OK** at the prompt when the rotation is completed.
20. Click **No** if you are prompted to reset the cache of the Application Server.

The OnBase Configuration module is closed automatically when you click **OK** after the rotation is completed. This is done to prevent the old executables being used to rotate the KEK again, which may corrupt encrypted documents. You must use the new executable to re-open the Configuration module. See, [Deploying the Rotated Key Encryption Key on page 96](#).

Deploying the Rotated Key Encryption Key

Once you have rotated the Key Encryption Key (KEK), you must deploy the new OnBase Client and Configuration executables, as well as the **Hyland.Core.GrabIcon.dll** if you are using the OnBase Application Server. Depending on whether you are using a legacy version of the OnBase Core, you may also need to deploy the **dmcore.dll**.

Deploying the KEK involves locating the new executables and DLLs created by rotating the KEK and copying them over to where the old files reside, thereby deleting the old executables and DLLs and replacing them with the new ones. The new files must then be copied to all the workstations that require use of these files.

The new executables and DLLs are stored in a folder named **NewKEKExecutables#**, where # is the number of times that you have rotated the KEK for the selected set of executables. For example, if this is the first time you have rotated the KEK for this set of executables, the folder is named **NewKEKExecutables1**. If this is the fourth time you have rotated the KEK for this set of executables, the folder is named **NewKEKExecutables4**. The **NewKEKExecutables#** folders are located in the same folder as the current executables (e.g., **C:\Program Files\Hyland\OnBase Client**).

If you delete the **NewKEKExecutables#** folder, OnBase increments the **NewKEKExecutables#** folder number based on any folders that exist the next time you rotate the KEK. For example, you rotate the KEK three times. You delete **NewKEKExecutables2** and **NewKEKExecutables3**. When you rotate the KEK the fourth time, the folder is named **NewKEKExecutables2**. If you delete all copies of the **NewKEKExecutables#** folder, such that no **NewKEKExecutables#** folders exist, the new folder is named **NewKEKExecutables1**.

Note: When you upgrade your OnBase executables, any existing **NewKEKExecutables#** folders are deleted.

To deploy the KEK:

1. Navigate to the file path(s) you specified in the **Executable Files** field as the locations of your OnBase Client and Configuration executables.
2. Deploy these new OnBase Client and Configuration executables by copying the executables from the **NewKEKExecutables#** folder and placing them in the folder where the current executables reside. This will overwrite the current executables.
3. If you selected the **Generate Core dll** check box, a new **Hyland.Core.GrabIcon.dll** is also available in the **NewKEKExecutables#** folder.

Copy the new **Hyland.Core.GrabIcon.dll** from this folder and paste it in the following locations, overwriting the old version of this file:

- **OnBase Core Services:** In a default installation, the Core files are located at **C:\Program Files\Hyland\Core** (32-bit operating systems) or **C:\Program Files(x86)\Hyland\Core** (64-bit operating systems).
- **OnBase Application Server:** In a default installation, this file is located at **C:\inetpub\wwwroot\AppServer\bin**.

- **OnBase Web Server:** In a default installation, this file is located at **C:\Inetpub\wwwroot\AppNet\bin**.

Tip: To ensure that you replace all old versions of **Hyland.Core.GrabIcon.dll**, perform a Windows search for **Hyland.Core.GrabIcon.dll**.

4. If you are using a legacy OnBase Core (released prior to OnBase 8.0), you also need to copy the new **dmcore.dll** from the **NewKEKExecutables#** folder and paste it in the folder containing the legacy OnBase Core files, overwriting the old version of the file. In a default installation the Core is installed to **C:\Program Files\Hyland\Core** for 32-bit operating systems or **C:\Program Files(x86)\Hyland\Core** 64-bit operating systems.
5. If your OnBase version is older than OnBase 11.0 and includes the OnBase Core, you will also need to copy the new **OBCorePlatMgmt.dll** from the **NewKEKExecutables#** folder and paste it in the folder containing the OnBase Core files, overwriting the old version of the file. In a default installation the Core is installed to **C:\Program Files\Hyland\Core** for 32-bit operating systems or **C:\Program Files(x86)\Hyland\Core** 64-bit operating systems.
6. Unlock your OnBase database.
7. Perform an IIS reset on the OnBase Application Server.

Upgrading After Rotating the Key Encryption Key

Caution: Do not upgrade the database until you have completed the steps below. Later in this process, you need to access the database using the old Configuration executable. If you upgrade the database, you can no longer log into the database using the old Configuration executable.

Upgrading OnBase is not part of the Key Encryption Key (KEK) rotation process. However, when you rotate the KEK used by OnBase, you are required to take additional steps when it is time to upgrade your OnBase solution. This is because the KEK piece stored in your upgraded version of the OnBase executables and DLLs does not match the piece stored in your OnBase database. Your upgraded OnBase solution will not function until you change the KEK piece stored in the upgraded OnBase executables and DLLs to match the piece stored in your OnBase database.

To rotate the KEK in the upgraded executables and DLLs:

1. Create a new folder and copy the old version of the OnBase Configuration executable into the folder. For example, your new folder may have a file path such as **C:\Program Files\Hyland\ConfigOld**.

Note: You only need to perform this step on the workstation that will be used to rotate the KEK. After the KEK is rotated, the new files can be copied to other user workstations, as long as those workstations are using the same version of OnBase.

2. Install the new version of OnBase on all of the workstations, including the workstation that will be used to rotate the KEK in the upgraded executables.

Caution: Do not upgrade the database until you have completed the steps below. Later in this process, you need to access the database using the old Configuration executable. If you upgrade the database, you can no longer log into the database using the old Configuration executable.

3. Log on to the Configuration module using the old OnBase Configuration executable.
4. Perform the steps in [Rotating the Key Encryption Key on page 92](#), ensuring that you:
 - Rotate the upgraded OnBase Client and Configuration executables, as well as the upgraded **Hyland.Core.GrabIcon.dll**, **dmcore.dll**, and **OBCorePlatMgmt.dll**, if necessary.
 - Change the **HSI**, **HSICORE**, and **HSINET** database passwords if you previously changed them (see step 13 under [Key Encryption Key Rotation](#)).
 - You use the same KEK that you previously used in step 16, generate a new KEK, or enter a new KEK.
5. Perform the steps in [Deploying the Rotated Key Encryption Key on page 96](#), making sure you replace the executables and DLLs on your workstation with the new executables and DLLs. You can then deploy the KEK to any number of workstations, as long as those workstations have upgraded to the same version of OnBase.

Unencrypting an Encrypted Disk Group

Data stored on Encrypted Disk Groups can be unencrypted using **Disk Group Migration**. Using this method, a new Disk Group without encryption is created, and the encrypted files are moved to this Disk Group, unencrypting them in the process.

To unencrypt an Encrypted Disk Group:

1. Create a new unencrypted Disk Group in OnBase Configuration. For more information, see [Creating and Editing Disk Groups on page 12](#).
2. Create a new Disk Group Migration job in the OnBase Client. For more information, see [Configuring a Disk Group Migration Job on page 100](#)
 - a. Set the source Disk Group constraint to be the Encrypted Disk Group.
 - b. Set the Destination Disk Group to the new unencrypted Disk Group.
3. Create a Disk Group Migration Processing task in the Unity Scheduler if one has not already been created. For more information on creating this task, see [Creating a Task on page 110](#).

Once the Disk Group Migration Processing task is executed as scheduled, the files in the Encrypted Disk Group are migrated to the new unencrypted Disk Group, effectively unencrypting these files.

Migrating an Existing Encrypted Disk Group to a Different Encryption Algorithm

A previously encrypted Disk Group can be migrated to a different encryption algorithm using **Disk Group Migration**. Using this method, a new Disk Group with the different encryption algorithm is created, and the encrypted files are moved to this Disk Group, changing their encryption algorithm.

To unencrypt an Encrypted Disk Group:

1. Create a new Disk Group with the different algorithm in OnBase Configuration. For more information, see [Creating and Editing Disk Groups on page 12](#).
2. Create a new Disk Group Migration job in the OnBase Client. For more information, see [Configuring a Disk Group Migration Job on page 100](#)
 - a. Set the source Disk Group constraint to be the Encrypted Disk Group.
 - b. Set the Destination Disk Group to the new Disk Group.
3. Create a Disk Group Migration Processing task in the Unity Scheduler if one has not already been created. For more information on creating this task, see [Creating a Task on page 110](#).

Once the Disk Group Migration Processing task is executed as scheduled, the files in the Encrypted Disk Group are migrated to the new Disk Group, effectively encrypting these files with the new algorithm.

Overview

Disk Group Migration is a process in OnBase that allows for the transfer of files from one Disk Group to another. Disk Group Migration can be used to perform several different tasks, including:

- Migrating files from an unencrypted Disk Group to an Encrypted Disk Group, which will encrypt those files. This can also be accomplished using Encryption Migration. However, Disk Group Migration is recommended as a much simpler process for achieving the same task. For more information on Encryption Migration, see [Encryption Migration on page 74](#).
- Migrating files from an Encrypted Disk Group to an unencrypted Disk Group, which will unencrypt the files. Disk Group Migration is the only method for performing this task.
- Separating Cold and TIFF documents into separate files for individual pages to remove specific pages from those documents.
- Migrating files between Disk Groups.

If using Disk Group Migration with Encrypted Disk Groups, see [Encrypted Disk Groups on page 86](#) for more information and requirements. Disk Group Migration is not available for any disk group using the Federated File Framework.

Note: If FIPS mode is enabled, Disk Group Migration cannot be used to migrate files to any disk group that is not FIPS compliant.

Disk Group Migration is performed using the OnBase Client to configure migration jobs that are then executed when a Disk Group Migration Processing task is scheduled in the Unity Scheduler. For more information, see:

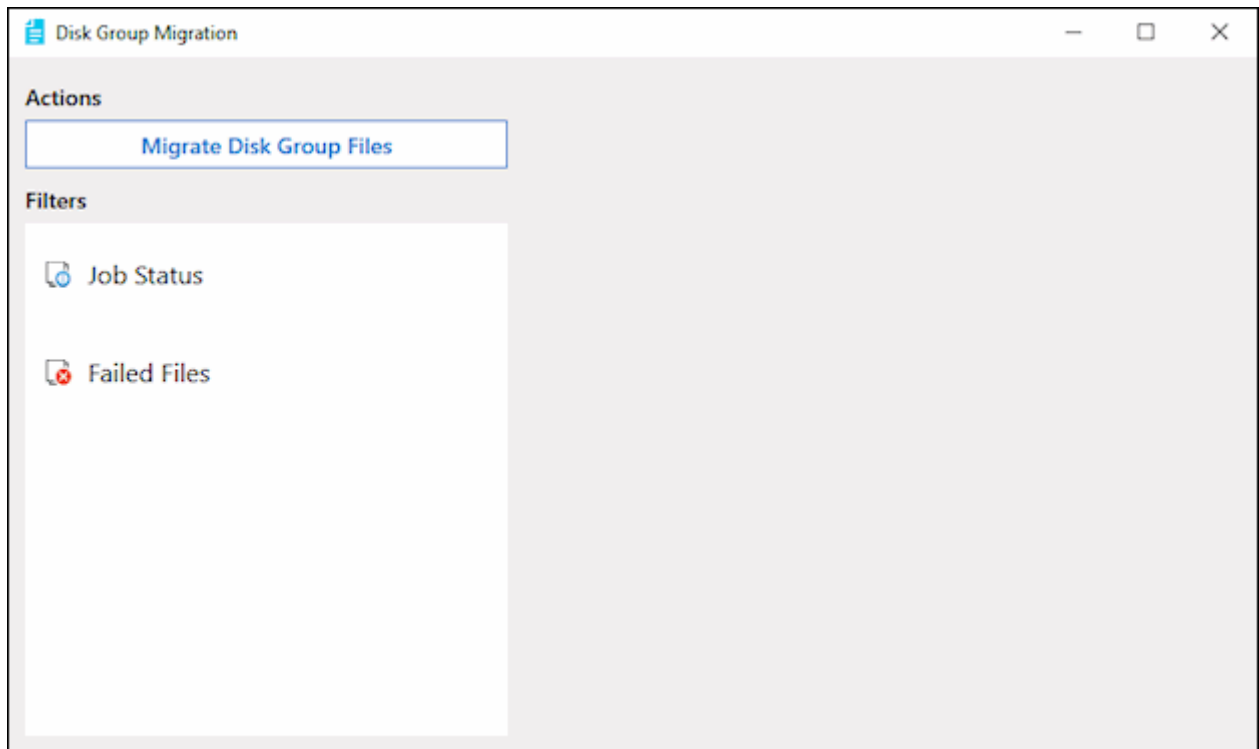
- [Configuring a Disk Group Migration Job on page 100](#)
- [Creating a Disk Group Migration Processing Task on page 104](#)
- [Using the Disk Group Migration Window on page 105](#)

Configuring a Disk Group Migration Job

Disk Group Migration Jobs are configured in the OnBase Client before they can be executed using the Unity Scheduler. Prior to creating a Disk Group Migration job, you must create the Disk Group you plan to migrate files to. When migrating files to encrypt or decrypt them, ensure that the new Disk Group is properly configured as the required type. For information on configuring an unencrypted Disk Group, see [Creating and Editing Disk Groups on page 12](#). For more information on configuring an Encrypted Disk Group, see [Configuring a New Disk Group as an Encrypted Disk Group on page 89](#).

To configure a new Disk Group Migration job in the OnBase Client:

1. Select **Admin | Disk Group Migration**. The **Disk Group Migration** window is displayed:



For more information on this window, see [Using the Disk Group Migration Window on page 105](#).

2. Select **Migrate Disk Group Files**. The **Migrate Disk Group Files** dialog box is displayed.

Migrate Disk Group Files

Migrate Disk Group files that satisfy the constraints below to another Disk Group

Constraints

Disk Group is any Disk Group

Add Constraint

And Document Type is any Document Type

Add Constraint

And Document Date is any date

Add Constraint

Destination Disk Group

<Select One>

File Migration Settings

☐ Divide multipage TIFFs into individual files

☐ Divide COLD documents into individual files

Process Settings

☐ Process Abort Threshold

☐ File Abort Threshold

Queue Migration Job

3. Select the constraints for the Disk Group Migration job in the Constraints section of the dialog box. To add a constraint
 - c. Click the **Add Constraint** button in the section of the constraint you want to add. A drop down list is displayed in that section.
 - d. Select the constraint from the drop-down list.

Multiple constraints can be selected for each type of constraint. The available constraints include:

Constraint	Description
Disk Group	<p>The source Disk Group of the files being migrated.</p> <hr/> <p>Note: At least one Disk Group constraint must be selected.</p> <hr/>
Document Type	The Document Types to be included in the migration. If no Document Types are selected, all documents in the selected Disk Group are migrated.
Document Date	An inclusive date range for documents to be included in the migration. Two drop-down lists appear, From and To . By default, the Document Date range is set in both drop-down lists to the current date.

4. Select the **Destination Disk Group** from the drop- down list.
5. Select the optional **File Migration Settings**. Enabling these settings can improve performance for a Disk Group Migration. These settings include:

File Migration Setting	Description
Divide multipage TIFFs into individual files	Multipage TIFF files stored in the original Disk Group are divided into multiple single-page files during the Disk Group Migration.
Divide COLD documents into individual files	Documents imported using the COLD process are divided into multiple individual files during the Disk Group Migration.

Note: This setting can be used to divide files that contain multiple pages or multiple documents into individual files. This allows for individual pages or documents to be deleted or modified as needed.

6. Select the optional **Process Settings**. These settings determine when the Disk Group Migration process as a whole and the migration of an individual file will be aborted during the Disk Group Migration job. When enabling these options, you must enter a number for each option in the field next to the option. These options include:

Process Setting	Description
Process Abort Threshold	If the number of files specified in the field fail to migrate consecutively during the Disk Group Migration, the entire job is stopped until the issue is addressed. After the issue has been addressed, the Disk Group Migration job can be executed again.
File Abort Threshold	If a single file fails to migrate successfully the number of times specified in the field, the file is not migrated and the Disk Group Migration job continues without that file.

7. Click **Queue Migration Job** to finish creating the Disk Group Migration job.

Once created, the Disk Group Migration job is added to the **Job Status** queue in the **Disk Group Migration** window.

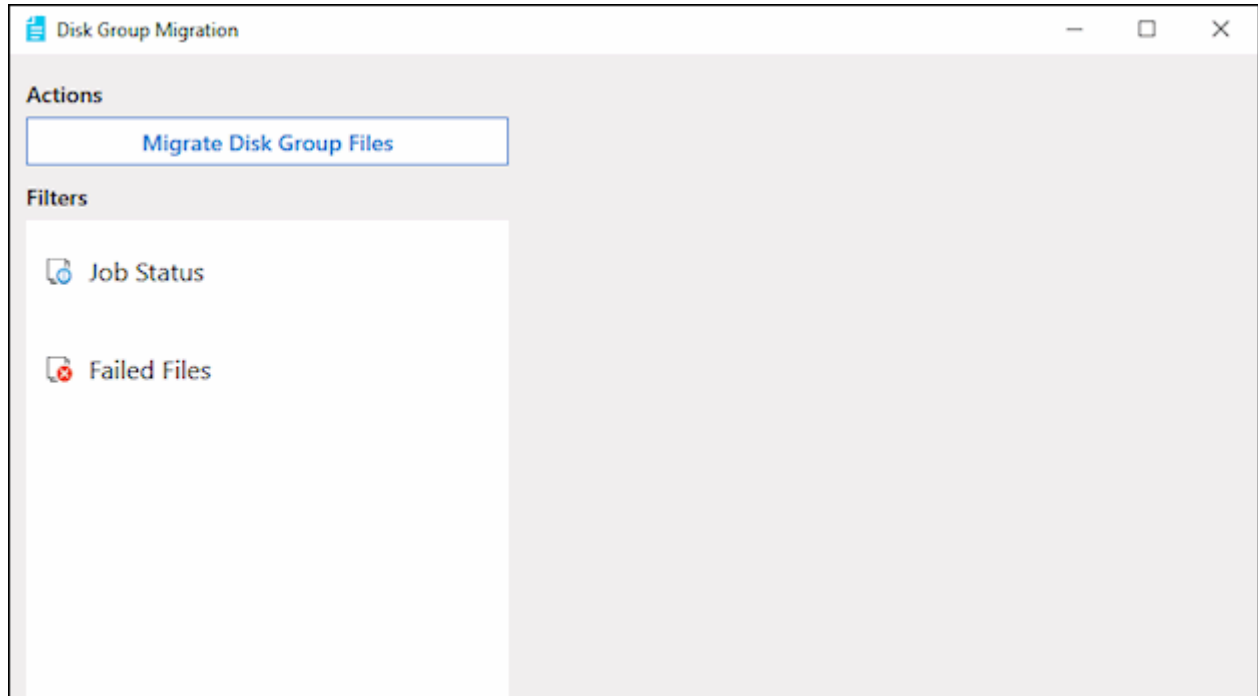
Creating a Disk Group Migration Processing Task

Disk Group Migration jobs are only executed when a Disk Group Migration Processing task is run as scheduled in the Unity Scheduler. For more information on configuring a Disk Group Migration job, see [Configuring a Disk Group Migration Job on page 100](#). The Disk Group Migration Processing Task must be manually configured in the Unity Scheduler. Whenever the task is executed, any waiting Disk Group Migration jobs in the Disk Group Migration Job Status queue are executed. For information on manually creating a Unity Scheduler task, see [Creating a Task on page 110](#).

Caution: During the execution of a Disk Group Migration Processing task, documents that are being migrated are locked and cannot be accessed.

Using the Disk Group Migration Window

Disk Group Migration jobs can be monitored using the Disk Group Migration window in the OnBase Client. To access this window, select **Admin | Disk Group Migration** in the OnBase client. The **Disk Group Migration** window is displayed:



The Disk Group Migration window is divided into two tabs that allow for the monitoring of individual jobs and failed files. For more information on these tabs, see:

- [Job Status Tab on page 105](#)
- [Failed Files Tab on page 107](#)

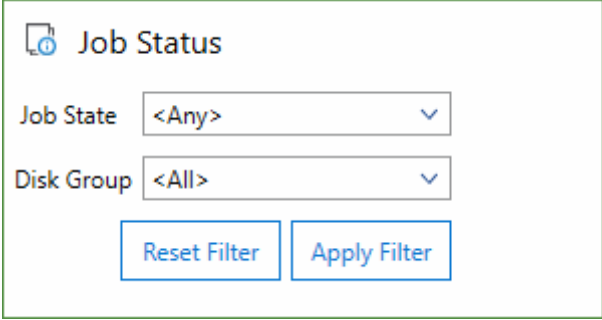
Job Status Tab

The **Job Status** tab of the **Disk Group Migration** window displays all of the currently created Disk Group Migration jobs currently configured. Within this tab, jobs are shown as queued, in progress, paused, or failed. The statuses that can be shown for a job include:

Status	Description
Active	The job will be run when the next Disk Group Migration Processing task is executed in the Unity Scheduler.
Finished	The job has been completed with no file failures.

Status	Description
Finished with Failures	The job was finished, but there were file failures during the migration. The Failed Files tab in the Disk Group Migration window shows which files failed and why. For more information on this tab, see Failed Files Tab on page 107 .
Paused	The job has been paused using the Pause button. The job will not be run until it has been resumed using the Resume button. For more information, see Changing the Job Status on page 107 .
Initializing	The job is currently being processed after a Disk Group Migration Processing task has been executed in the Unity Scheduler.
Deleted	The job has been deleted using the Delete button. For more information, see Changing the Job Status on page 107 .

By default, the Job Status tab shows all Disk Group Migration jobs currently configured. You can filter which jobs are shown by using the Job Status filters.



To filter the Disk Group Migration jobs displayed:

1. Select a **Job State** from the drop-down list for the jobs you want displayed. Select **<Any>** to see jobs with any state at all.
2. Select a **Disk Group** from the drop-down list for the jobs you want displayed. Select **<All>** to display jobs from all available Disk Groups.
3. Click **Apply Filter**. All jobs meeting the selected requirements are displayed in the **Job Status** tab.

To remove all filters, select **Reset Filters**. This returns the filters to **<Any>** and **<All>** and displays every configured Disk Group Migration job.

Changing the Job Status

Once a job is selected, several buttons may appear for the job. These buttons can be used to change the status of the job, and include:

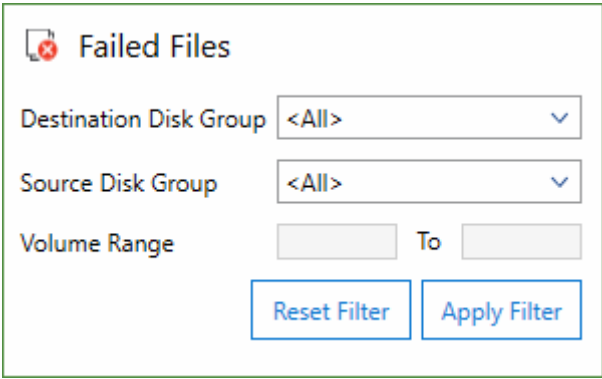
Button	Description
Pause	Pauses the selected job and prevents it from running when the next Disk Group Migration Processing task is run in the Unity Scheduler.
Resume	Resumes a paused job, meaning that it will be run when the next Disk Group Migration Processing task is run in the Unity Scheduler.
Delete	Deletes the job permanently. Can be used on jobs with any status except In Progress.
Requeue	Queues a finished with failures job for processing again. Once a job has finished with failures, the files that failed cannot be reprocessed without re-queuing the job. Only requeue a job once you have addressed the issue causing the failure, as found in the Failed Files Tab. For more information on this tab, see Failed Files Tab on page 107 .

The buttons available depend on the status of the job. For example, only paused jobs have the **Resume** button available.

Failed Files Tab

The **Failed Files** tab of the **Disk Group Migration** window displays information for files that have failed during an attempted Disk Group Migration job. These jobs are listed in the **Job Status** tab as **Finished with Failures** as the Job Status. For more information on the **Job Status** tab, see [Job Status Tab on page 105](#).

By default, the Failed Files tab shows all files that have failed to properly migrate. You can filter which files are shown by using the Failed Files filters.



The screenshot shows a dialog box titled "Failed Files" with a red 'x' icon. It contains three filter fields: "Destination Disk Group" and "Source Disk Group", both set to "<All>" with dropdown arrows. Below these is a "Volume Range" field with two input boxes separated by "To". At the bottom are two buttons: "Reset Filter" and "Apply Filter".

To filter the failed files displayed:

1. Select a **Destination Disk Group** from the drop-down list. The Destination Disk Group is the location the file was attempting to migrate to when the migration failed. Select **<All>** to see files migrating to any Disk Group.
2. Select a **Source Disk Group** from the drop-down list. The Source Disk Group is the original location of the file being migrated. Select **<All>** to display files from all available Disk Groups.
3. Enter a range of volumes you want to view failed files from on the selected Disk Groups.
4. Click **Apply Filter**. All failed files meeting the selected requirements are displayed in the **Failed Files** tab.

To remove all filters, select **Reset Filters**. This returns the filters to **<Any>** and **<All>** and displays every configured Disk Group Migration job.

Each file listed includes a reason for a failure, including failure to lock the file, the file not being found, or the file being part of an uncommitted batch. To resolve the failure of the migration job, address the identified issue and requeue the job in the Job Status tab of the Disk Group Migration window.

A list of failed files can be exported to a CSV file by right-clicking on the list of failed files and selecting **Export Filtered Records To CSV**. A dialog box opens, allowing you to name the file and select a location for the file to be stored in. Click **Save** to store the CSV file.

PLATTER MANAGEMENT UNITY SCHEDULER TASKS

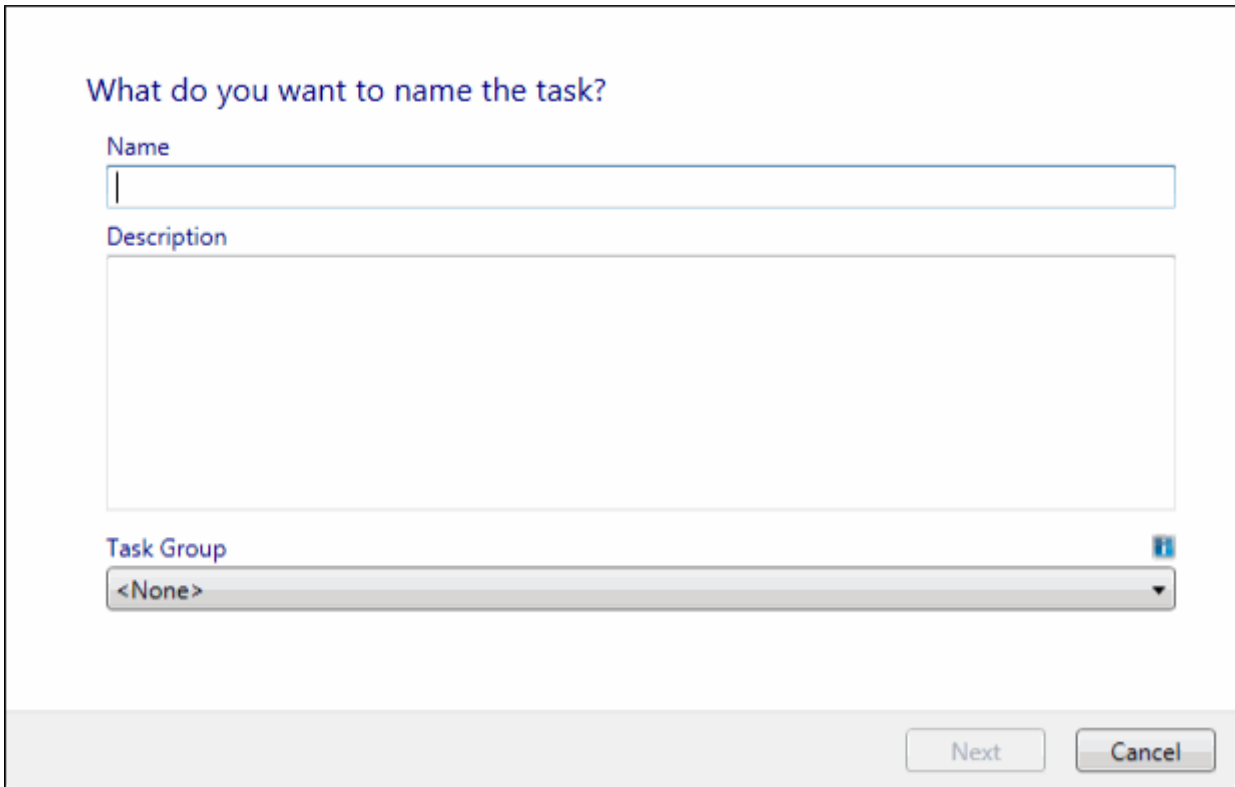
Several Platter Management tasks can be executed in the Platter Management in the Unity Management Console. Certain tasks are configured automatically as System Tasks that are executed automatically every 24 hours. For more information on these tasks, see [System Tasks on page 115](#). For any other task to be executed, you need to create the appropriate task within Unity Scheduler and determine when the task is executed. For more information, see [Creating a Task on page 110](#).

Note: Users must have the proper platter management privileges to configure these tasks, in addition to access the Unity Scheduler. If you are unable to configure these tasks, contact your administrator to ensure the proper privileges have been granted.

Creating a Task

To create a task:

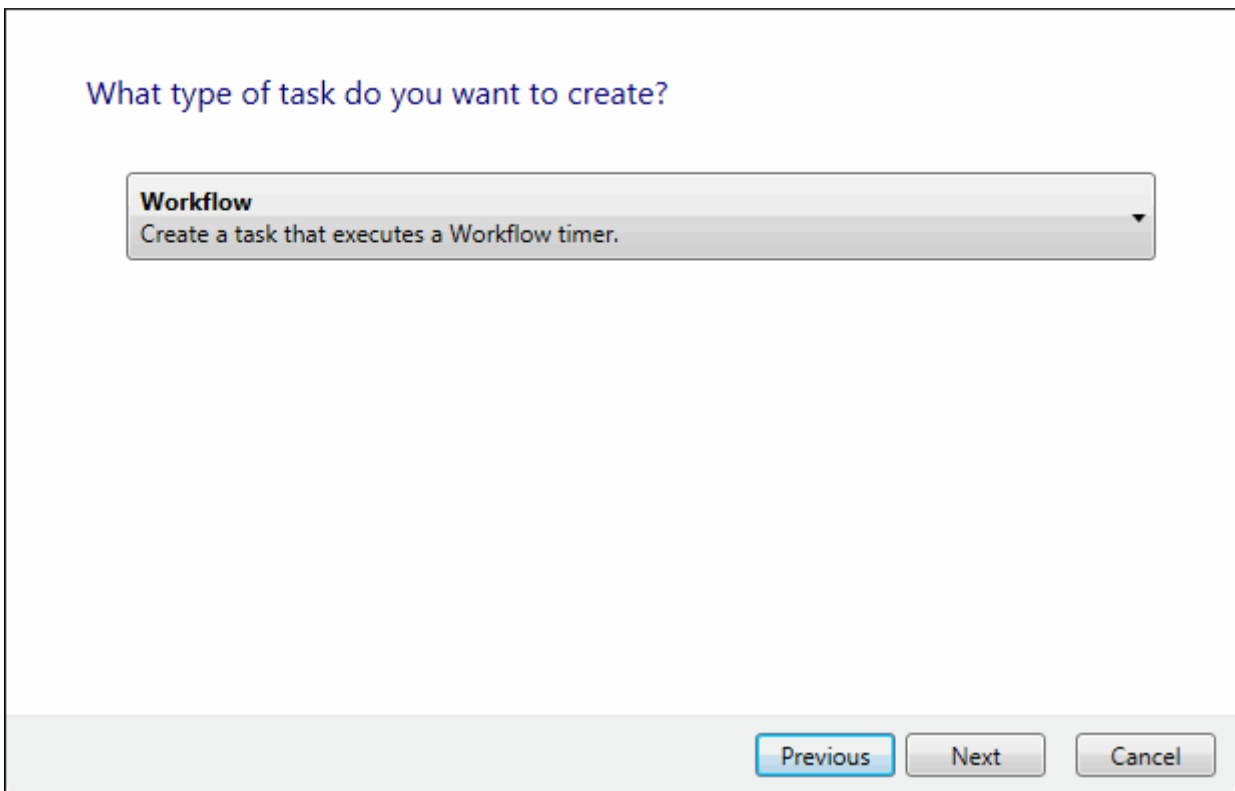
1. In the **Console** tree, select the task scheduler for which you want to add a task.
2. Right-click and select **Create Task**, or select **Create Task** in the **Action** pane.
The **Task Wizard** is displayed.



The screenshot shows a 'Task Wizard' dialog box with the title 'What do you want to name the task?'. It contains three main input areas: a 'Name' field with a single character 'I' entered, a 'Description' field which is empty, and a 'Task Group' drop-down menu currently set to '<None>'. To the right of the drop-down is a small icon of two overlapping squares. At the bottom right, there are 'Next' and 'Cancel' buttons.

3. Enter a unique name for the task in the **Name** field.
4. Enter a description for the task in the **Description** field.
5. Select a task group from the **Task Group** drop-down list. Existing task groups are available for selection. If **<None>** is selected, the task is added to the **<Unassigned>** task group.

6. Click **Next**. The **Task Type Selection** page is displayed.



What type of task do you want to create?

Workflow
Create a task that executes a Workflow timer.

Previous Next Cancel

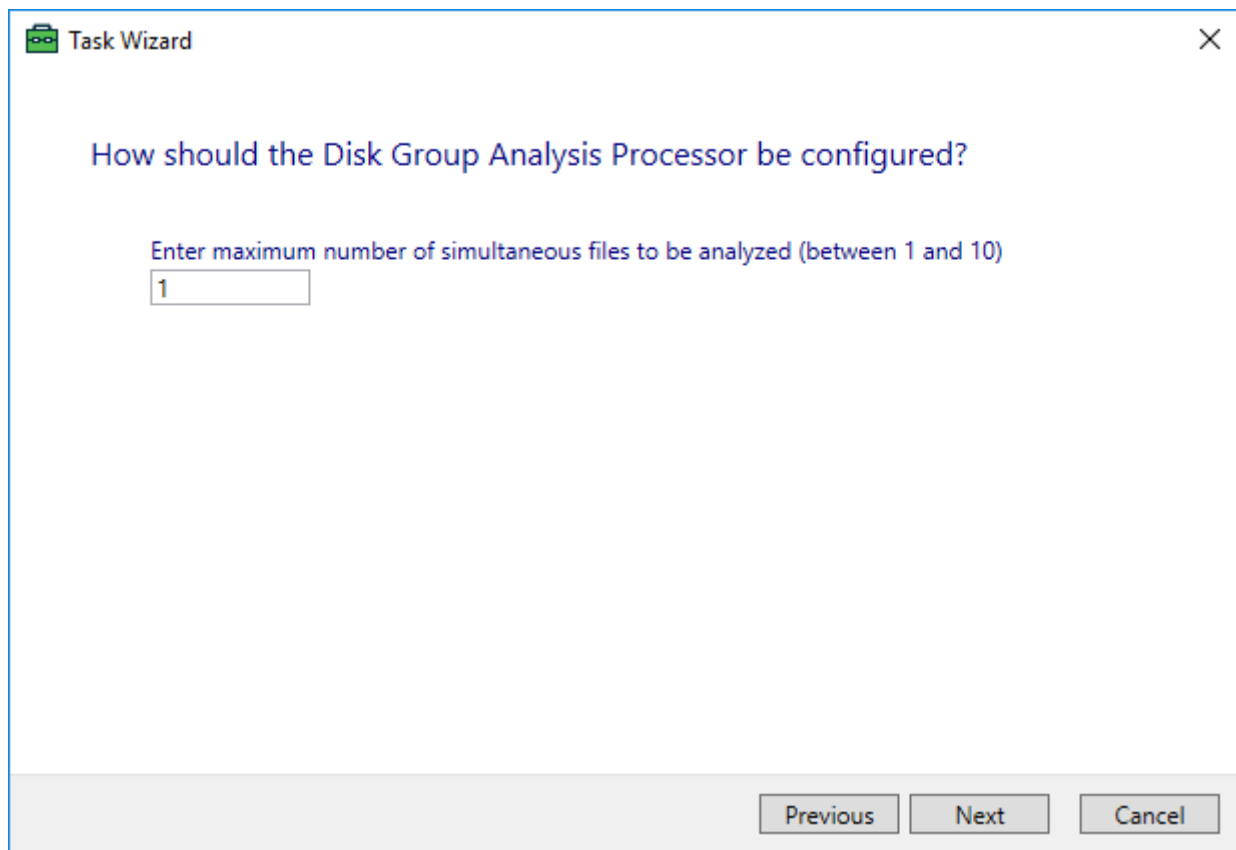
7. Select a Platter Management task to perform the appropriate processing. For more information specific Platter Management tasks within the Platter Management, see:
 - [Disk Group Analysis Processing on page 111](#)
 - [Platter Deletion Processing on page 112](#)
 - [S3 Upload Cache Processing on page 114](#)
 - [Disk Group Analysis Processing for S3 Disk Groups on page 114](#)
 - [Disk Group Migration Processing on page 114](#)

Disk Group Analysis Processing

The **Disk Group Analysis Processing** task performs all of the analysis jobs configured. For more information on analysis jobs, see [Analyze on page 123](#).

To configure a task to perform disk group analysis:

1. Select **Disk Group Analysis Processing** from the drop-down list when prompted to select the type of task you want to create.
2. Click **Next**. The **Disk Group Analysis Processor** page is displayed.



The screenshot shows a window titled "Task Wizard" with a close button (X) in the top right corner. The main text asks, "How should the Disk Group Analysis Processor be configured?". Below this, a prompt reads, "Enter maximum number of simultaneous files to be analyzed (between 1 and 10)". A text input field contains the number "1". At the bottom right, there are three buttons: "Previous", "Next", and "Cancel".

3. Select the maximum number of simultaneous files to be analyzed.

Note: The recommended maximum number of simultaneous files to be analyzed is 2. Higher settings are available, but users will need to monitor their systems to ensure the higher setting does not negatively impact performance.

4. Click **Next**. The User Group selection page of the **Task Wizard** is displayed.

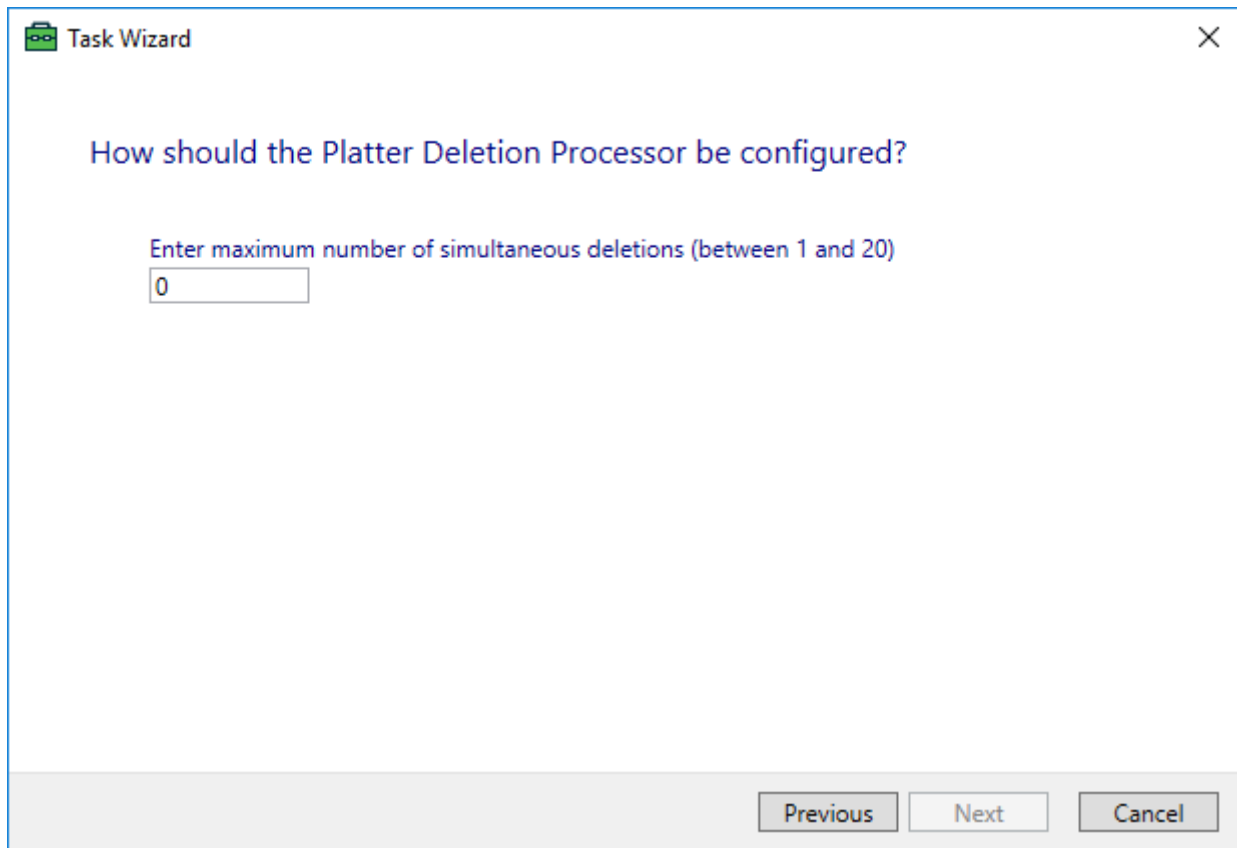
To finish configuring the task, see the **Unity Scheduler** module reference guide.

Platter Deletion Processing

The **Platter Deletion Processing** task executes any platter deletion jobs that have been approved in Platter Management Administration. For more information on platter deletion jobs, see [Platter Deletion Jobs on page 143](#).

To configure a **Platter Deletion Processing** task:

1. Select **Platter Deletion Processing** from the drop-down list when prompted to select the type of task you want to create.
2. Click **Next**. The **Platter Deletion Processor** page is displayed.



The image shows a 'Task Wizard' dialog box with a title bar containing a green icon and the text 'Task Wizard'. The main content area has the heading 'How should the Platter Deletion Processor be configured?' in blue. Below this is a text prompt 'Enter maximum number of simultaneous deletions (between 1 and 20)' in blue. A text input field contains the number '0'. At the bottom right, there are three buttons: 'Previous', 'Next', and 'Cancel'.

3. Type the maximum number of simultaneous deletions into the field. The value entered into this field must be between 1 and 20.

Note: The recommended maximum number of simultaneous deletions is 2. Higher settings are available, but users will need to monitor their systems to ensure the higher setting does not negatively impact performance.

4. Click **Next**. The User Group selection page of the **Task Wizard** is displayed.

To finish configuring the task, see the **Unity Scheduler** module reference guide.

S3 Upload Cache Processing

The **S3 Upload Cache Processing** task moves the data in the S3 upload cache from the local location to the cloud storage on a configured S3 provider. For more information on the S3 upload cache, see [Configuring S3 Upload Cache Processing on page 62](#). A single **S3 Upload Cache Processing** task is automatically configured as a system task when the Unity Scheduler is launched. This task must have user groups and a schedule assigned to it before it will execute.

To configure an additional **S3 Upload Cache Processing** task:

1. Select **S3 Upload Cache Processing** from the drop-down list when prompted to select the type of task you want to create.
2. Click **Next**. The User Group selection page of the **Task Wizard** is displayed.

To finish configuring the task, see the **Unity Scheduler** module reference guide.

Disk Group Analysis Processing for S3 Disk Groups

The **Disk Group Analysis Processing for S3 Disk Groups** task performs any S3 disk analysis rules that have been created and queued for processing. For more information on creating analysis rules, see [S3 Disk Group Analysis Rules on page 79](#). For more information on queuing analysis jobs, see [Viewing Analysis Jobs on page 70](#).

To configure an additional **Disk Group Analysis Processing for S3 Disk Groups** task:

1. Select **Disk Group Analysis Processing for S3 Disk Groups** from the drop-down list when prompted to select the type of task you want to create.
2. Click **Next**. The User Group selection page of the **Task Wizard** is displayed.

To finish configuring the task, see the **Unity Scheduler** module reference guide.

Disk Group Migration Processing

The Disk Group Migration Processing task executes any Disk Group Migration jobs that have been previously configured in the OnBase Client. For more information, see [Configuring a Disk Group Migration Job on page 100](#).

To configure a Disk Group Migration Processing task:

1. Select **Disk Group Migration Processing** from the drop-down list when prompted to select the type of task you want to create.
2. Click **Next**. The User Group selection page of the **Task Wizard** is displayed.

To finish configuring the task, see the **Unity Scheduler** module reference guide.

System Tasks

Several Platter Management tasks in the Unity Scheduler are configured as System Tasks. These tasks are automatically executed every 24 hours. These tasks cannot be configured manually but can be viewed in the Systems Task list in the Unity Scheduler.

Incomplete Commit Queue Processing

The **Incomplete Commit Queue Processing** task commits any documents remaining in the Incomplete Commit Queue. If the automatic commit fails upon an ad hoc (single document) import, the document is added to the Incomplete Commit Queue.

Incomplete Delete Queue Processing

The **Incomplete Delete Queue Processing** task deletes any items in the Incomplete Delete Queue in Platter Management. If deletion cannot be completed on these items due to issues with permissions, connections, a lack of access, or another reason, these items remain in the Incomplete Delete Queue.



Platter Management

User Guide

Usage

Platter Management is the administration of the physical data files that contain your data through Disk Group management. Disk Groups are the logical groupings of the individual physical files. Most Platter Management operations are performed in the OnBase Client. Platters can be backed up, moved, deleted, and exported. This section covers the Platter Management options available in the OnBase Client and Configuration module:

- System ID File
- Viewing Document Locations
- Managing Disk Groups and Queues
- Computing Volume Size
- Analyze Source (Platter)
- Promoting a Volume
- Copying Volumes and Platters
- Moving Platters
- Using the Storage Migration Queue
- Backing Up Platters
- Copying a Backup Platter (Reset on Backup Queue)
- Deleting Platters
- Exporting Platters

System ID File

When a mass storage copy, a backup copy, or a removable copy is created for a Disk Group, an ID file (OnBase.ID) is also created, unless the copy is created on an EMC Centera or IBM Tivoli system. This ID file is placed in the same physical location designated in the Disk Group for the data files.

The relationship between Disk Groups and data files is referenced in the database and tracked by the OnBase.ID file. All data that is brought into the document management system must be referenced to a Disk Group and its associated ID file.

Whereas the database tracks the physical location of the Disk Group, the system ID file tracks the detailed status of the volumes and platters within the Disk Group, and how data files are mapped within the volume/platter structure. It is this unique volume/platter structure that allows OnBase to perform specialized data management functions.

The ID file contains lines of information that map the Disk Group number, volume number, copy number, and install ID:

- The **Disk Group Number** is the value used by OnBase to reference the Disk Group internally in the database. This number can also be found in Configuration under the **Disk Mgmt | Disk Groups** menu.
- The **Volume Number** corresponds to a Disk Group volume. An entry is added to the ID file for each new volume of a Disk Group.
- The **Copy Number** indicates the copy of the Disk Group where the ID file resides.
- The **Install ID** is a unique value assigned to the OnBase system when the system is installed.

The format of the ID file that contains these fields is as follows: **Disk Group #-Volume #-Copy #:Install ID**. For example, 103-2-2:HSI is the ID for Disk Group 103, volume 2, copy 2 for the system with the install ID of HSI.

This text file flags locations for the system's use. When a document is requested for retrieval, the system first gets the Disk Group and volume number for the document from the database. It then verifies the existence of the ID file for that Disk Group. Based on the ID file, it uses the relative path stored in the database to locate and retrieve the file.

Missing System ID Files

If the system ID file cannot be located for the first copy of the Disk Group, the next copy is searched, and so on, until an ID file is located. If one cannot be found, the user is prompted for the location of a valid ID file. This location should point to an ID file for the Disk Group volume's copy. The system will not display any data that cannot be logically connected between the data file, database reference, Disk Group, and ID file.

If the ID file is missing or corrupt, it can be recreated using any text editor. In the event that data files are physically moved on the network, the ID file must be moved along with them, and the new location must be edited in the **Volume Information** for the Disk Group.

Tip: Missing ID files are also reported under the **Error Viewer** tab of the Diagnostics Console for Core-based platter management. See the Diagnostics Service module reference guide for details on using the Diagnostics Console.

Mass Storage System ID Files

Mass Storage copies maintain multiple entries in the system ID file, one for each volume stored there. As volumes are deleted, the word **DELETED** is added at the beginning of the volume copy line. For example:

DELETED 101-1-1:TRAINME

101-2-1:TRAINME

101-3-1:TRAINME

Because removable and backup copies only maintain one volume per location, the ID file at these locations only contains a single line.

Because of this retrieval logic, all structure beneath the ID file is identical. When a copy is created during Disk Group setup, only the ID file is created. However, as soon as a file is stored at the Disk Group location, the sub-directory structure is created.

Each new volume creates a **V#** directory. For example, when volume 1 (**V1**) is closed and a new file is placed in volume 2, a **V2** structure is created. Below the **V#** directories, subdirectories are created that contain 500 files. The 501st file causes a new subdirectory to be created for the next 500 files, and so on.

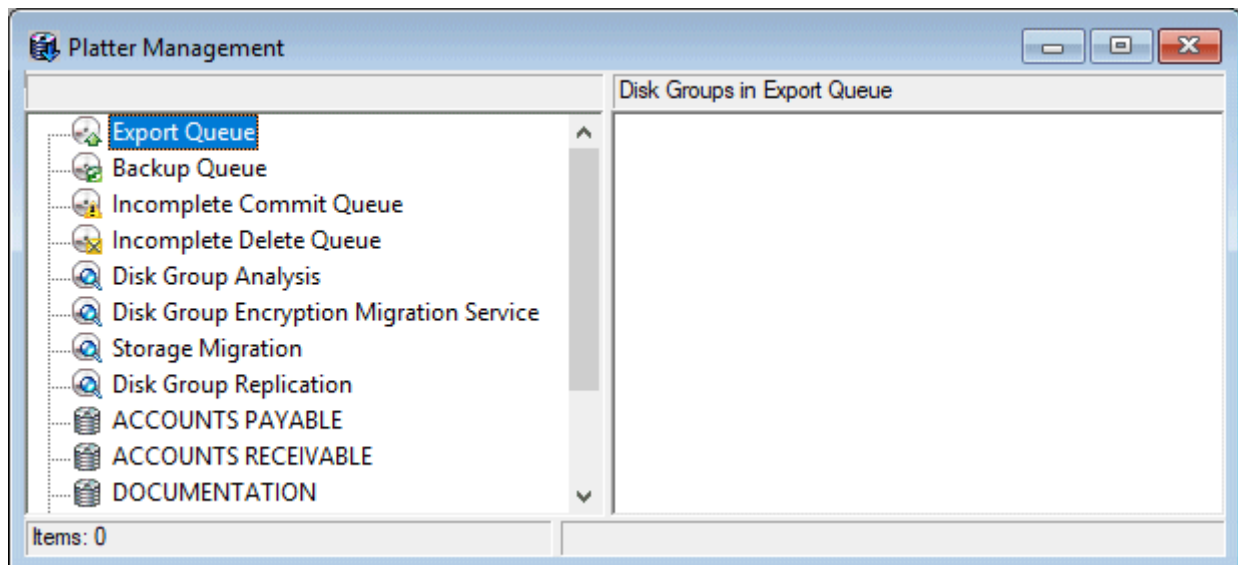
Note: Subdirectories will increment from 0 to 9999, and after filling the 9999th, will rollover back to 0 in order to keep the file path length to a manageable size. In some cases this may cause the newest files in a volume to be placed in the same subdirectory as the oldest files in a volume.

This **V#** directory structure is the same, regardless of the copy type (except **Export**). Because of this, a copy can be relocated anywhere, so long as the system knows where to find the ID file.

The OnBase Client caches the parsed OnBase.ID file to improve performance impacted by parsing the file continuously. The Client checks to see if the OnBase.ID file has been modified since it was last parsed. Modification of the file is determined by whether or not the file size or the modified date of the file has changed. If either have changed, the file is parsed.

Managing Disk Groups and Queues

Platter management functions are used to maintain redundant copies of data within a Disk Group and manage the migration of that data to long-term storage devices. The **Platter Management** window displays all currently configured Disk Groups and the queues into which a Disk Group volume can be transitioned.



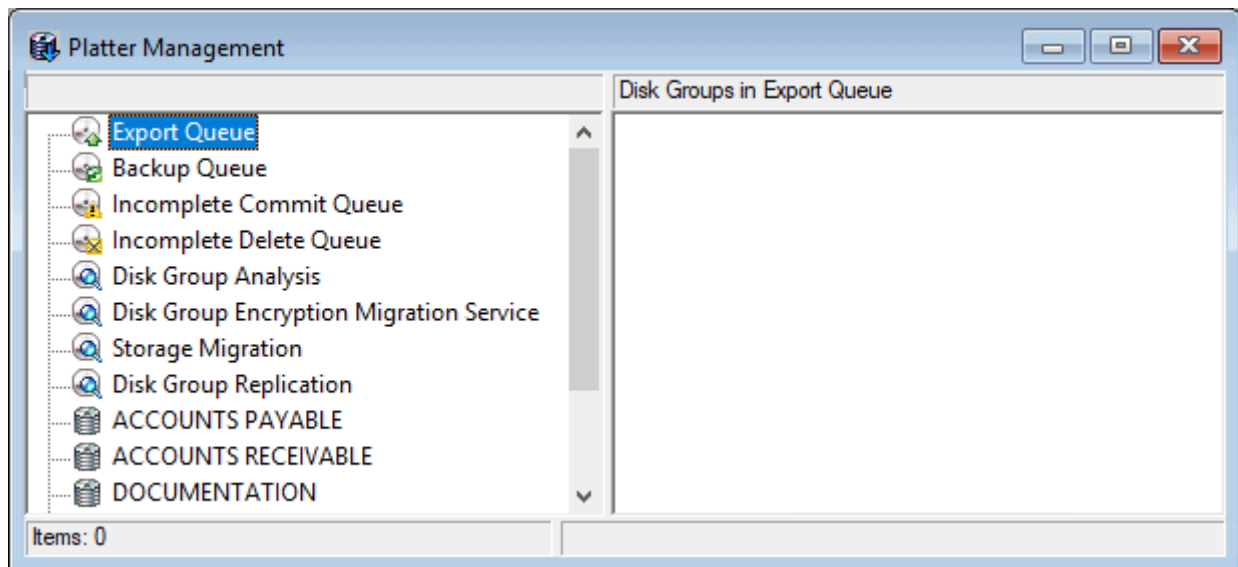
The **Platter Management** window contains several queues, including:

Queue	Description
Export Queue	<p>The queue contains any Disk Group volume that was designated as an export copy when the Disk Group was created. The data files from this volume can then be moved in their entirety, along with the appropriate database indices, to another database, according to the export format selected.</p> <hr/> <p>Note: An Export license is required to export platters.</p> <hr/>
Backup Queue	<p>Any Disk Group awaiting backup appears in this queue. A Disk Group must have been created with a backup platter in order for the Disk Group to appear in the Backup Queue. In addition, a volume will appear when a volume is closed either by reaching its maximum disk size or being promoted.</p>
Incomplete Commit Queue	<p>If the automatic commit fails upon an ad hoc (single document) import, the Disk Group containing that document is added to the Incomplete Commit Queue. Disk Groups can then be committed from this queue. The queue consists of three columns listing the Disk Group where the platter is located, the ID of the platter, and the number of files on the platter which are not committed.</p> <hr/> <p>Note: In some configurations involving non-revisable Document Types, an entry for an item will appear in the queue even though the file no longer exists. To remove the entry from the queue, right-click on the document and then click Commit.</p> <hr/>
Incomplete Delete Queue	<p>If a scrub, delete, or purge action fails, the document, batch, or platter is added to the Incomplete Delete Queue. The scrub, delete, or purge action can be retried or canceled from this queue. The queue consists of three columns list the Disk Group where the platter is located, the ID of the platter, and the number of files on the platter which are to be deleted.</p>
Disk Group Analysis	<p>The Disk Group Analysis queue contains platter analysis jobs scheduled for later execution.</p> <hr/> <p>Note: Depending on system licensing, additional queues may be shown in the Platter Management window. Refer to the documentation for these additional products and licenses for specific information on queues not listed here.</p> <hr/>

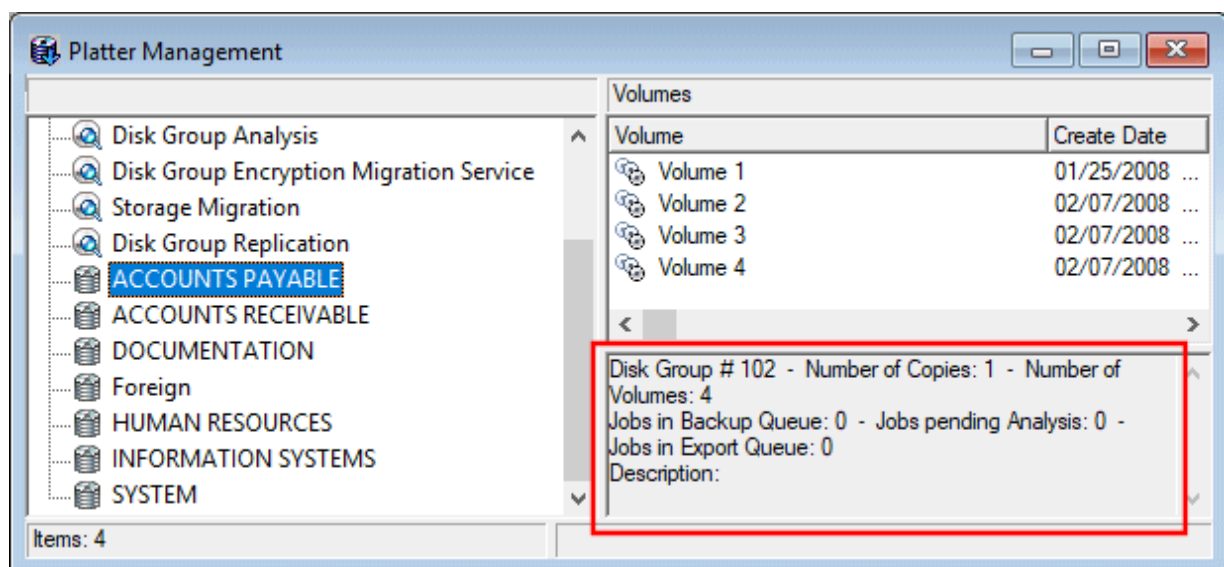
Platter Management Functions

Using a logical interface where the data actually resides on the network (Disk Groups) and tracking of the data within a Disk Group, OnBase is able to locate/relocate, categorize, and perform specialized platter management functions on the data without losing data integrity.

To access platter management functions, select **Admin | Platter Management** in the Client module to access the **Platter Management** window.



Whenever a Disk Group is selected within the Platter Management window, the **Disk Group Information Pane** is displayed at the bottom of the **Volumes** column:



This pane contains information about the Disk Group including its identification number, number of copies, number of volumes, description, and any jobs it may have in queues.

The type of platter management functions that can be initiated at the right-click menu depend on whether the volume is accessed within a Disk Group volume or platter, or within a queue.

Note: Platter management functions for S3 Disk Groups are limited to only **Compute Volume Size**. All other options are unavailable. For more information on performing similar functions on S3 Disk Groups, see [S3 Disk Groups on page 52](#).

Copy

Available from the Disk Group volume or platter. Allows the user to manually copy any platter to any selected media accessible to the system. Only platters that are closed can be copied. This function is not available for platters that are not created or have been deleted.

Write

Available from the Backup Queue. Allows the user to manually backup a platter in the **Backup Queue** to any selected media accessible to the system.

If your system is licensed for CD or DVD Authoring, **Write to CD-R** is available; if your system is licensed for Centera, **Write to Centera** is available; if your system is licensed for Tivoli, **Write to Tivoli** is available.

Compute Volume Size

Available from the Disk Group volume or Backup Queue. Calculates the current space occupied by data in the volume (in KB).

Analyze or Analyze Source

Available from the Disk Group platter, Backup Queue, or Export Queue. Produces statistics for the platter that indicate errors or missing files and any data that has been moved. This function is not available for platters that are not created or have been deleted.

Verify Access

Verify access to a platter copy to ensure the proper permissions are present on the platter for the current user.

Promote

Available from the Disk Group volume. Sets a system flag for the selected volume, indicating that it cannot be processed into.

Export

Available from the Disk Group platter and Export Queue. Copies the data files and database indices for those files into a preconfigured folder structure designated by an export format configuration. Requires **Export** licensing. This function is not available for platters that are not created or have been deleted.

Export to DIP

Available from the Disk Group volume. Produces a tagged DIP text file of each document stored in the selected volume. During export you can select whether you want all volumes exported or just the selected volumes. If you are generating for more than one volume, you can generate one file for each volume or a single file for all of the volumes.

Note: Documents stored in encrypted Disk Groups cannot be accessed outside of OnBase and cannot be imported to other OnBase systems.

Reset on Backup Queue

Available from the Disk Group volume or platter. Generates another backup platter and places it in the **Backup Queue**.

Note: **Reset on Backup Queue** is only available for volumes configured with a backup copy.

Add to Export Queue

Available from the Disk Group volume. This option is only available for Disk Groups that are configured with an Export copy.

Move

Available from the Delete Queue. Relocates the Disk Group to another storage area, anywhere on the network that is accessible to the workstation. Only platters that are closed can be moved (use Force Promote with the **Change Platter Path** option selected to move open platters). This function is not available for platters that are not created or have been deleted.

Manual Delete

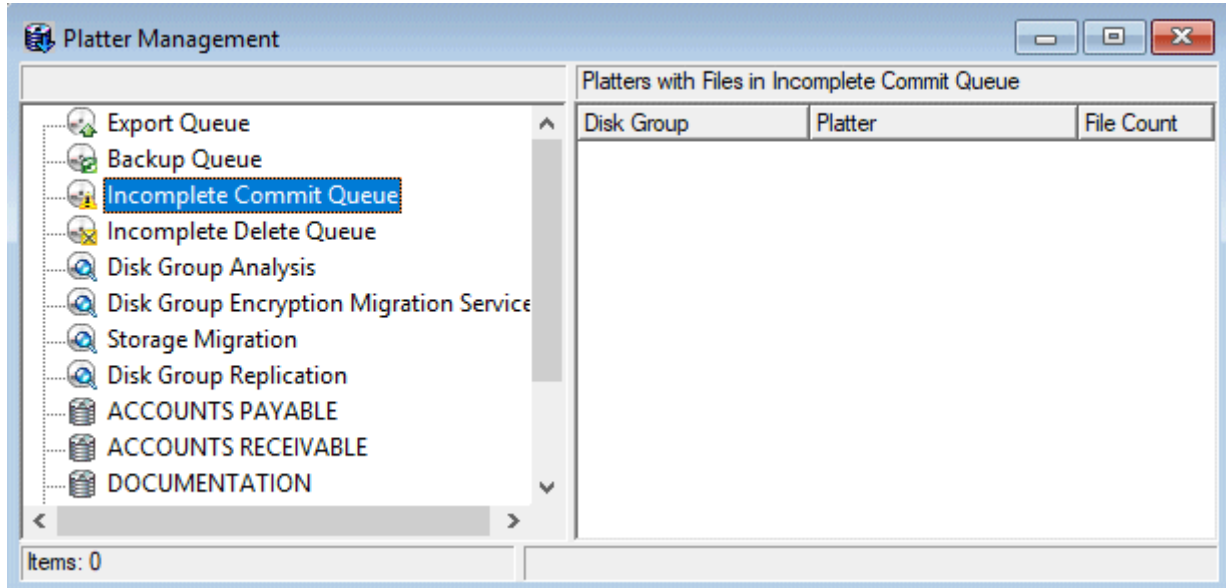
Available from the Disk Group platter. Removes the selected platter and its associated data files from the Disk Group volume. This function is not available for platters that are not created or have been deleted.

Process

Run or retry the process associated with the queue. For example, selecting **Process** from the right-click menu in the **Incomplete Delete Queue** retries the failed scrub, purge, or delete action on the selected items.

Incomplete Commit Queue Functions

The following functions are only available from the **Incomplete Commit Queue**. To select Platter Management functions, right-click on a platter in the right pane of the **Platter Management** window. To access document functions, double-click a platter in the right pane then right-click on the document.



Commit

From the platter, commits all documents in the selected platter. From the document, commits the selected document.

Open Document

Open the selected document for viewing.

Note: In order to view any documents in the **Incomplete Commit Queue**, a user must have rights to view those documents.

Properties

Display the Document Properties of the selected document.

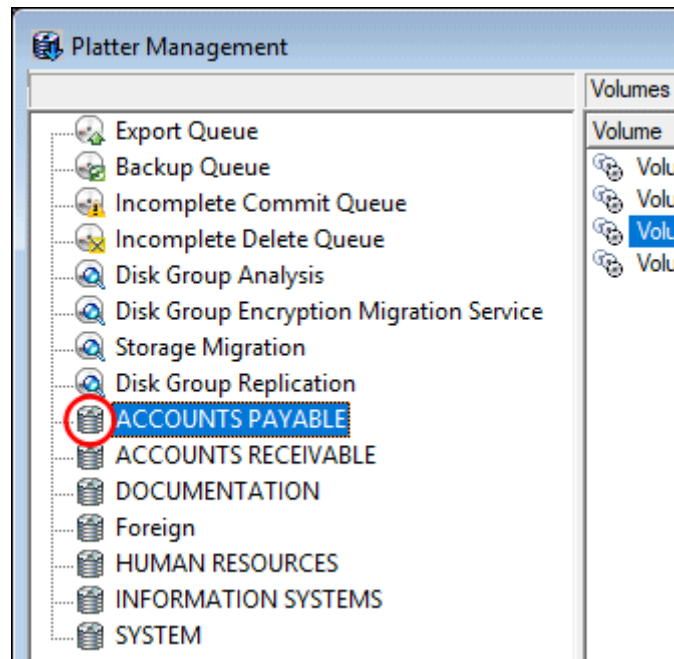
Computing Volume Size and Splitting Volumes

The space occupied by data on any volume in any Disk Group can be obtained by running **Compute Volume Size** for the selected volume. If a volume is larger than its configured size, it can be split to reduce its size.

Computing Volume Size

To compute the volume size:

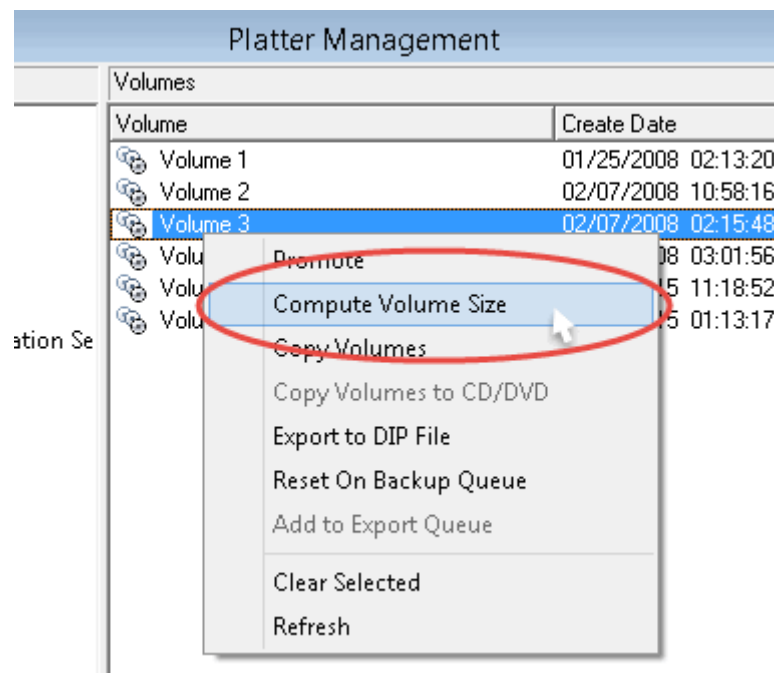
1. Select a Disk Group in the left pane of the **Platter Management** window. Disk Groups are denoted by the Disk Group icon.



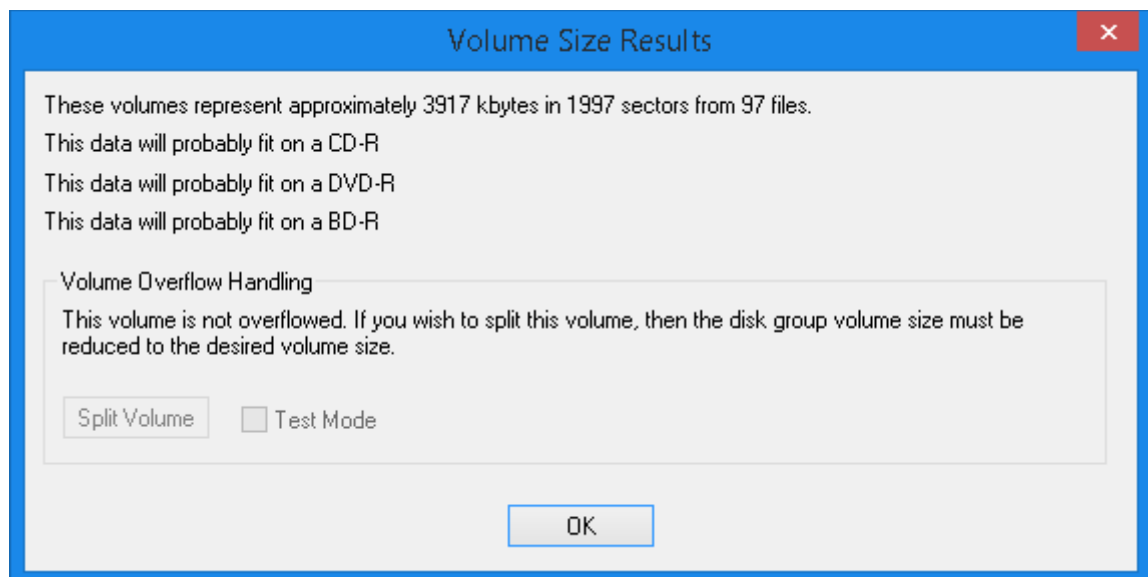
The volumes associated with the selected Disk Group are displayed in the right pane.

2. Select a volume in the right pane and right-click it.

3. Select **Compute Volume Size** from the right-click menu.



The results are displayed in the **Volume Size Results** dialog box:



Splitting a Volume

Some import processes can hold a volume open, resulting in volume sizes too large to be written to the configured back up media. Volumes that have grown to a size larger than the configured maximum size can be split, migrating some of the files out of the overfilled volume and into a new volume. The migration performed when a volume is split only changes the logical location of the files; the physical location of the files remains unchanged.

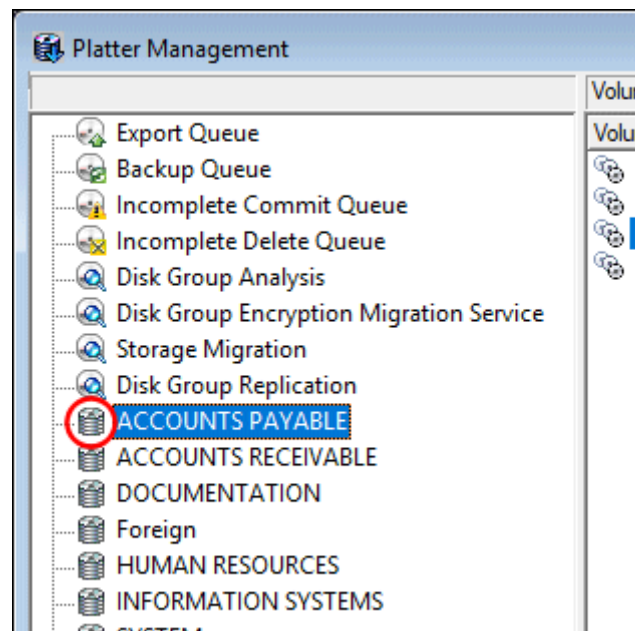
In order to split a volume, you must first compute the volume size. Volume splitting is further limited by the following parameters:

- Volumes in Foreign, Imported, or Encrypted Disk Groups cannot be split.
- Only volumes that have been closed can be split. For example, you cannot split the currently active volume.
- Only one volume at a time can be split.
- Volumes that contain a copy that utilizes Storage Integration for Tivoli cannot be split.

To split a volume:

Note: It is a best practice to only split volumes when there is little or no activity in the Disk Group that contains the volume being split, such as during off-peak hours. The Disk Group that contains the volume being split is locked during the split process.

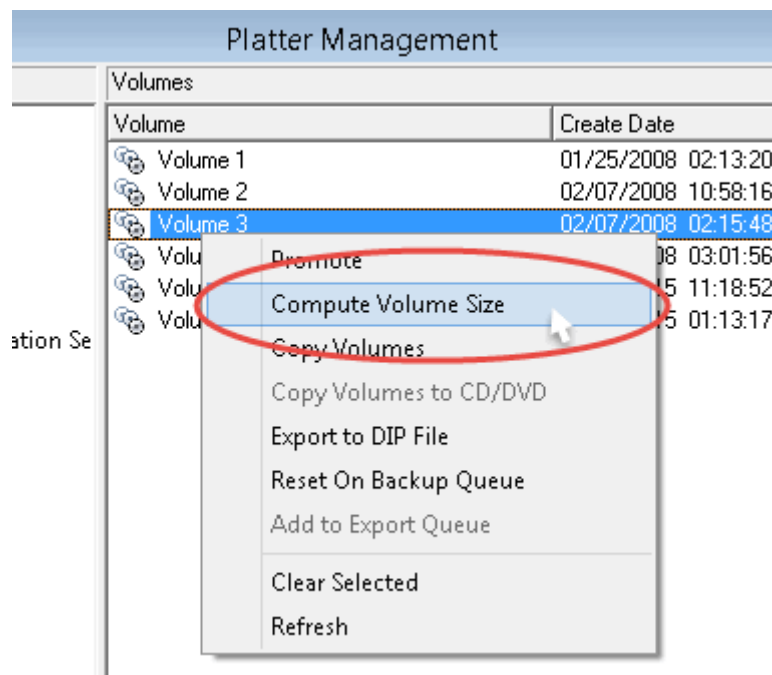
1. Select the Disk Group in the left pane. Disk Groups are denoted in the left pane of the **Platter Management** window by the Disk Group icon.



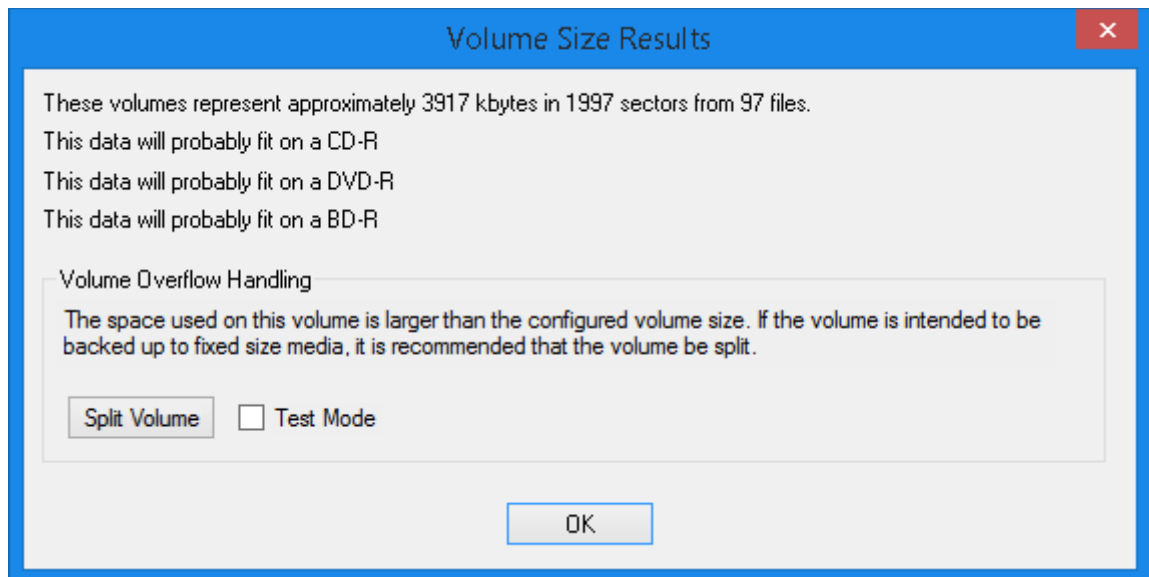
The volumes associated with the selected Disk Group are displayed in the right pane.

2. Select a volume in the right pane and right click it.

3. Select **Compute Volume Size** from the right-click menu.



The results are displayed in the **Volume Size Results** dialog box:



4. To test the split process first, select **Test Mode** in the **Volume Size Results** dialog box. No files are migrated to a new volume in test mode.

5. Click the **Split Volume** button in the **Volume Size Results** dialog box.

Note: This button is not available if the volume is not overfilled.

6. Confirm the split process at the prompt.

After the split process is completed, a verification report is displayed. This report is also archived under the **SYS - Platter Management Reports** Document Type.

If **Test Mode** is selected, a verification report of the activities that would have occurred is generated, but no files are migrated to a new volume.

Analyze

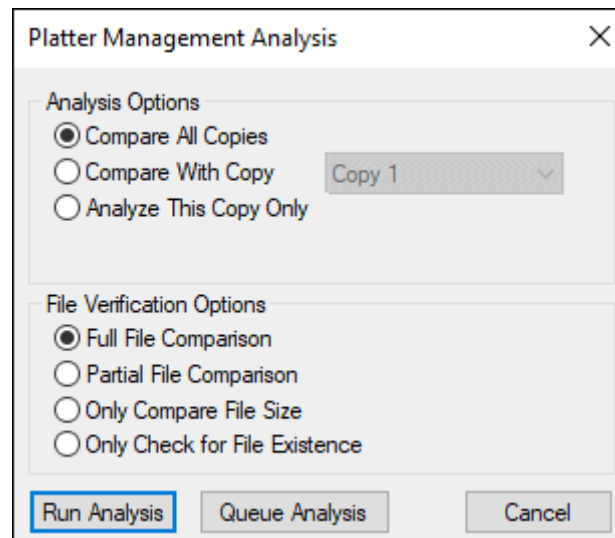
The **Analyze** and **Analyze Source** right-click menu options check the selected platter for errors, such as missing files. The analysis also determines the number of files in the platter, as well as the disk space occupied by the files.

1. In the **Platter Management** dialog box in the OnBase Client, select a platter copy or one or more volumes from the **Backup Queue**.
2. Select **Analyze** or **Analyze Source** from the right-click menu.

Note: **Analyze Source** is only available when selecting platters in the **Backup Queue**. This function analyzes the source of the backup, not the backed up files themselves. Otherwise, it is functionally the same as **Analyze**.

Note: This function is not available for platters that are not created or have been deleted.

3. At the **Platter Management Analysis** dialog box, select **Analysis Options**, **File Verification Options**, and **Analysis Flags** if available:



Analysis Option	Description
Compare All Copies	Compares the selected copy of a volume to all available copies of that volume.
Compare With Copy	Compares one copy of a volume with another copy of the same volume. Use the drop-down list to select the other copy within the current volume.
Analyze This Copy Only	Analyzes only the selected copy without comparing it to any other copies of the volume.

File Verification Options	Description
Full File Comparison	Performs a byte-by-byte check of every file created in the platter and compare these files to the original files.
Partial File Comparison	Performs a partial file comparison of all files in the volume using the following rules: <ul style="list-style-type: none"> • If a file is smaller than 5 MB, the full files are compared. • If the file is larger than 5 MB, the first megabyte, the last megabyte, and a random megabyte in the middle are compared between copies. If any difference is found between two copies, a full file analysis is performed.
Only Compare File Size	Compares the sizes of files between copies.

File Verification Options	Description
Only Check for File Existence	Checks only for the existence of files on all copies being analyzed. Note: If you are analyzing a platter that only has one available copy for analysis, Only Check for File Existence is the only type of file verification that can be performed, as all other types require multiple copies to analyze.

Analysis Flags	Description
Validate KOMpliance file retention	Ensures that files on a KOM server are properly retained. This option is available only if the platter is on a KOM server.

- When all the appropriate options are selected, click one of the following:
 - Run Analysis** to analyze the items immediately.
 - Queue Analysis** to add this analysis as a job to the **Analysis Jobs** queue to be executed using a task in the Unity Scheduler. Once **Queue Analysis** is selected, you are returned to the **Platter Management** window. For more information on how to execute queued analysis jobs, see [Disk Group Analysis Tasks on page 179](#).
- If you clicked **Run Analysis**, the **Verify Platter** dialog box is displayed. The platter analysis can be canceled at any time by clicking **Cancel**. A confirmation message is displayed when the analysis is complete. If the analysis is unable to be completed, a message is displayed with the reason the analysis failed. If the analysis failed due to files that could not be repaired during analysis, you can view a report that shows which files could not be repaired. For information on viewing reports, see [Viewing Analysis Reports on page 132](#).

Repairing Files During Analysis

During analysis, platters that are analyzed will be automatically repaired based on the copy they are compared to. Three types of issues in a platter will be addressed during analysis by auto-repair, as shown below:

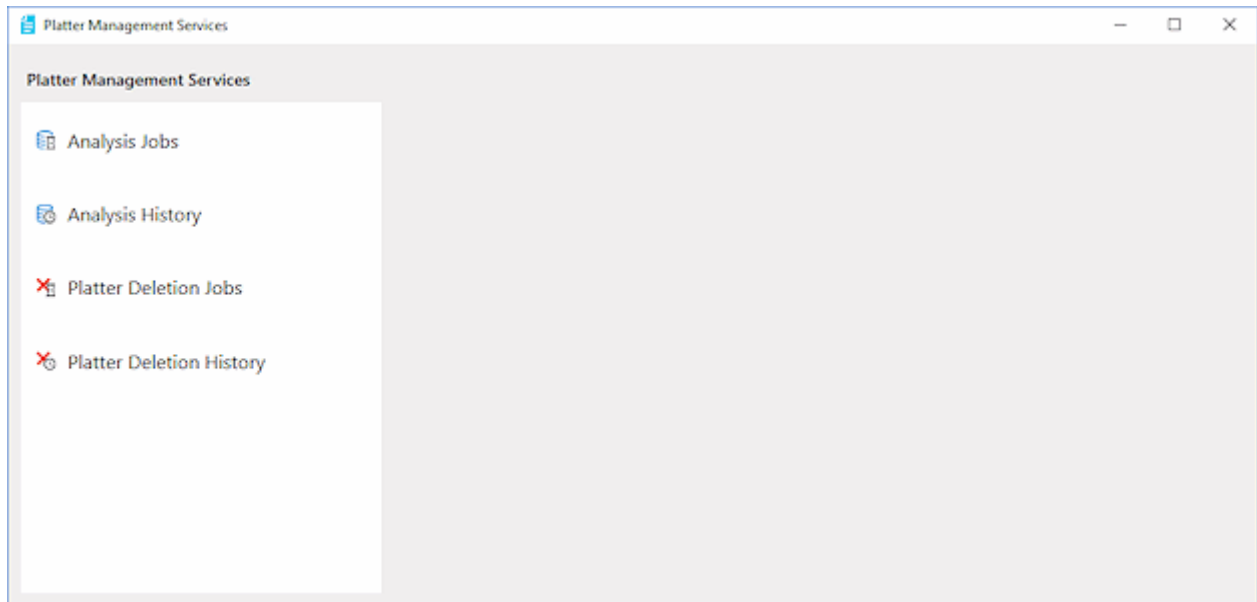
Issue	Description	Auto-Repair Action
Missing file	A file on the comparison platter is not on the analyzed platter.	The file is copied to the analyzed platter.
Zero byte file	A file on the analyzed platter is zero bytes in size.	The file is replaced with a full sized version from the comparison platter.
Partial file	A file on the analysis platter is smaller than the matching file on the comparison platter.	The file is not replaced, but is noted as partial in the analysis report.

Auto-repair is only available for mass storage platters, removable platters, and backup platters. Auto-repair is not performed on externally filled platters, import platters, foreign platters, or cloud replication destinations.

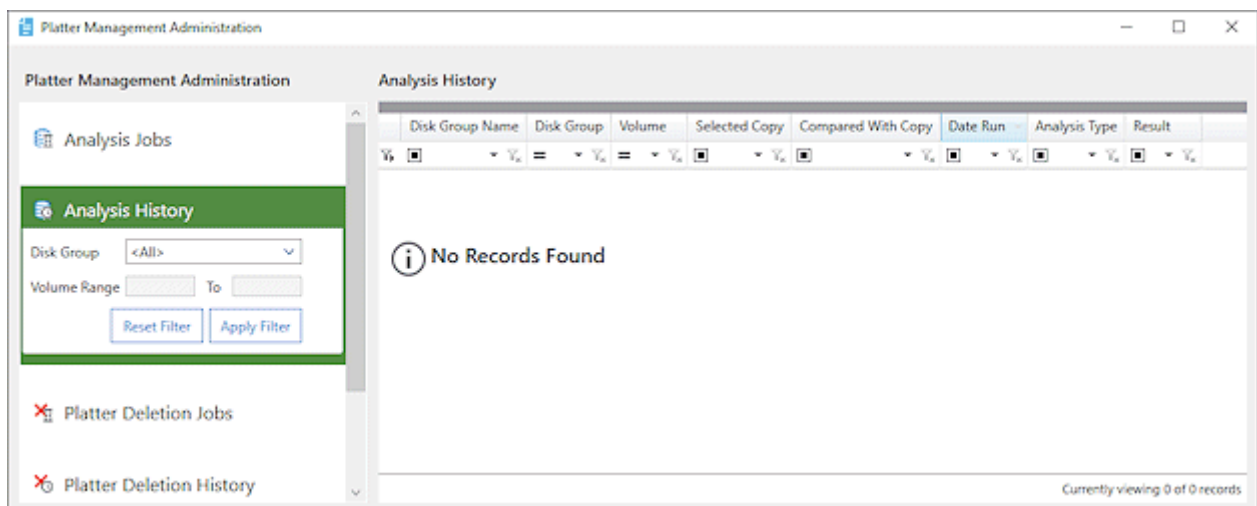
Viewing Analysis Reports

Reports can be generated for any completed analysis task in the OnBase Client. To view a report on the analysis:

1. Click **Admin | Platter Management Services** to open the **Platter Management Administration** window.

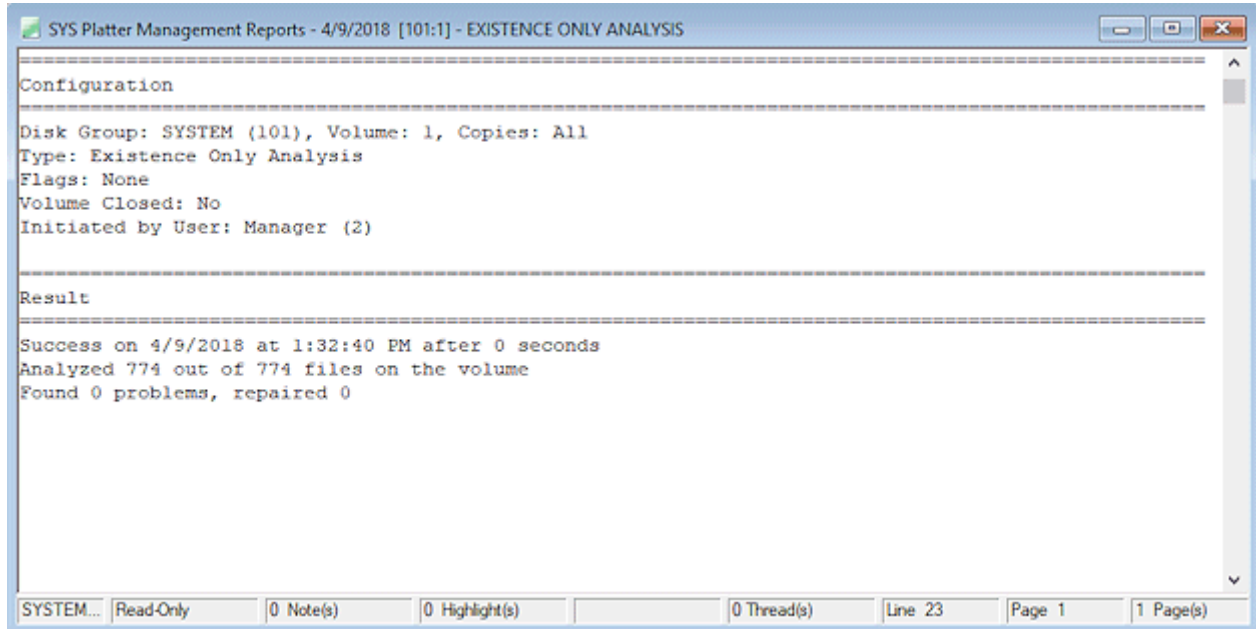


2. Click **Analysis History** to view a history of completed analysis jobs.



3. Select the Disk Group of the analysis history you want to view from the **Disk Group** drop-down select menu, or select **<All>** to view analysis jobs for all Disk Groups.

4. To view results from a range of volumes, enter the volume numbers in the **Volume Range** fields.
5. Click **Apply Filter** to search for analysis jobs fitting your selections. A list of analysis jobs meeting those requirements is displayed.
6. Right-click on the appropriate analysis job in the history and select **Generate Report**. The report for the selected job is displayed. Once generated, the report is archived in OnBase under the **SYS Platter Management Reports** Document Type. The report displays the results and parameters of the analysis. If an analysis was canceled before it completed, a **Process Canceled by User Request** warning is written to the Platter Management Report.



Analysis Results

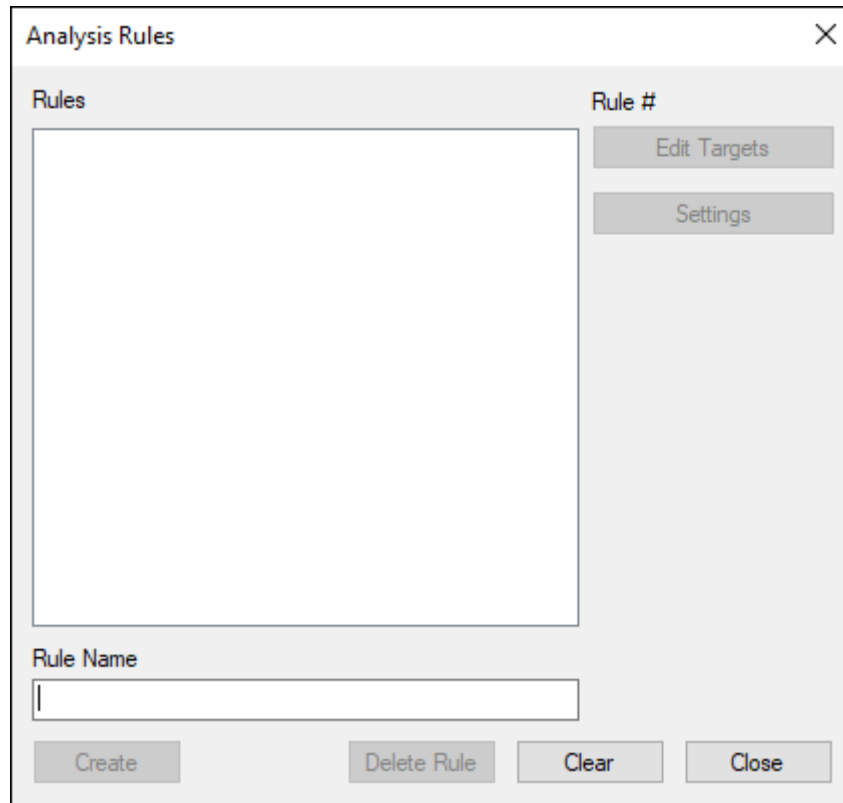
After being run, analysis jobs can have one of three results, shown below:

Analysis Result	Description
Success	The analysis job was successfully completed as planned. Right-click on the job and select Generate Report for more information on the job.
Partial Success	The analysis job was partially successful due to platters targeted for analysis that were not available. As long as two platters can be found for analysis, the analysis job continues and the job is deemed a partial success. Right-click on the job and select Generate Report for details on the missing platters and the parts of the analysis job that succeeded.
Failure	The analysis job failed. To determine the reason for the failure, right-click on the job and select Generate Report . For file specific information on the reason for failure, right-click on the job and select View File Details .

Analysis Rules

The **Analysis Rules** function in the Configuration module allows you to create rules that predetermine how analysis is performed. To create an analysis rule to perform scheduled analysis jobs in **Configuration**:

1. Select **Disk Mgmt | Analysis Rules**. The **Analysis Rules** dialog box is displayed.



The screenshot shows the 'Analysis Rules' dialog box. It has a title bar with the text 'Analysis Rules' and a close button (X). The main area is divided into two sections. The left section is labeled 'Rules' and contains a large empty rectangular box. The right section is labeled 'Rule #' and contains two buttons: 'Edit Targets' and 'Settings'. Below the 'Rules' section is a text input field labeled 'Rule Name'. At the bottom of the dialog box are four buttons: 'Create', 'Delete Rule', 'Clear', and 'Close'.

2. Type the name of the rule you are creating in the **Rule Name** field.

3. Click **Create**. The **Rule Settings** dialog box is displayed.

4. Select one of the following options in the **Trigger analysis when:** section to configure when analysis is triggered:

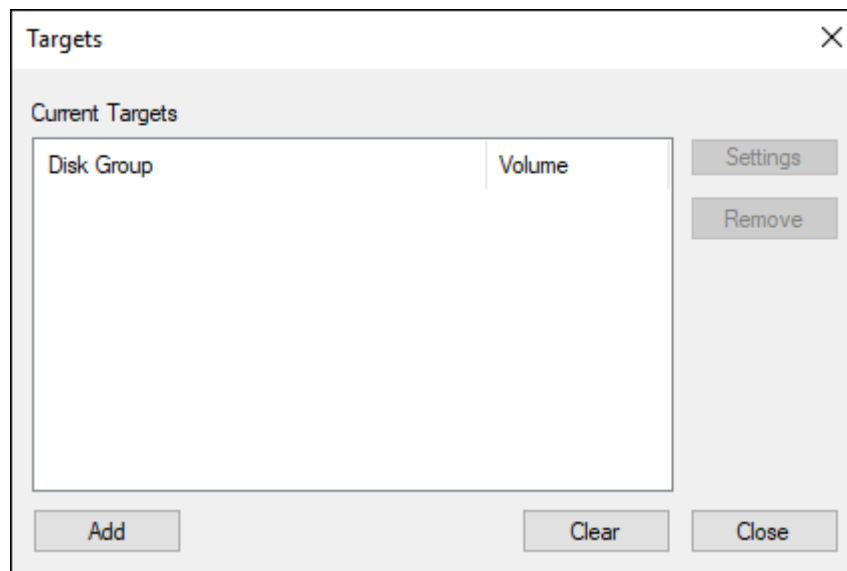
Analysis Trigger	Description
Closed volumes threshold reached	Analysis is triggered when a certain number of volumes are closed. When this option is selected, enter a number of volumes in the Volumes field to specify when analysis occurs.
Volume is closed	<p>Analysis is triggered after the volume is closed. Specify when this occurs by typing a number of days into the Begin analyzing after field.</p> <p>To reanalyze the volume after a period of time, select the Reanalyze every option and enter a number of days in that field.</p> <p>To stop reanalysis after a set period of time, select the Stop reanalyzing after option and enter a number of days into that field.</p>

5. Select an option from the **File verification method** drop-down list. The available options include:

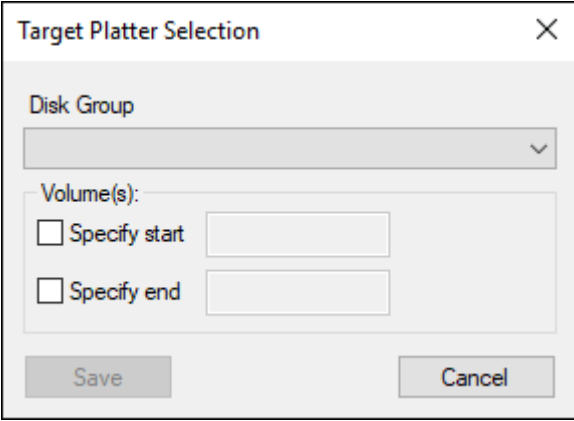
File Verification Methods	Description
Full File	Performs a byte-by-byte check of every file created in the platter and compare these files to the original files.

File Verification Methods	Description
Partial File	Performs a partial file comparison of all files in the volume using the following rules: <ul style="list-style-type: none"> • If a file is smaller than 5MB, the full files are compared. • If the file is larger than 5MB, the first megabyte, the last megabyte, and a random megabyte in the middle are compared between copies. If any difference is found between two copies, a full file analysis is performed.
File Size	Compares the sizes of files between copies.
Existence Only	Checks only for the existence of files on all copies being analyzed. Note: If you are analyzing a platter that only has one available copy for analysis, Only Check for File Existence is the only type of file verification that can be performed, as all other types require multiple copies to analyze.

6. Select the **Validate KOMpliance file retention** option to ensure that files in on a KOM server are properly retained.
7. To disable the rule to prevent it from being enacted immediately, select the **Disable rule** option. This option can also be enabled or disabled at a later time if the rule should no longer be active.
8. Once all settings are configured for the rule, click **Save**.
9. Select the rule you configured and click **Edit Targets** to select which Disk Groups, volumes, and copies will be analyzed using the rule. The **Targets** dialog box is displayed.



10. Click **Add** to select targets for the analysis rule. The **Target Platter Selection** dialog box is displayed.

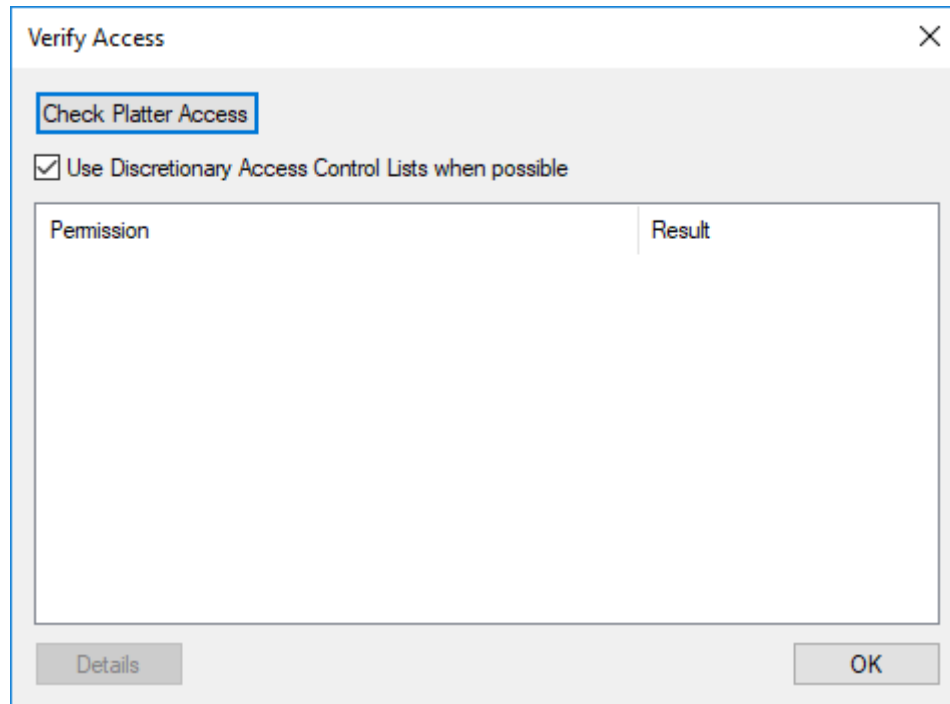
The image shows a 'Target Platter Selection' dialog box. It has a title bar with a close button (X). Inside, there is a 'Disk Group' label above a drop-down menu. Below that is a 'Volume(s):' label. Under 'Volume(s):', there are two checkboxes: 'Specify start' and 'Specify end'. Each checkbox is followed by a text input field. At the bottom of the dialog, there are two buttons: 'Save' and 'Cancel'.

11. Select a Disk Group from the **Disk Group** drop-down list.
12. If you only want certain volumes in that Disk Group to be analyzed using this rule, select the **Specify Start** and **Specify End** options under **Volume(s)**. Enter the first and last volumes to include in the respective fields.
13. Click **Save**.
14. To add more Disk Groups or volumes to be targeted by this rule, click **Add** again and repeat steps 10 through 13. Otherwise, click **Close**.
15. Repeat steps 2 through 13 for each analysis rule you want to configure.
16. Once all rules and targets are configured, press **Close** to close the **Analysis Rules** dialog box and save the rules settings.

Once configured, analysis rules will run automatically as specified in their settings. When a rule runs, it will add an analysis job to the **Analysis Jobs** queue in the **Platter Management Administration** window in the Client. Analysis jobs in this queue are executed whenever a **Disk Group Analysis Processing** task is executed in the Unity Scheduler.

Verify Access

The **Verify Access** dialog box is accessed by right-clicking on a platter copy and selecting **Verify Access**. The **Verify Access** dialog box allows the user to check their permissions on the selected platter copy.

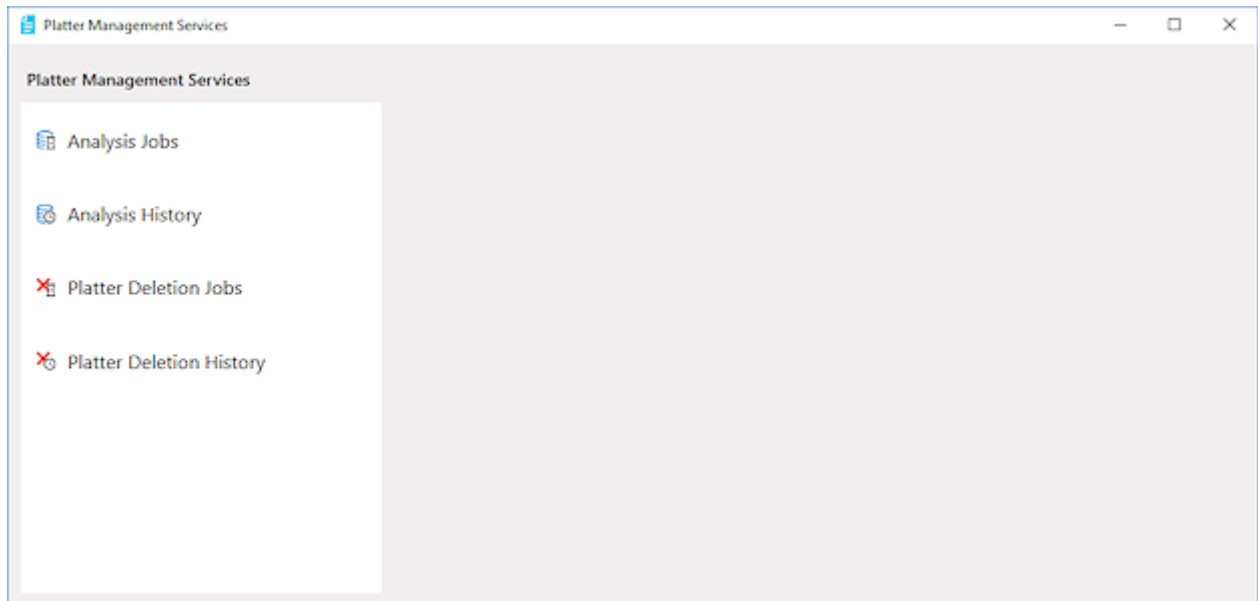


Click **Check Platter Access** to see a list of all applicable permissions and the access levels granted to the current user for each of these permissions. The **Use Discretionary Access Control Lists when possible** option is activated by default. When this option is selected, Verify Access uses access control lists to determine if the permissions are granted. When the option is deselected, Verify Access attempts to perform each of the actions as applicable to each permission and reports on the success or failure of each. Once you have clicked **Check Platter Access**, a list of permissions is displayed with results. For additional details on how access levels were determined, click **Details** to view the specific actions and checks performed for each access checked.

Once you have determined the levels of access available, click OK to close the Verify Access dialog box.

Platter Management Services

Platter Management Services is a tool for monitoring platter management jobs that are queued to be run in the Unity Scheduler and view the history of these completed jobs. Platter Management Services is accessed in the Client by navigating to **Admin | Platter Management Services**. Platter Management Services is divided into a number of separate queues including **Analysis Jobs**, **Analysis History**, **Platter Deletion Jobs**, and **Platter Deletion History**.

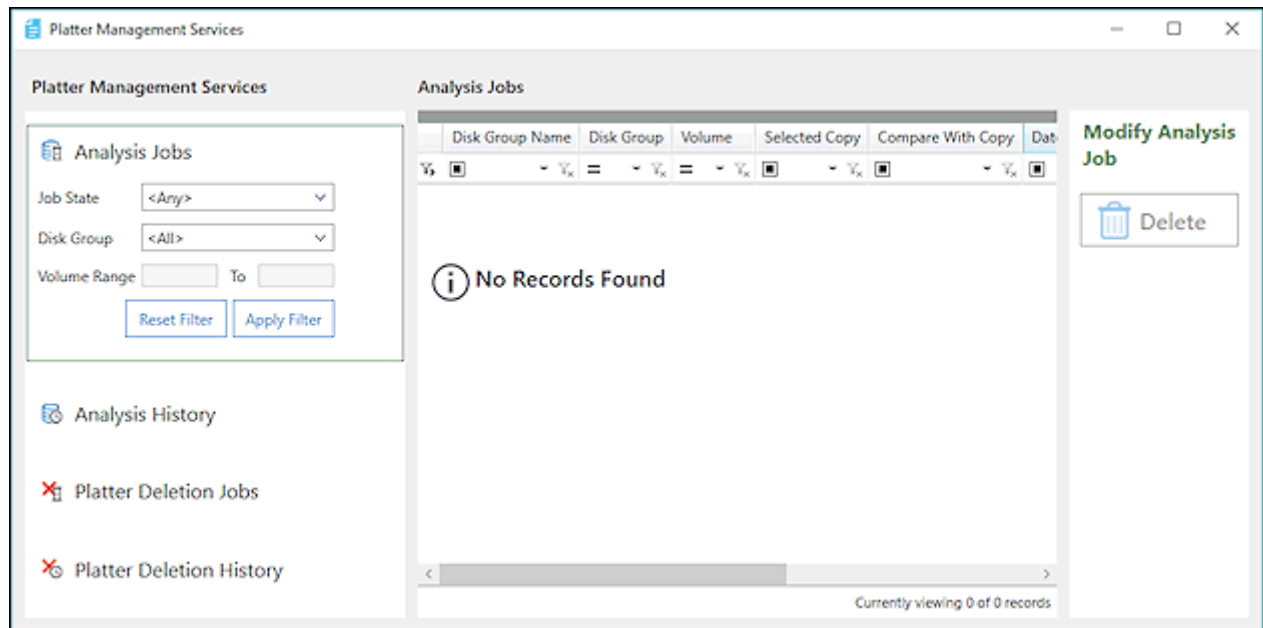


Analysis Jobs

The **Analysis Jobs** queue displays any job that has been queued up using either the **Analyze** right-click menu option in Platter Management or an analysis rule. For more information on Disk Group analysis, see [Analyze on page 123](#) and [Analysis Rules on page 128](#).

To view analysis jobs currently in the queue in **Platter Management Services**:

1. Click **Analysis Jobs**. The **Analysis Jobs** queue is displayed on the right with no jobs in the queue. The Analysis Jobs queue filter options are displayed on the left.



2. Select the filter options to determine the jobs displayed in the queue.

The screenshot shows a window titled 'Analysis Jobs' with a green header. Inside, there are three filter sections: 'Job State' with a dropdown menu showing '<Any>', 'Disk Group' with a dropdown menu showing '<All>', and 'Volume Range' with two empty input boxes separated by 'To'. At the bottom, there are two buttons: 'Reset Filter' and 'Apply Filter'.

Filter Option	Description
Job State	Set this filter option to determine the state of the jobs shown in the queue. Filter options include: <ul style="list-style-type: none"> • Enabled: Shows all jobs that will be processed when the Disk Group Analysis task is run in Unity Scheduler. • Disabled: Shows jobs that will not be processed when the task is run. • <Any>: Shows all jobs regardless of state.
Disk Group	Set this filter to only show jobs relating to a specific Disk Group or set it to <All> to show all jobs regardless of disk group.
Volume Range	Enter the range of volume numbers to show as an inclusive range. Leaving these fields blank includes all volumes on the selected Disk Group.

3. Once the desired filter options are selected, click **Apply Filter** to show all analysis jobs meeting those requirements in the Analysis Jobs queue. If you want to clear all options, click **Reset Filter**.

Disable a job by selecting the job and clicking the **Disable Job** button. This prevents the job from being executed during the next Disk Group Analysis task. A disabled job can be enabled by selecting the job and clicking the **Enable Job** button.

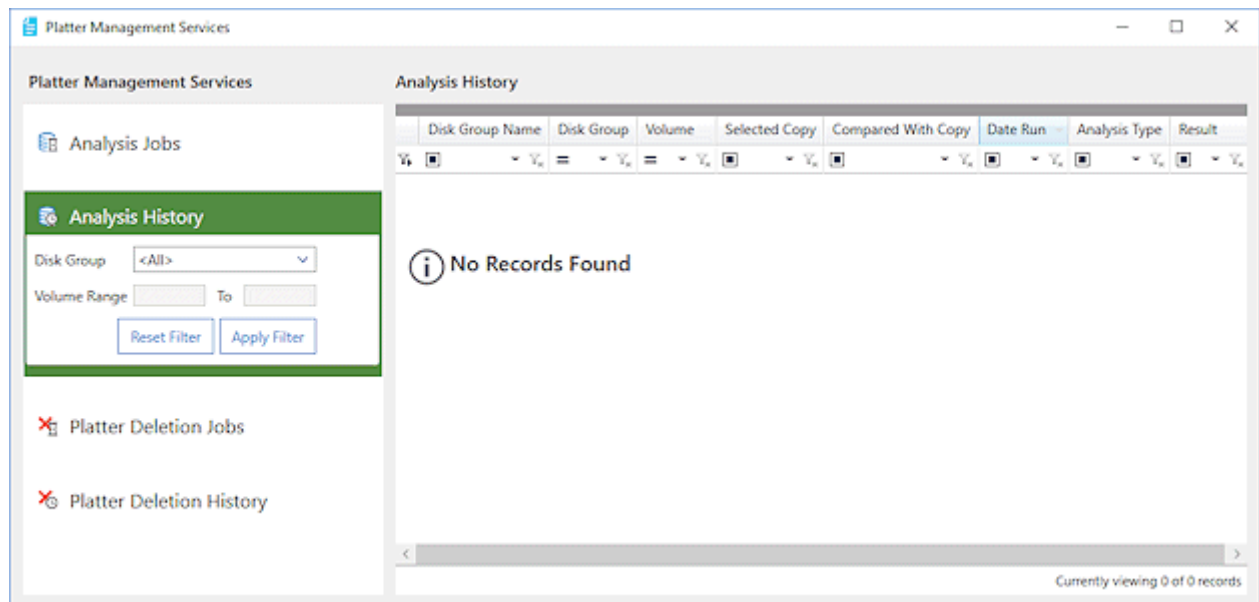
Delete a job in the **Analysis Job** queue by selecting a job and clicking the **Delete** button. A prompt is displayed to confirm that you want to delete the analysis job. Click **OK** to continue.

Analysis History

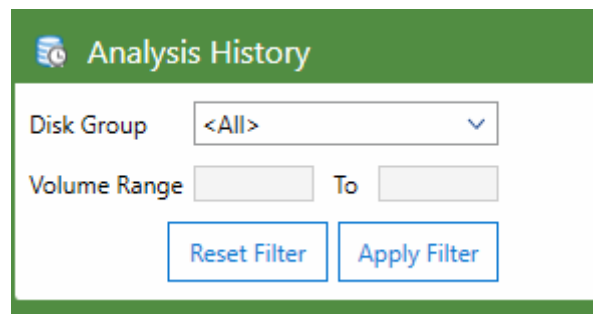
The **Analysis History** log displays any analysis jobs that have been processed. These jobs are processed using the **Run Analysis** button in the **Analyze** right-click menu option in **Platter Management** or using of a **Data Group Analysis** task in **Unity Scheduler**. For more information on performing analysis see [Analyze on page 123](#) and [Disk Group Analysis Tasks on page 179](#).

To view analysis jobs that have been completed in **Platter Management Services**:

1. Click **Analysis History**. The **Analysis History** log is displayed on the right. No jobs are displayed in the log until filter options are selected. The **Analysis History** filter options are displayed on the left.



2. Select filter options to determine the jobs to be displayed in the log.



Filter Option	Description
Disk Group	Select a disk group from the drop-down list to show completed analysis jobs for that Disk Group. Select <All> to show all jobs regardless of Disk Group.
Volume Range	Enter the range of volume numbers to show as an inclusive range. Leaving these fields blank includes all volumes on the selected Disk Group.

3. Once the desired filter options are selected, click **Apply Filter** to show all analysis jobs meeting those requirements in the Analysis History log. If you want to clear all options, click **Reset Filter**.

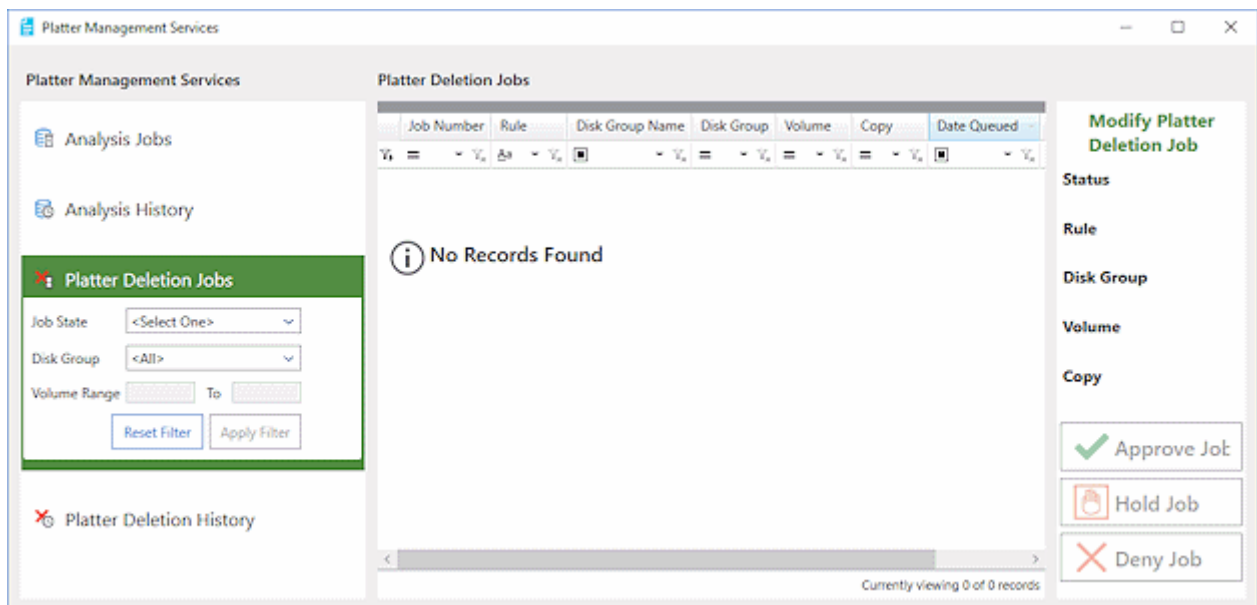
If an analysis job is not able to be completed, you can right click on the job and select **View File Details** to see the specific files that prevented the analysis and details for each. For all analysis jobs, you can right click and select **Generate Report** to see a detailed report on the analysis job.

Platter Deletion Jobs

The **Platter Deletion Jobs** queue displays any deletion job that is waiting to be processed using the **Platter Deletion Processing** task in **Unity Scheduler**. Before a deletion can be successfully processed, it needs to be approved in the **Platter Deletion Jobs** queue. For more information on **Platter Deletion Processing**, see [Platter Deletion Processing Tasks](#) on page 174.

To view deletion jobs that are awaiting processing in **Platter Management Services**:

1. Click on **Platter Deletion Jobs**. The Platter Deletion jobs queue will be displayed on the right with no jobs in the queue. The Platter Deletion jobs queue filter options will be displayed on the left.



2. Select the filter options to limit the jobs displayed in the queue.

Filter Option	Description
Job State	<p>Set this filter to only display deletion jobs that are in one of the following states:</p> <ul style="list-style-type: none"> • Unapproved: Jobs that have been queued for deletion but have not been approved, held, or denied and will remain in the queue until such action is taken. • Approved: Jobs that have been queued and approved for deletion during the next Platter Deletion Processing task. • On Hold: Jobs that have been held in the queue. These jobs will remain held in the queue and until they are finally approved or denied. • Denied: Jobs that have been denied for deletion that will not be processed. • <All>: Shows all jobs currently in the queue.
Disk Group	<p>Set this filter to only show completed deletion jobs relating to a specific disk group or to <All> to show all jobs regardless of disk group.</p>
Volume Range	<p>Enter the range of volume numbers within a disk group to show in the queue as an inclusive range, or leave these fields blank to show all volumes.</p>

3. Once the desired filter options are selected, click **Apply Filter** to show all deletion jobs meeting those requirements in the Platter Deletion History queue. If you want to clear all options, click **Reset Filter**.

Approving or Denying Deletion Jobs

Before a deletion can be completed using a **Platter Deletion Processing** task in the **Unity Scheduler**, the deletion job needs to be approved in the **Platter Deletion Jobs** queue. This provides a final step to confirm that deletion should take place, requiring manual confirmation on the part of an administrator or someone with rights to access **Platter Management Services**. For each job in platter management, several different buttons can appear to set the status of the job, based on the current status.

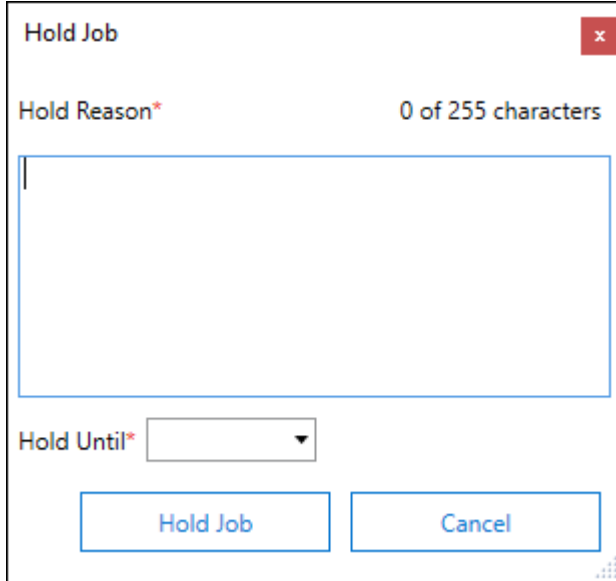
The screenshot displays the 'Platter Management' interface. On the left, a table lists deletion jobs with columns: Status, Job Number, Rule, Disk Group Name, Disk Group, Volume, Copy, and H. The 'Unapproved' job (Job Number 12400) is selected. On the right, a sidebar titled 'Modify Platter Deletion Job' shows the details of the selected job: Status (Unapproved), Rule (Deleted Rule (98765)), Disk Group (HUMAN RESOURCES), Volume (1), and Copy (2). Below these details are three buttons: 'Approve Job' (with a green checkmark icon), 'Hold Job' (with a red hand icon), and 'Deny Job' (with a red X icon).

Status	Job Number	Rule	Disk Group Name	Disk Group	Volume	Copy	H
Denied	12401	Deleted Rule (98765)	HUMAN RESOURCES	104	1	2	1/
Unapproved	12400	Deleted Rule (98765)	HUMAN RESOURCES	104	1	2	1/
Approved	12429	Deleted Rule (98765)	HUMAN RESOURCES	104	1	2	1/
On Hold	12430	Deleted Rule (98765)	HUMAN RESOURCES	104	1	2	4/

Currently viewing 4 of 4 records

With a deletion job selected, choose one of the following:

Button	Appears for Status	Description
Approve Job	Unapproved	Click this button to approve the deletion job for execution when the next Platter Deletion Processing task is run in the Unity Scheduler. The job's status is changed to Approved .

Button	Appears for Status	Description
Hold Job	Unapproved, Approved	<p>Click this button to hold the deletion job in the Platter Deletion Jobs queue to approve or deny at a later date. The following dialog box is displayed:</p>  <p>To place a job on hold, follow these steps:</p> <ol style="list-style-type: none"> 1. Add a reason the job is being placed on hold in the Hold Reason field. 2. Select a date to hold the job until from the Hold Until drop-down list. 3. Click Hold Job to change the job's status to On Hold. <p>Once a job is placed On Hold, it will remain with that status until the selected date, at which point the job's status is set to Unapproved.</p>
Deny Job	Unapproved, On Hold	<p>Click this button to deny the job, preventing the deletion from occurring when the next Platter Deletion Processing task is run. The job's status is changed to Denied.</p>
Remove Denial	Denied	<p>Click this button to remove the denial of a job, allowing the job to be approved for deletion. A dialog box appears to confirm the choice. Click Yes to continue. The job's status is changed to Unapproved.</p>
Release Hold	On Hold	<p>Click this button to remove the hold on the job, allowing the job to be approved or denied. A dialog box appears to confirm the choice. Click Yes to continue. The job's status is changed to Unapproved.</p>

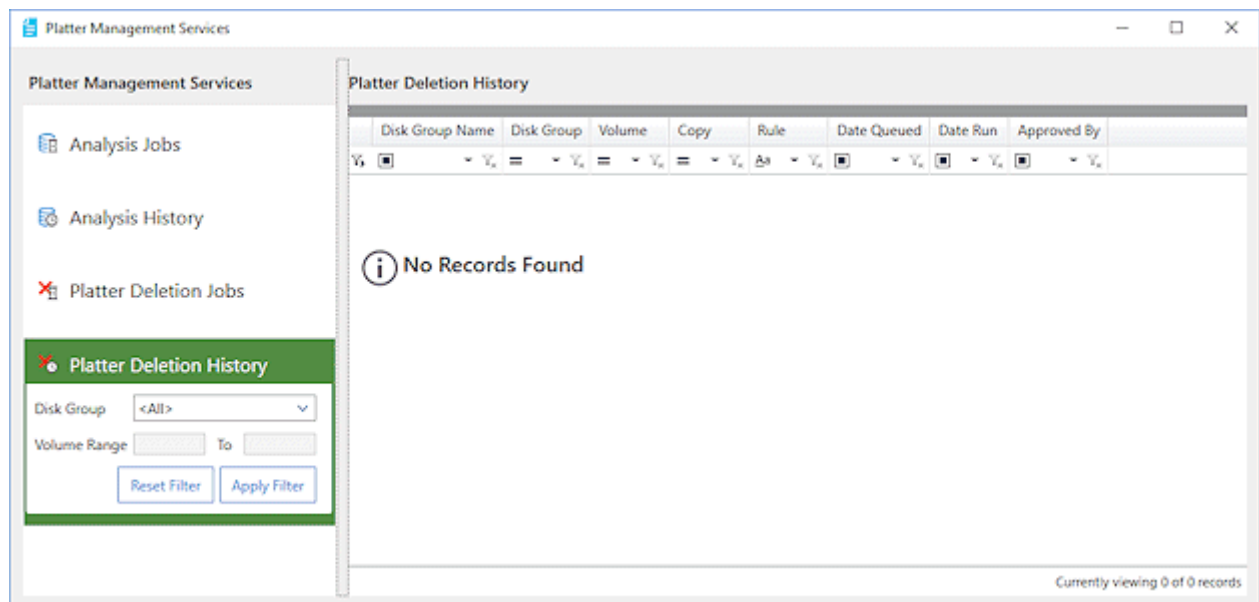
Jobs that have been approved are moved to the **Platter Deletion History** queue once the task has been run in the **Unity Scheduler**. All other jobs remain in the **Platter Deletion Jobs** queue unless approved.

Platter Deletion History

The **Platter Deletion History** queue displays any deletion job that has been processed. Jobs can be deleted using the **Manual Delete** right-click option or through the use of a **Platter Deletion Processing** task. For more information on the **Manual Delete** right-click menu option, see [Deleting Platters on page 169](#). For more information on **Platter Deletion Processing**, see [Platter Deletion Processing Tasks on page 174](#).

To view deletion jobs that have been completed in **Platter Management Services**:

1. Click **Platter Deletion History**. The **Platter Deletion History** queue is displayed on the right with no jobs in the queue. The **Platter Deletion History** queue filter options are displayed on the left.



2. Select the filter options to limit the jobs displayed in the queue.

The image shows a dialog box titled "Platter Deletion History" with a green header bar. Inside, there is a "Disk Group" dropdown menu currently set to "<All>". Below it are two input fields for "Volume Range" separated by a "To" label. At the bottom are two buttons: "Reset Filter" and "Apply Filter".

Filter Option	Description
Disk Group	Set this filter to only show completed deletion jobs relating to a specific Disk Group or to <All> to show all jobs regardless of Disk Group.
Volume Range	Enter the range of volume numbers within a Disk Group to show in the queue, or leave these fields blank to show all volumes.

3. Click **Apply Filter** to show all deletion jobs meeting those requirements in the **Platter Deletion History** queue. To clear all options, click **Reset Filter**.

Generating a Platter Deletion Report

Once a job appears in the **Platter Deletion History** queue, you can right-click it and select **Generate Report**. This report details what volumes and copies were deleted as well as when the job was queued and completed. The report also displays the user who approved of the deletion.

Customizing a Filter's Display

The display of each of the filters available in Platter Management Administration can be customized, including resizing columns, moving columns, and grouping by column headings.

Resizing Columns

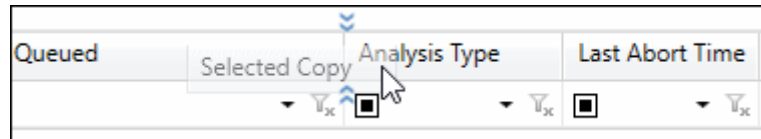
To resize a column, place your cursor over the column border that you would like to resize. The cursor becomes an arrowed line, as seen in the following example:



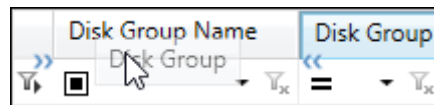
Click and drag the column's edge to the desired width.

Moving Columns

You can change the order of columns by clicking on a column header and dragging it to the location you prefer. Chevrons are displayed above and below the column headers, indicating the new location of the column header. The following is an example:



In addition, you can stack columns by clicking on a column header and dragging it to the column you want to display it under. Chevrons are displayed on the left and right sides of the column header to be stacked. The following is an example:

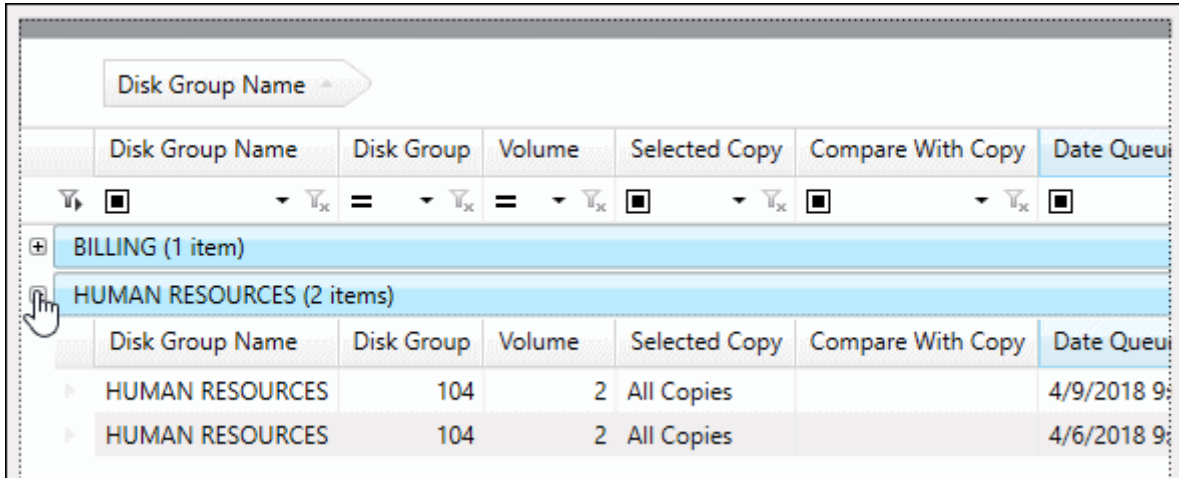


Grouping Data

Data in a Platter Management Administration view can be grouped using the column headers. To do this, click and drag a column heading to the area above the columns. The area expands, and after you drop the column header into that area, data is grouped according to it. For example, the **Disk Group Name** column is dragged above the other columns in the Analysis Jobs queue:

group by area Drag a field here to group by that field						
Disk Group Name	Disk Group	Volume	Selected Copy	Compare With Copy	Date Queued	
▶ HUMAN RESOURCES	104	2	All Copies		4/9/2018 9:09:00	
▶ BILLING	111	1	All Copies		4/6/2018 9:41:00	
▶ HUMAN RESOURCES	104	2	All Copies		4/6/2018 9:38:00	

The jobs shown in the queue are then grouped by Disk Group name, and these groups can be expanded by clicking on the + symbol.



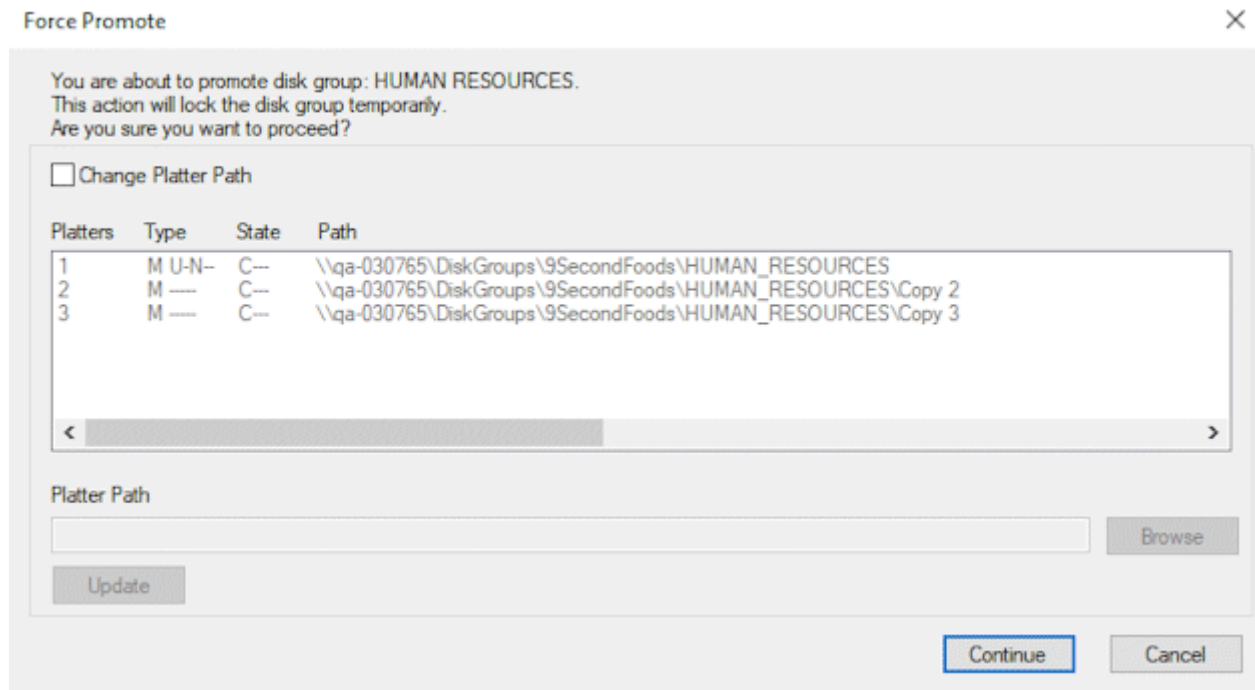
	Disk Group Name	Disk Group	Volume	Selected Copy	Compare With Copy	Date Queued
+	BILLING (1 item)					
+	HUMAN RESOURCES (2 items)					
	HUMAN RESOURCES	104	2	All Copies		4/9/2018 9:30
	HUMAN RESOURCES	104	2	All Copies		4/6/2018 9:30

Promoting a Volume in the Client

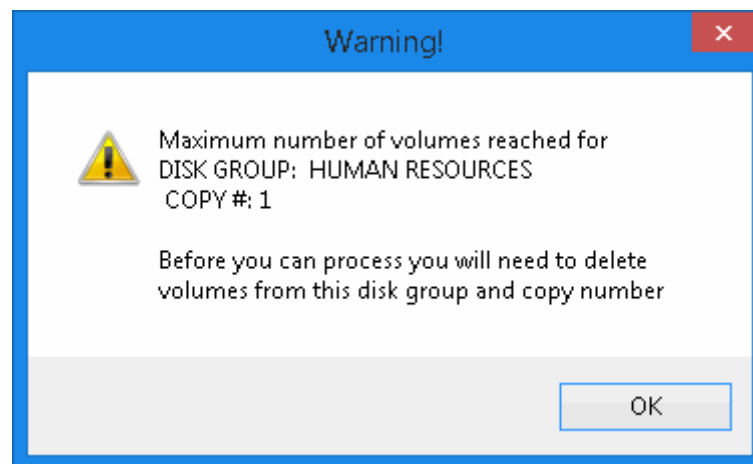
Promoting a Disk Group closes the current Volume and begins the next Volume. (The system automatically promotes a Disk Group when the current Volume is full during document processing.) To manually promote a volume:

1. From the Client module, select **Admin| Platter Management**. Select the Disk Group that contains the volume to promote. The available volumes appear on the right side of the **Platter Management** window.
2. Select a volume in the Disk Group to be promoted, and right-click it.

3. Select **Promote** from the right-click menu. The **Force Promote** dialog box is displayed.



If you have reached the maximum number of volumes designated for the Disk Group, a warning message is displayed instead.



4. If you need to change the platter path of the promoted copies, select **Change Platter Path**.
 - a. Select the platter path to change in the **Platters** pane. The current path is displayed in the **Platter Path** field.

Note: Platter paths must be UNC paths at the time of promotion. Changing paths for backup or removable copies is not allowed.

- b. Edit the path in the **Platter Path** field, or click **Browse** to select a new location for the promoted copies.
- c. Click **Update** to save your changes to the platter path.

Note: You cannot promote a volume to a location already used by another Disk Group.

5. Click **Continue** to promote the volume and create a new volume to continue storing data.

Note: If you **Force Promote** a volume, causing the minimum number of volumes to be met, copies that would enter the delete queue during an automatic promote do not enter the delete queue, even if all backup copies have been created.

Copying, Moving, and the Storage Migration Queue

Volumes and platters can be copied and moved within the **Platter Management** window. The **Storage Migration** queue offers access to the Copy and Move process jobs. These processes can also be scheduled using the familiar **Process Scheduling** interface.

Note: Jobs that are being copied are placed under a **process lock**. In **Process Lock Administration** in the Configuration module, the **Lock Type** is displayed as **Storage Migrator**. The **Key Value** field reflects the **Job ID**. If a job fails, you may have to manually remove the process lock before running the job again. For more information on Process Lock Administration, refer to the System Administration module reference guide.

Note: When using right-click to select volumes for copy or move processes, a Copy is dynamically selected if all volumes are in place. If you want to move or copy a specific Copy, you must click through to the desired Copy before right-clicking.

See the below sections for information on:

- [Copying Volumes and Platters on page 152](#)
- [Moving Platters on page 155](#)
- [Storage Migration on page 152](#)
- [Scheduling Copy or Move Processes on page 155](#)

Copying Volumes and Platters

At any time during operation, the data contained on an EMC Centera, IBM Tivoli, KOMpliance, UNC, or related Distributed Disk Service volume or platter in a Disk Group can be copied to any selected media accessible to the system, including configured devices. Only platters that are closed can be copied. This function is not available for platters that are not created or have been deleted.

Unlike the **Write** function (available in the **Backup Queue**), the **Copy** function can be performed at any time during the collection of data in a volume or platter. The **Copy** function is not intended as a permanent method of archiving data.

Note: Only one scheduled Move or Copy job can be performed at a time on the same workstation.

Tip: Copying requires independent tracking of the data contained in a volume, especially when determining when a platter is at its maximum capacity and must be copied prior to its deletion. For this reason, creating a Disk Group with a backup copy and utilizing the **Write** function to make off-line backups is recommended.

To copy a volume or platter:

1. From the Client module, select **Admin | Platter Management**.
2. Select the Disk Group in the left pane. Its volumes are displayed in the right pane.
To copy volumes, select the volumes to be copied in the right pane, then right-click and select **Copy Volumes** from the right-click menu.
To copy a platter, double-click the volume in the right pane to display its platters, then select the platter to copy, right-click, and select **Copy** from the right-click menu.
The **Copy Platter** dialog is displayed.

Copy Platter

Source Setup

Disk Group: 103

Copy: 1 ☐ Auto repair missing or null files

Volumes: 1 Select Volumes

Target Setup

Disk Group: 103 ☒ Verify Copied Files

Copy: 1

Volumes: 1

Platter Type: UNC

Platter Path:

Start Queue for Service Cancel

- [illegible]

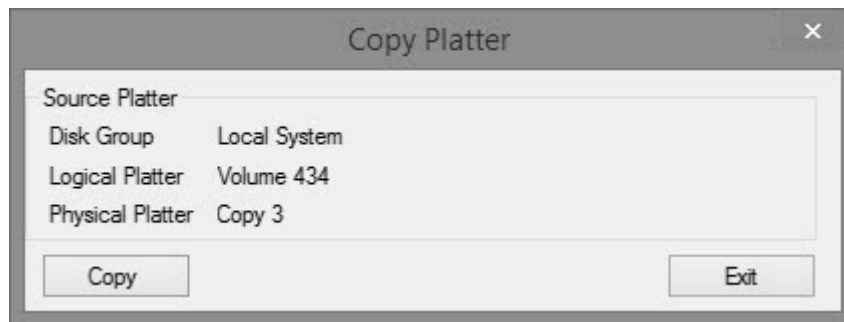
- Note:** Platter Paths are limited to 255 characters.

- 154

Copying Volumes and Platters to CD/DVD

If you are licensed for CD or DVD Authoring, you can copy files to CD or DVD from the **Platter Management** window.

1. From the Client module, select **Admin | Platter Management**.
2. Select the Disk Group in the left pane. Its volumes are displayed in the right pane.
To copy volumes, select the volumes to be copied in the right pane, then right-click and select **Copy Volumes to CD/DVD** from the right-click menu.
To copy a platter, double-click the volume in the right pane to display its platters, then select the platter to copy, right-click, and select **Copy to CD/DVD** from the right-click menu.
The **Copy Platter** dialog is displayed.



3. Click **Copy** when ready to Copy files to CD or DVD.

Moving Platters

In some cases, you may want to move an existing Disk Group to a new location. This can be accomplished in Platter Management using the Move function. Moving a platter relocates the Disk Group to another storage area or device.

Note: Files cannot be moved from one foreign device to another.

When a platter is moved, you can opt to automatically verify new files against the original files in the old location before being purged, if purge has been configured.

The **Storage Migration** queue in the Platter Management window contains queues for various job statuses.

Note: Moving from a KOMpliance platter is not supported.

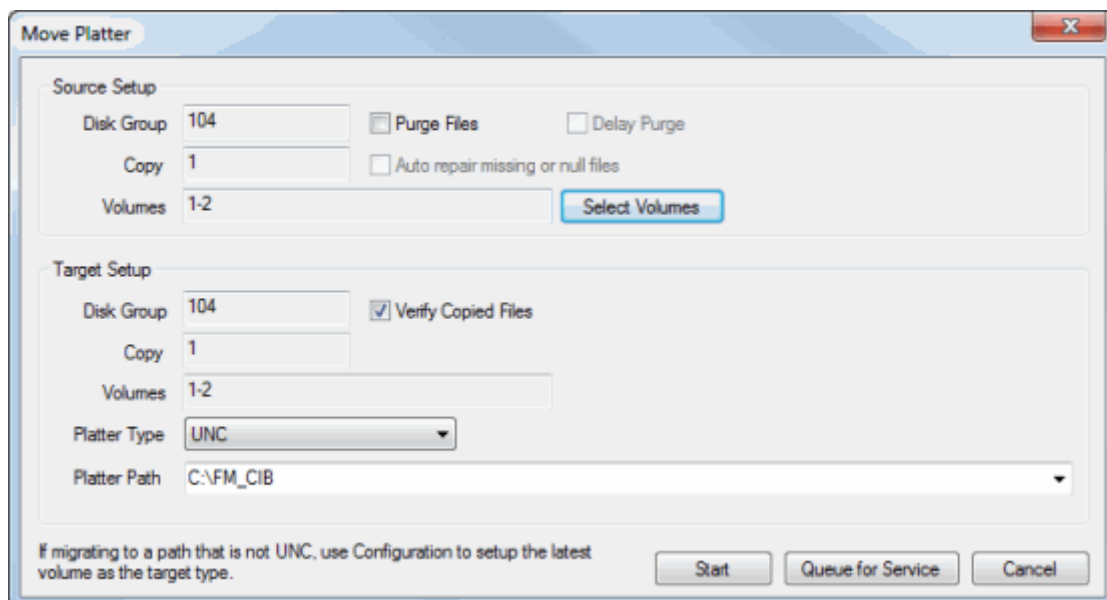
Only platters that are closed and committed can be moved (use Force Promote with the **Change Platter Path** option selected to move open platters). This function is not available for platters that are not created or have been deleted.

Note: Only one scheduled Move or Copy job can be performed at a time on the same workstation.

To move a platter:

1. In the **Platter Management** dialog box, double-click on the Disk Group in the left pane that contains the volumes you want to move.
2. Double-click on the volume in the right pane that you want to move.
3. Select the copy you want to move.
4. Right-click on the copy and select **Move**. The **Move Platter** dialog box is displayed.

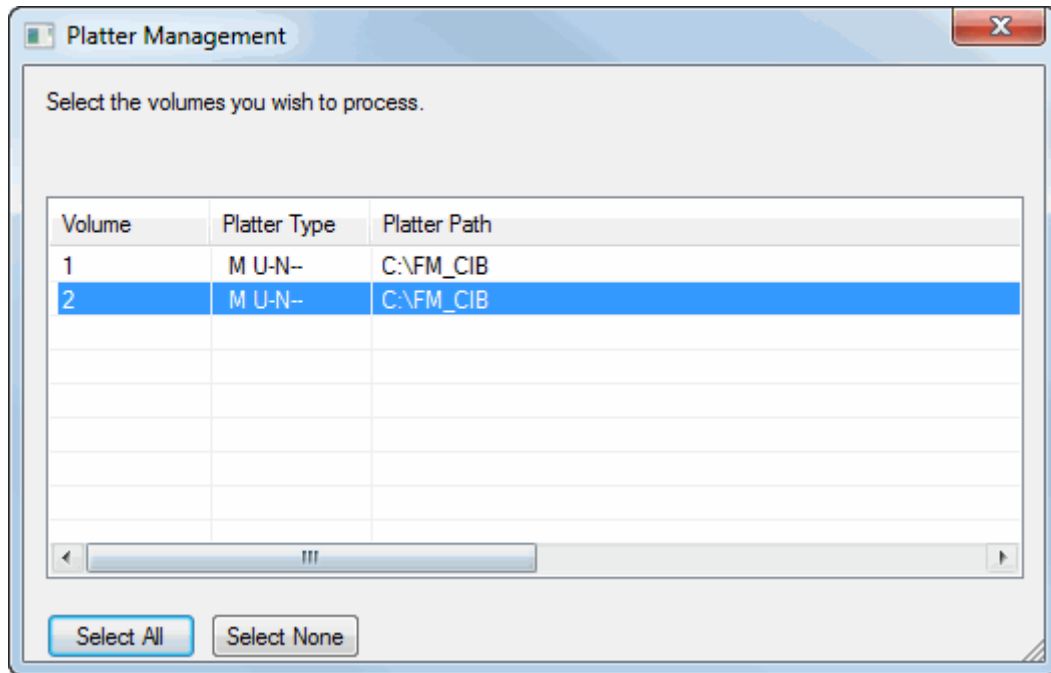
Note: This function is not available for platters that are not created or have been deleted.



5. Select **Purge Files** if you would like the files in the original destination to be deleted upon completion of the Move.
6. If you selected Purge Files, you can also choose to **Delay Purge**. Selecting Delay Purge disables the job until an administrator manually enables the job, allowing the purge to complete.

Note: If you are moving files off of an EMC Centera device, an additional option to **Purge Centera Path Aliases** is displayed. Select this option to clear database entries, but leave files on the Centera device. This option should be used with caution as files can no longer be accessed on the EMC Centera device after purging their path aliases.

7. Select **Auto repair missing or null files** if you would like source files to be auto repaired. The source file is analyzed and, if missing or the file size is reported to be 0 bytes, is replaced with an existing copy. If no suitable file is found on another copy, the file is set as an error and the job displays an Error State.
8. Select additional volumes, if needed, by clicking **Select Volumes**. A range of volumes can be selected in the **Platter Management** window that opens:



9. Click **OK** when the desired volumes have been selected.
10. In the Move Platter dialog, select **Verify Copied Files** if you require a byte-by-byte comparison with original files before changing the file path.
11. In the **Platter Type** drop down, select the new destination. This can be **UNC**, **EMC Centera**, or **IBM Tivoli**, if configured. If moving to EMC Centera or IBM Tivoli, the Copy must already be configured for the selected type of platter.

Note: Files cannot be moved from one foreign device to another.

12. Enter a valid **Platter Path**. The drop-down menu suggests recently used paths and paths of configured devices, but a new path can be entered if moving to a UNC location.

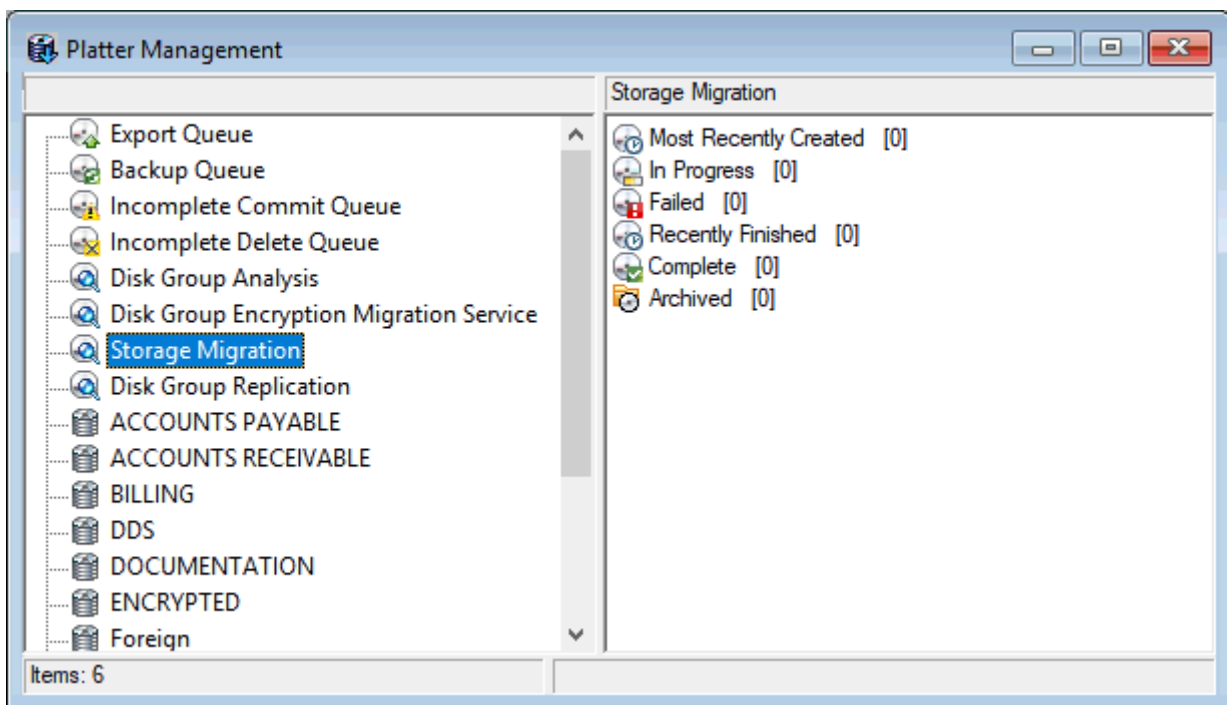
Note: Platter Paths are limited to 255 characters.

13. Click **Start** if you would like to immediately start the Move process. Click **Queue for Service** if you would like to queue the job to begin. This may be initiated by a scheduled Move Process or through the Storage Migration queue.
14. Restart all Clients and the Web Server in order for the change to be recognized.

Note: If the copy is moved from a WORM device, the files will not be automatically removed from the original location. They will need to be removed manually from the WORM device.

Storage Migration

Copy and Move process jobs are listed in the **Storage Migration** queue in the **Platter Management** window.



The following categories are available:

Category	Description
Most Recently Created	Displays the most recent 100 jobs created in Storage Migration.
Queued	Displays any jobs queued for Copy or Move processes. This category is not displayed if no jobs are queued.
In Progress	Displays jobs currently running.
Failed	Displays jobs that have failed. Refer to the Error and Error Type columns for insight on why the job may have failed. For more information on error types, see Reviewing Jobs in the Storage Migration Queue on page 160 . Jobs in the Failed queue can be run again immediately with the Run Now right-click option, or can be queued for later processing.
Recently Finished	Displays the most recent 100 jobs finished in Storage Migration.
Complete	Displays all completed jobs.
Archived	Displays jobs that have been archived. Jobs of any state may be archived. Archived jobs cannot be started again. You may consider archiving a job if it is presenting too many failures and is impeding other processes. To archive a job, right-click the job and select Archive .

Tip: All categories, except for **Most Recently Created** and **Recently Finished**, can be sorted by clicking the header of the column you would like to sort by.

Depending on the category and the status of a job, the following right-click options may be available: **Enable**, **Disable**, **Archive**, **Run Now**, **Restart**, **Retrieve Log**, **View Settings**, and **Refresh**. See the sections below for more information on actions performed in the Storage Migration Queue.

Note: Restarting moves the job to the beginning of the step it last started (Copying, Verifying, Purging, etc.).

Enabling and Disabling Jobs in the Storage Migration Queue

Jobs that have not been archived can be enabled or disabled. Enabled files are eligible for Move or Copy processing. Disabled files will not be included the next time the job is run.

To enable a job, right-click and select **Enable**.

To disable a job, right-click and select **Disable**.

Reviewing Jobs in the Storage Migration Queue

To review a job, you can view any **Failed Files**, **Error Types**, **Platter Management Reports**, and previously configured settings for the job.

Double-clicking a job will reveal the **Failed Files** for the selected job. Failed Files display **Job ID**, **File Path**, **Job State**, **Error**, **Run Number**, and whether the job is **Enabled** or not. Double-clicking the Failed File will attempt to open the OnBase document.

There are three **Error Types** you may encounter in the Storage Migration queue:

- **Recoverable:** Jobs displaying this error have encountered a recoverable file-based or job level error.
- **Non-recoverable:** These jobs have encountered a larger error and require manual intervention from an administrator to be re-enabled. Jobs can be set in this state if 100 consecutive or 15 non-consecutive non-recoverable errors are encountered.
- **No error:** These jobs did not encounter an error.

To view any available logs, right-click on a completed or archived job and select **Retrieve Log**. The **Platter Management Report**, also found in the **SYS - Platter Management Report Document Type**, is displayed.

To view the settings of a job, right click the desired job, in any queue, and select **View Settings**. The **Move** or **Copy Platter** dialog for the selected job is displayed as read-only if the job has started, but can be modified if the job has not yet started.

Move Platter

Source Setup

Disk Group: 104 ☒ Purge Files ☐ Delay Purge

Copy: 1 ☐ Auto repair missing or null files

Volumes: 1

Target Setup

Disk Group: 104 ☒ Verify Copied Files

Copy: 1

Volumes: 1

Platter Type: UNC

Platter Path: C:\FM_CIB1

If migrating to a path that is not UNC, use Configuration to setup the latest volume as the target type.

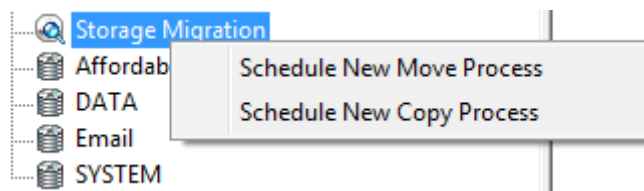
Click **Start** or **Queue for Service** if you have modified the job. Click **Cancel** if you are finished viewing the job settings without making changes.

Scheduling Copy or Move Processes

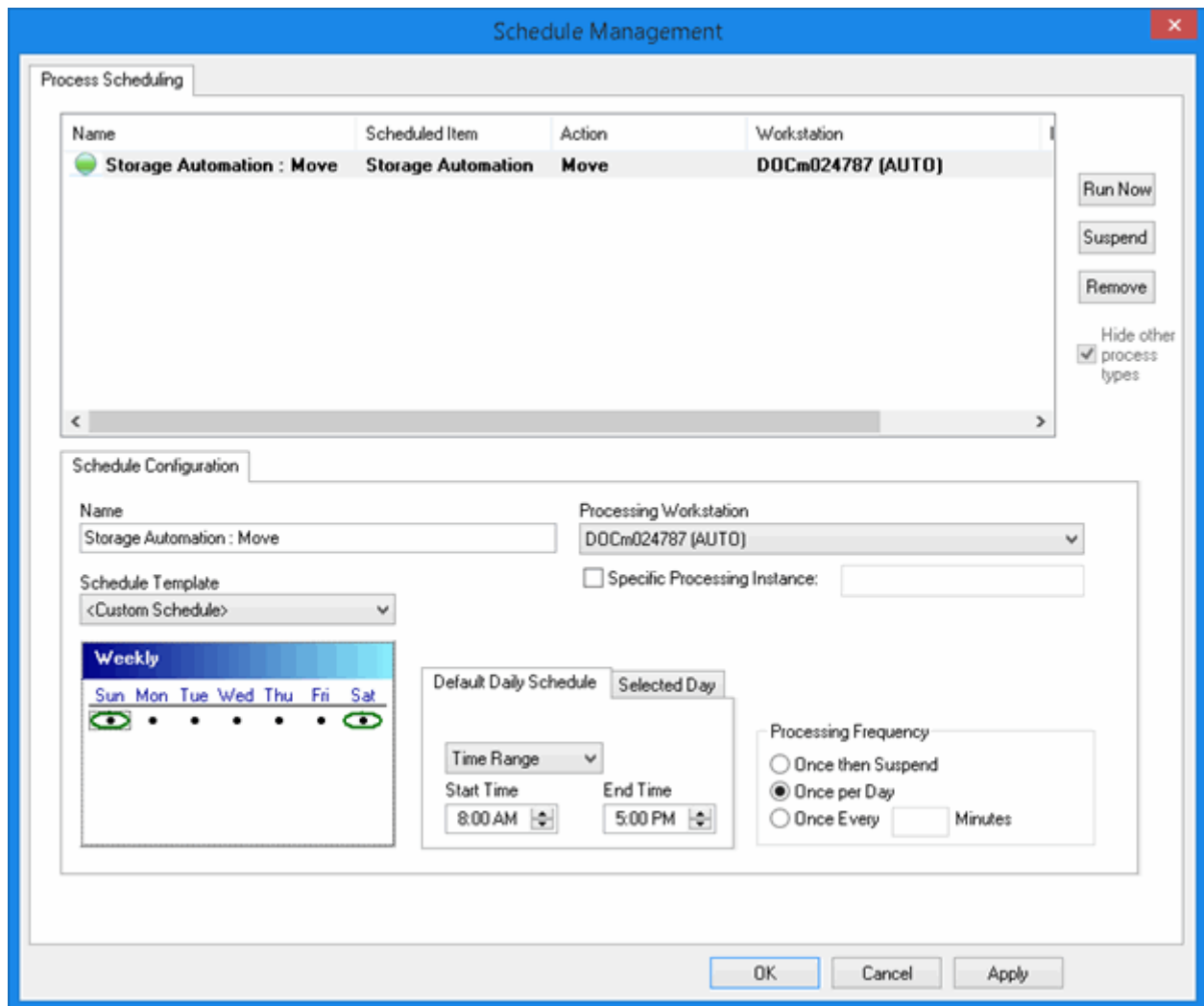
Copy and Move processes can be scheduled using the **Schedule Management** interface. Scheduling processing for off-hours is an automated way to conserve system resources. Each workstation can only move one scheduled process at a time.

Note: The **Scheduler Administrative Processing Privilege** is needed to schedule and create new jobs in the Process Scheduling dialog. When viewing jobs without editing them, or when using the **-SCHED** switch to run the processes themselves, no special rights are required.

Right-click the **Storage Migration** queue to select **Schedule New Move Process** or **Schedule New Copy Process**.



The **Schedule Management** dialog is displayed.



The first options that must be configured for the scheduled process are the Schedule Configuration options on the **Schedule Configuration** tab. This tab is displayed by default.

1. In the **Name** field, enter a name for the scheduled process.
2. Using the **Processing Workstation** drop-down, select the workstation that will be used to run the scheduled process.

Note: This workstation will need to be running with the **-SCHED** or **-SCHEDINST** command line switch in order to run the scheduled process.

3. If you always want the scheduled process to be run from a specific instance of the OnBase Client, select the **Specific Processing Instance**, then enter the name of the instance in the **Specific Processing Instance** text field.

Note: If you select the **Specific Processing Instance** option but leave the **Specific Processing Instance** text field blank, the scheduled process can be run from any instance of the OnBase Client.

4. Using the **Schedule Template** drop-down, select one of the schedule templates for the process or select **<Custom Schedule>** to manually configure the schedule for this process.

Note: For information on creating a **Custom Schedule** or **Schedule Template**, see below.

5. Select how often you would like the scheduled process to run by selecting one of the Processing Frequency radio buttons.
 - **Once then Suspend.** The scheduled item will be processed once, then the scheduled process is suspended.
 - **Once per Day.** The scheduled item will be processed once per day.

Note: If the scheduled item is modified, the process may be run again on the same day.

- **Once every "" Minutes.** The scheduled item is processed in the interval (measured in minutes) entered in the field. The maximum number of minutes that can be entered is 99999.

Caution: This option is only supported when the **Default Daily Schedule** is set to **Time Range**. If your **Default Daily Schedule** is set to **Specific Time**, the scheduled item will only be processed at the specified time.

6. When you are finished setting the **Schedule Configuration** options, click **Apply**.

Calendar

The calendar is used to select the day(s) on which a scheduled process should be run.

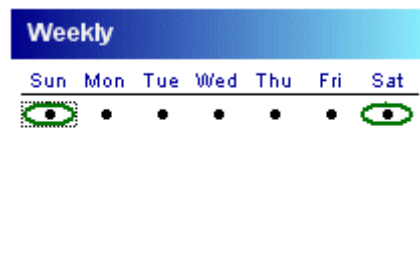
Note: The calendar is displayed based on your Workstation Regional Settings and the OnBase language DLL that you are using.

To change the view of the calendar, click the calendar heading (in the example above, **Weekly**) to display a menu. Select one of the following options to display a different calendar for configuration:

- **Weekly.** Allows you to configure a process to run on a certain day of the week (i.e., Thursday).
- **Monthly.** Allows you to configure a process to run monthly, on a particular date (i.e., the 1st and 15th of the month).

- **Monthly** (Day-Relative). Allows you to configure a process to run on a relative day of the month (i.e., the first Saturday of the month, the 2nd Wednesday of the month).
- **Annual**. Allows you to configure a process to run on a certain day of the year (i.e., June 30).
- **Full Calendar**. Allows you to configure a process to run on specified days of specified years (e.g., August 10, 2011 and/or July 17, 2012).

To select days that you would like to run a scheduled process, double-click the day on the calendar. The selected day is circled.

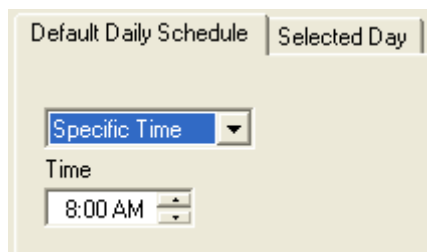
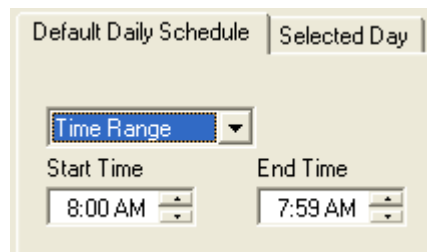


Note: In the example above, two days are selected but **Sunday** is the currently-selected day.

To deselect a day, double-click it.

Default Daily Schedule

The **Default Daily Schedule** tab allows you to configure the processing configuration for all days that do not have a **Selected Day** tab configuration.

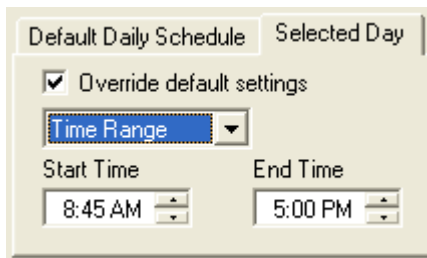


The drop-down list allows you to select **Time Range** or **Specific Time**. If you select **Time Range**, a **Start Time** box and an **End Time** box are displayed. Define the range of time in which you want your job or format to begin processing. If you select **Specific Time**, a **Time** box is displayed. Select the time at which you want the job or format to begin processing.

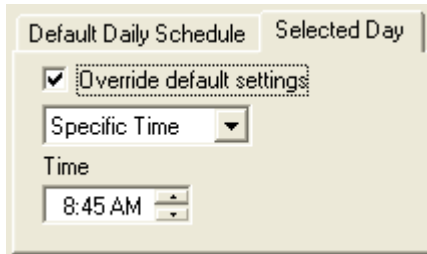
Tip: Specifying a **Time Range** and using the **Once Per Day** option will allow a scheduled process to run even if another process runs over its starting time, as long as the process is able to start within the specified range.

Selected Day

The **Selected Day** tab allows you to specify settings for the selected day that differ from the settings specified in the **Default Daily Schedule** tab. In order for the **Selected Day** tab to be enabled, you must click a day to select it and you must select the **Override default settings** check box.



The screenshot shows the 'Selected Day' tab in a software interface. It features a checked checkbox labeled 'Override default settings'. Below this is a dropdown menu currently set to 'Time Range'. Underneath the dropdown are two time selection boxes: 'Start Time' set to '8:45 AM' and 'End Time' set to '5:00 PM'. At the top of the tab, there are two sub-tabs: 'Default Daily Schedule' and 'Selected Day'.



The screenshot shows the 'Selected Day' tab in a software interface. It features a checked checkbox labeled 'Override default settings'. Below this is a dropdown menu currently set to 'Specific Time'. Underneath the dropdown is a single time selection box labeled 'Time' set to '8:45 AM'. At the top of the tab, there are two sub-tabs: 'Default Daily Schedule' and 'Selected Day'.

The drop-down list allows you to select **Time Range** or **Specific Time**. If you select **Time Range**, a **Start Time** box and an **End Time** box are displayed. Define the range of time in which you want your job or format to begin processing. If you select **Specific Time**, a **Time** box is displayed. Select the time at which you want the job or format to begin processing.

Tip: Specifying a **Time Range** and using the **Once Per Day** option will allow a scheduled process to run even if another process runs over its starting time, as long as the process is able to start within the specified range.

At every processing state reached by the enabled item, the scheduler checks for the end time. If the end time is reached, the job is paused until the next beginning time. The job is shown in the **Queued** and **In Progress** categories of Storage Migration.

Backing Up Platters

If a Disk Group is created with a backup platter, the process of making a backup of the data when a platter is closed can be semi-automated or fully automated. When a volume is closed (through promotion or when the maximum size is reached) the backup platter from the closed volume is displayed in the Backup Queue.

The platter remains in the Backup Queue until a semi-automatic or automatic backup copy is made, at which time the platter is moved to the Delete Queue.

- If the workstation is licensed for **CD Authoring**, the data can be moved to permanent off-line CD storage with the **Write to CD-R** right-click menu option (specific to the Backup Queue).
- If the workstation is licensed for **Automated CD Authoring**, the data can be moved to permanent off-line CD storage without any operator intervention, when the copy reaches maximum size.
- If the workstation is licensed for **Automated CD Authoring**, and the **-AUTOWRITECD** switch is applied, the workstation can be used as an Automated CD Authoring server, and the data to be backed up can automatically be sent to a Rimage production server for creating CDs.

Note: The service will not start if the client has been running for longer than 24 hours. In order for the service to be executed daily, the client must be restarted each day after the configured time window has elapsed.

- If the workstation is licensed for **DVD Authoring**, the data can be moved to permanent off-line DVD storage with the **Write to DVD-R** right-click menu option (specific to the Backup Queue).
- If the workstation is licensed for **Automated DVD Authoring**, and the **-AUTOWRITECD** switch is applied, the workstation can be used as an Automated CD Authoring server, and the data to be backed up can automatically be sent to a Rimage production server for creating DVDs.

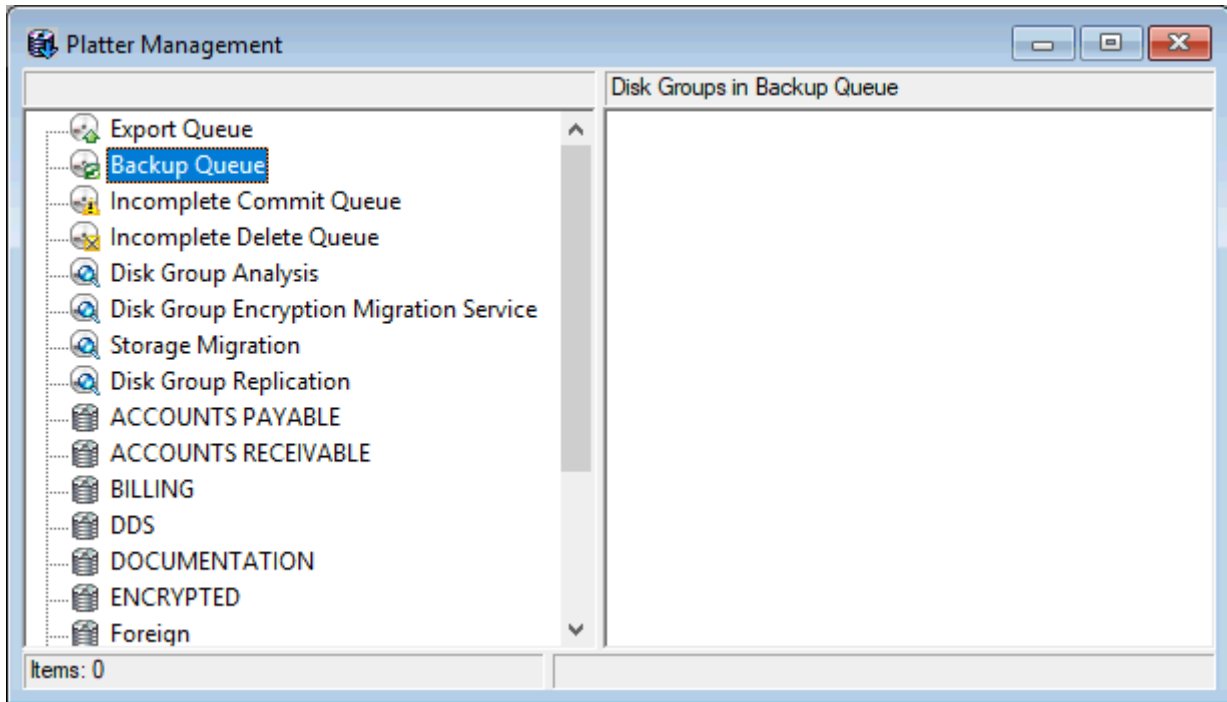
Automated backups are created in chronological order based on the promotion date of the platters in the queue (platters that entered the queue longest ago are backed up first).

Reports for each volume backed up are stored under the **SYS - Platter Management Reports** Document Type in OnBase.

Backup to CD or DVD

To backup a platter to a CD or DVD:

1. Click on the **Backup Queue** to display the Disk Groups that have been moved to a backup state.



2. Double-click on a Disk Group in the right side of the **Platter Management** window to display the platters of the Disk Group that are available for backup.
3. Select the desired platter and right-click. Select either **Write to Disk** or **Write to CD-R/ DVD-R**, depending on the media used for the backup.

Note: Unlike the **Copy** function, the **Write** functions can only be used for closed platters and are intended to produce an offline backup of the data that exists in a final state.

4. Navigate to the location where the backup will be stored (you must specify a full path) and click **OK**. The files are copied to the location specified.

Automated Backup to Rimage

If the following setup conditions have been met, backup jobs are automatically queued as soon as a Disk Group promotes (i.e., backup platter is created):

- Dedicated Workstation with **-AUTOWRITECD** switch
- Rimage fully operational and integrated into the network
- Client Workstation licensed for Automated CD Authoring or Automated DVD Authoring

If the Rimage Unit supports both CD and DVD production, and the Automated DVD Authoring license was purchased and installed, the system will create CDs if the Disk Group size is less than 1 GB. If it is 1GB or larger, then a DVD will be produced.

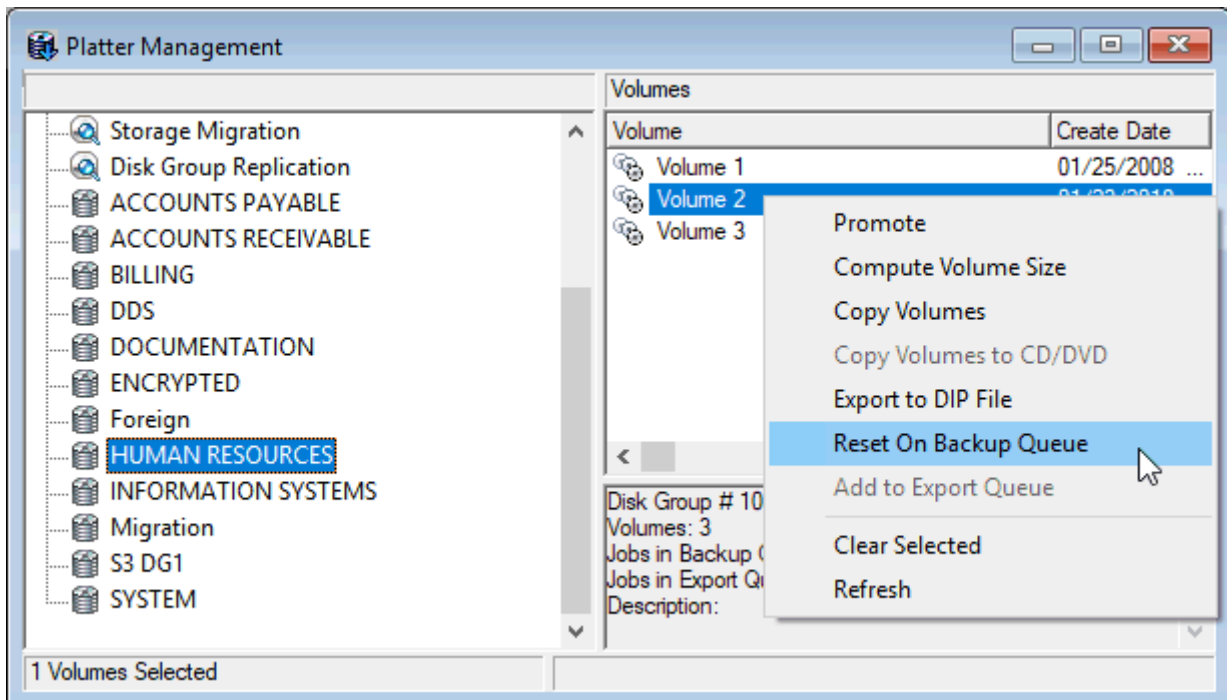
Reset on Backup Queue

Selecting this option places an entry for the volume in the Backup Queue, allowing any of the available right-click options to be performed for the platter.

This function is intended to generate additional backup copies for volumes that have been previously backed-up (that is, volumes whose backup platters no longer exist in Platter Management).

Note: The **Reset on Backup Queue** option cannot be used to generate multiple copies of the same backup platter in the Backup Queue. Only one backup platter can exist in the Backup Queue for each Disk Group volume.

1. Select **Admin | Platter Management** in the OnBase Client to access the **Platter Management** window.
2. Double-click the desired Disk Group to display the available volumes; double-click a volume to display the available copies.
3. Select the volume or copy that contains the backup platter to be reset. Right-click and select **Reset on Backup Queue**.



A copy of the backup platter is sent to the Backup Queue.

Deleting Platters

Platter deletion is only available for:

- Mass storage platters
- Removable platters
- Backup platters

Platter deletion cannot be performed on externally filled platters, import platters, foreign platters, cloud replication destinations, and platters that have active disk encryption migration jobs in progress.

Platter deletion can be performed using several different methods. These methods include:

- Configuring Disk Groups in **Volume Configuration** to hold only a **Maximum # of Volumes** online. As volumes are filled or promoted, the maximum number of volumes that can be kept online is reached, and volumes must be deleted in order to continue processing data into OnBase. Volumes beyond the specified maximum number are automatically added as deletion jobs to the **Platter Deletion Jobs** queue.
- Deleting Platters manually using the **Manual Delete** right-click menu option in Platter Management.
- Scheduling deletion based on **Platter Deletion Rules**, which create jobs in the **Platter Deletion Jobs** queue based on specific conditions for targeted platters.

For all platter deletions except those done using **Manual Delete**, the deletion is established as a job in the **Platter Deletion Jobs** queue. Jobs in this queue need to be manually approved or denied. Approved jobs are executed the next time a **Platter Deletion Processing** task is run in the Unity Scheduler.

Note: For all platter deletions, an analysis of the platter is automatically completed prior to deletion. This analysis ensures that the platter being deleted is not the sole copy of that data; the platter is not deleted if it is the sole copy. Additionally, analysis verifies that all files are fully intact and present on the platter being deleted and in any remaining copies of the same data. Analysis also repairs any files on the copies that are not being deleted. Platter deletion is completed even if these repairs are not successful. For more information on viewing reports on these analyses, see [Viewing Analysis Reports on page 132](#).

Note: Platter deletion cannot be performed if the platter being deleted is the only copy of the data stored on that platter. Automatic checks will be performed to prevent the platter from being either manually deleted or scheduled as a platter deletion job.

Manually Deleting Platters from the Disk Group

If the deletion is performed at the Disk Group level, any platter can be selected. You cannot delete a copy unless all batches found in it have been fully committed. If the copy contains items to be committed or items in the **Incomplete Commit Queue**, it cannot be deleted.

For all deletions, an analysis of the platter is automatically performed prior to deletion. For more information on analysis, see [Analyze on page 123](#).

Caution: Once a copy is deleted, it cannot be recovered.

To delete platters from a Disk Group:

1. Select the Disk Group in the **Platter Management** window. The volumes associated with that Disk Group are displayed in the right pane.
2. Double-click a volume to display its copies.
3. Right-click the copy to delete and select **Manual Delete**.
4. You are prompted to confirm that you want to delete the platter. Click **Yes** to continue.
5. You are prompted once again to confirm that you want to delete the platter. Click **Yes** to continue.
6. A progress bar is displayed while the deletion is completed. To cancel the deletion in progress, click **Cancel**. This adds the deletion as a job in the **Platter Deletion Jobs** queue in **Platter Management Services** to be run at a later time. For more information on this queue, see [Platter Deletion Jobs on page 143](#).

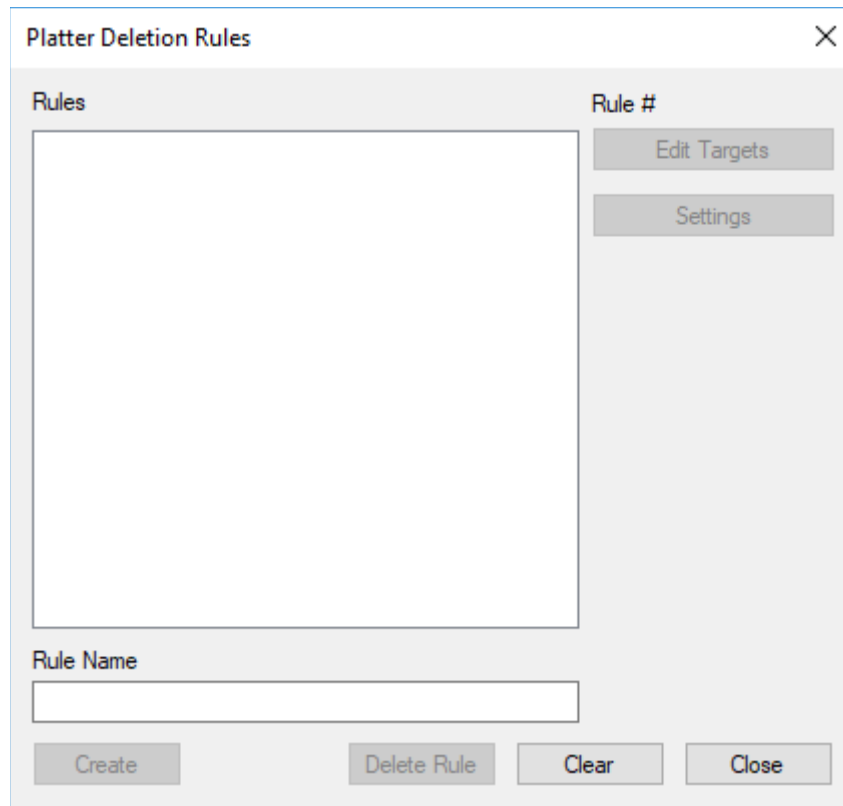
Note: If a manual deletion job is canceled, the job may still be created in the **Platter Deletion Jobs** queue in the **Platter Management Services** window. You should check to be sure the job is not there to ensure it is not executed with the next Platter Deletion Processing task. If the job is present in the queue, place it on **Hold** to prevent it from being executed.

Note: To produce a log of the files deleted, select the **Enable generation of deleted file reports** option under the **Platter Management** tab of the **Global Client Settings** dialog box in the OnBase Configuration module. This report contains the full paths to all copies of all files deleted from the Disk Groups and is stored in OnBase as **Deleted Files** under the **SYS - Platter Management Reports** Document Type. See the Configuration help files for details on selecting this option.

Platter Deletion Rules

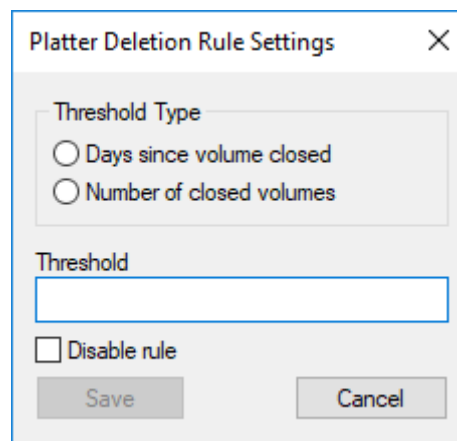
Platter deletion of specific volumes can be scheduled based on specific conditions using the **Platter Deletion Rules** function in the Configuration module. To create a rule to schedule deletion jobs in the Configuration module:

1. Click **Disk Mgmt | Platter Deletion Rules**. The **Platter Deletion Rules** dialog box is displayed.



The **Platter Deletion Rules** dialog box features a title bar with a close button (X). The main area is divided into two sections. The left section, labeled **Rules**, contains a large empty rectangular box. The right section, labeled **Rule #**, contains two buttons: **Edit Targets** and **Settings**. Below the **Rules** section is a text input field labeled **Rule Name**. At the bottom of the dialog are four buttons: **Create**, **Delete Rule**, **Clear**, and **Close**.

2. Type the name of the rule you are creating in the **Rule Name** field.
3. Click **Create**. The **Platter Deletion Rule Settings** dialog box is displayed.

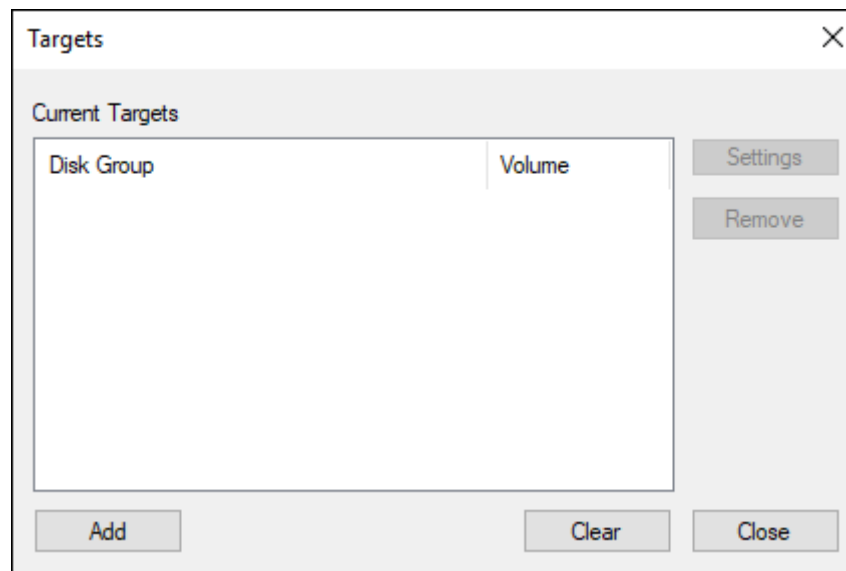


The **Platter Deletion Rule Settings** dialog box has a title bar with a close button (X). It contains a section labeled **Threshold Type** with two radio button options: **Days since volume closed** and **Number of closed volumes**. Below this is a text input field labeled **Threshold**. At the bottom left is a checkbox labeled **Disable rule**. At the bottom right are two buttons: **Save** and **Cancel**.

4. Select when the deletion will be scheduled to occur, based on two different threshold types.

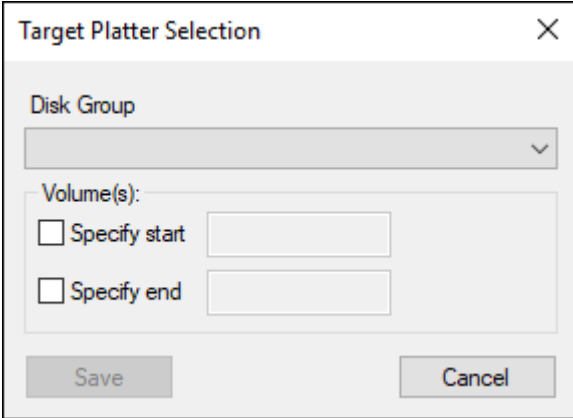
Threshold Type	Description
Days since volume closed	Select this option to specify that deletion occurs after a number of days after the volume was closed.
Number of closed volumes	Select this option to specify that deletion occurs after a certain number of volumes have been closed.

5. Type the threshold number you want to set into the **Threshold** field. Depending on the choice of **Threshold Type**, this will be either a number of days or a number of volumes.
6. Enable the **Disable rule** option to temporarily prevent the rule from going into effect. This option can later be changed in the **Settings** menu in the **Platter Deletion Rules** dialog box.
7. Once all settings are configured for the rule, click **Save**.
8. Select the rule you configured and click **Edit Targets** to select which Disk Groups, volumes, and copies will be targeted for deletion using the rule. The **Targets** dialog box is displayed.



Note: Each Disk Group can only be targeted by one rule at a time. If a rule already targets a Disk Group, no new rules will be able to target that Disk Group.

- Click **Add** to select targets for the deletion rule. The **Target Platter Selection** dialog box is displayed.

The image shows a dialog box titled "Target Platter Selection" with a close button (X) in the top right corner. Inside the dialog, there is a "Disk Group" label above a drop-down menu. Below this, there is a "Volume(s):" label. Under "Volume(s):", there are two options: "Specify start" with a text input field, and "Specify end" with a text input field. At the bottom of the dialog, there are two buttons: "Save" and "Cancel".

- Select a Disk Group from the **Disk Group** drop-down list.
- If you only want certain volumes in that Disk Group to be deleted using this rule, select the **Specify Start** and **Specify End** options under **Volume(s)**. Enter the first and last volumes to include in the respective fields.
- Click **Save**.
- Add more targets as needed, then click **Close**.
- Once all rules and targets are configured, press **Close** to close the **Platter Deletion Rules** dialog box.

Once configured, deletion rules run automatically as specified in their settings. When a rule runs, it adds a deletion job to the **Platter Deletion Jobs** queue in the **Platter Management Services** window in the Client. Deletion jobs in this queue are executed whenever a **Platter Deletion Processing** task is executed in the Unity Scheduler.

Additional Resources

For more information on platter deletion, see the following:

- [Platter Deletion Jobs on page 143](#)
- [Platter Deletion Processing Tasks on page 174](#)

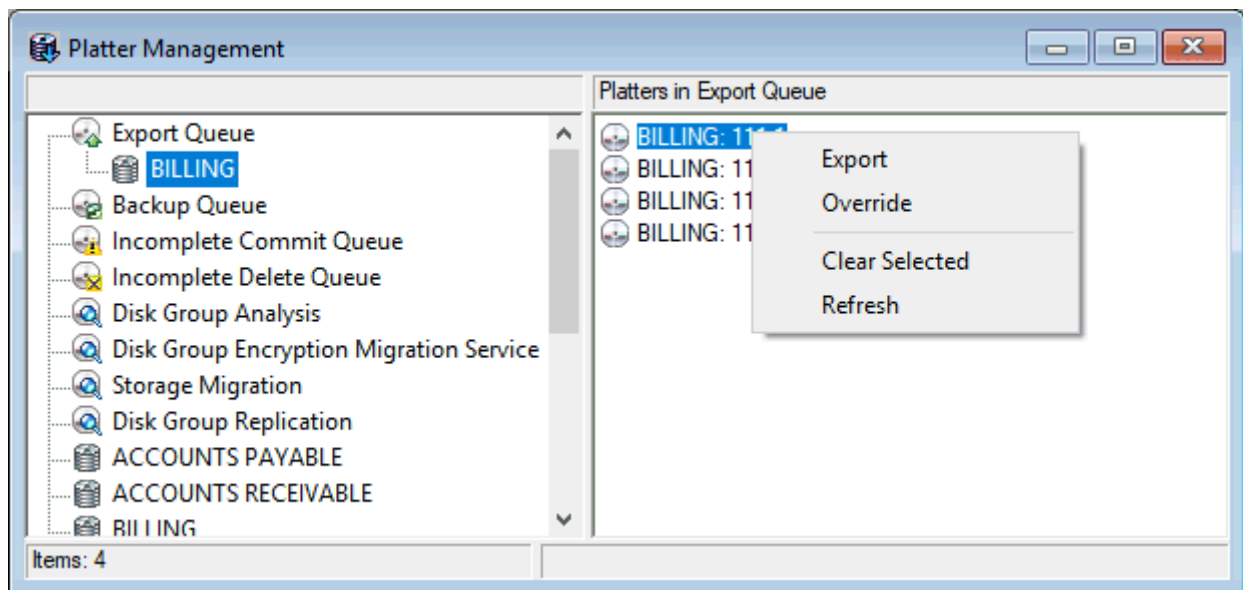
Exporting Platters

The **Export Queue** contains any Disk Group volume that was designated as an export copy when the Disk Group was configured. The data files from this volume can be moved in their entirety, along with the appropriate database indices, to another database, using the **Export** right-click option. Disk Group volumes are not added to the Export Queue until the Disk Group has been promoted and the volume is closed.

Note: The **Export** license is required in order to export platters from the Export Queue.

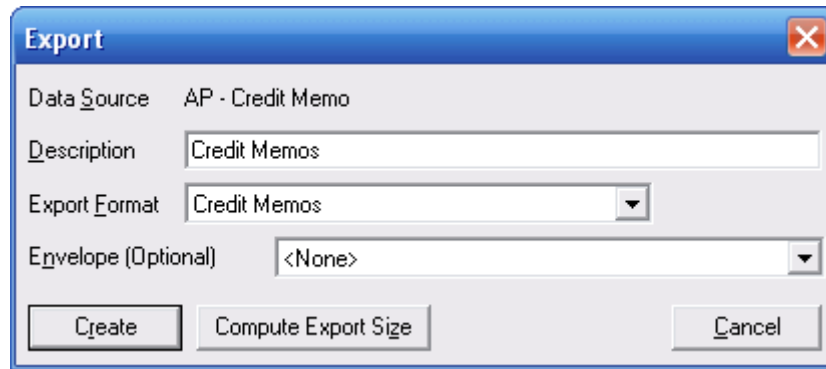
In addition to the **Export Queue**, data can also be exported on an individual platter basis from any of the Disk Groups in the **Platter Management** window.

1. In the OnBase Client, select **Admin | Platter Management**. The **Platter Management** window is displayed.
2. To export from the Export Queue, select **Export Queue** in the left pane of the **Platter Management** window.
To export from a Disk Group, select the Disk Group in the left pane of the **Platter Management** window.
3. Double-click a Disk Group in the right pane, then select an eligible platter within the Disk Group.
4. Right-click the platter to be exported and select **Export**. This function is not available for platters that are not created or have been deleted.



Tip: To remove a promoted volume from the Export Queue, select **Override** from the right-click menu. You are prompted to confirm the removal of the volume.

5. The **Export** dialog box is displayed, the parameters of which are explained below.



Parameter	Description
Data Source	The volume information of the selected source.
Description	A user-defined, alphanumeric description of the collection of exported data.
Export Format	The Export Format that will be used to direct the export of data. Export Formats are defined in the Configuration module and can be selected from the drop-down list.
Envelope (Optional)	<p>If desired, the data contained in an Envelope can be included in the export. Select the Envelope from the drop-down list to include its contents.</p> <p>To add customized system icons and bitmaps (SYS System Bitmaps and SYS System Icons) associated with the exported data, include them in an Envelope.</p>
Compute Export Size	Allows the user to calculate the number of discs required to export the selected data, before the data is exported.

6. Supply the appropriate Export parameters and click **Create** to add the data to the Export database.
7. The export proceeds and a progress bar is displayed. When complete, select **Refresh** at the queue level. The volume will be removed from the list of available volumes to be exported.

You can also select **Compute Export Size** to estimate the number of discs required for the selected Export, before it is produced. This button becomes active after a **Description** and **Export Format** are selected. If selected, the process is run and the **Estimated Export Requirements** dialog box is displayed. This dialog provides information about the estimated number of discs required for the Export and the space used on each disc.

The information is presented in two ways: A list of Items, which displays the size for each disc number and Disk Group volume number (e.g., **Disc 1, Disk Group Volume 1**); and the **Grand Total**, which is the estimated sum of space required for all supporting files and discs listed (Publishing requires supporting files, such as the installer and runtime client).

Click **Create** in the **Compute Export Size** dialog box to run the Export process, or click **Cancel** to return to the **Export** dialog.

Note: The **Compute Export Size** button is not active if a Release of Information (ROI) export format is selected. If only ROI is licensed, this button is not available when exporting through the ROI queue.

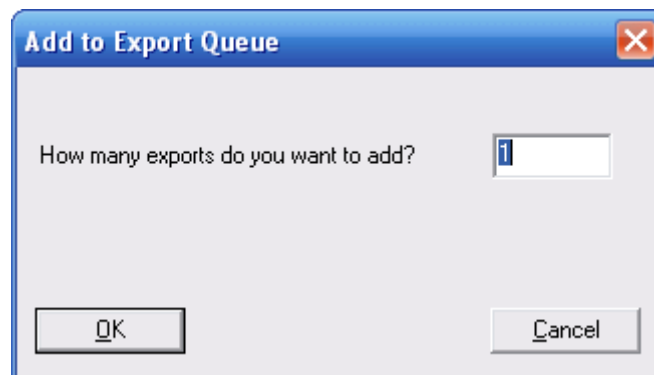
Adding a Platter to the Export Queue

The **Add to Export Queue** menu item is available for any Disk Group that is configured with an export copy. It generates an export copy and places it in the Export Queue. Otherwise, export copies are not placed in the Export Queue until a new Disk Group volume is created or the Disk Group is promoted.

1. In the Client module, select **Admin | Platter Management** to display the **Platter Management** window.
2. Select a Disk Group in the left pane to display its volumes.
3. Select a volume in the right pane and select **Add to Export Queue** from the right-click menu.

Note: If the Disk Group was not configured with an Export copy, the **Add to Export Queue** right-click option is not available. Contact your system administrator to verify the Disk Group settings.

4. The **Add to Export Queue** dialog box is displayed.



Enter the number of export copies to add to the Export Queue, then click **OK**. Click **Cancel** to exit the process without placing any data in the Export Queue.

Viewing Document Locations

Users that have the **Disk Group Configuration** configuration right are able to view hidden UNC paths.

To view a hidden UNC path:

1. Right-click on an open document or a document in a search results list and select **Properties**. The **Document Information** dialog is displayed.

Document Information for Document Handle:7513

Document Name : Employee I9 Form for ANDREW LINCOLN (Employee #102)

Batch Number : 267 Document Date: 2007-03-10 Date Stored : 2008-03-07

Time Stored: 5:06:11PM

Document Type Number : 113 DT Rev. : 1 Revision : 1

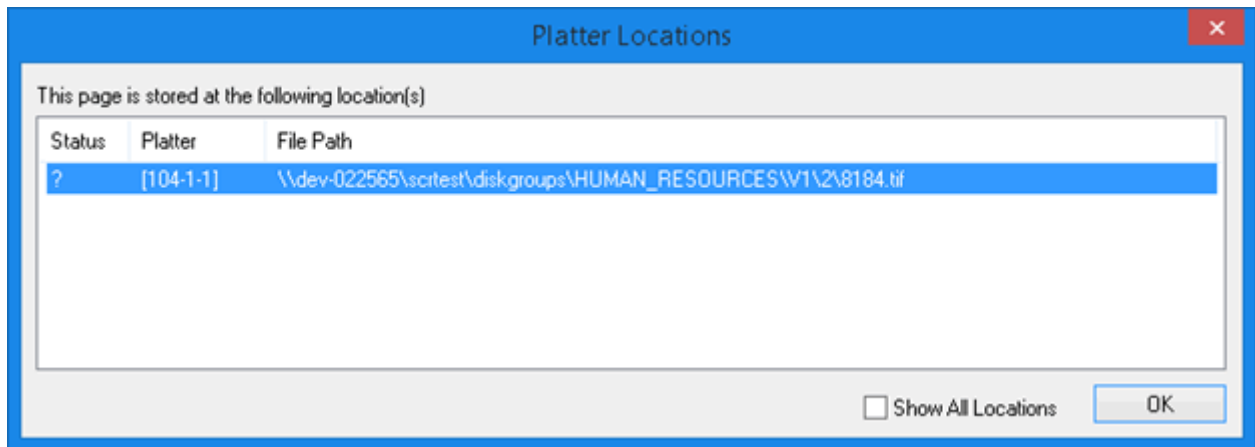
Document Type Name : HR - I-9 Form Document Status : 0

Author : Manager Security Value : 0

Page	Disk Group	Volume	Number of Pages	Number of Lines	File Format	Item Offset	Item Size	File Path
0	104	1	1	0	2	0	160940	\\V1\2\8184.tif

Locations Exit

2. Double-click on the file information item in the box or click once to highlight the information and click **Locations**. The **Platter Locations** dialog box is displayed.



Note: If the document is in the cache, a line that says **Cache** is displayed in this dialog box.

3. Right-click on the path and select **Verify File Is Online**. The **Status** column will update with the location of the file (e.g. **OK**, **NO**)
4. Right-click on the path and select **Show Hidden Shares**. The full path is displayed. To hide the full path to the document, right click on the full path and select **Obscure Hidden Shares**.
5. Right-click on the path and select **Open Containing Folder**. The physical folder where the document actually resides is displayed.
6. Right-click on the path and select **Save File Unaltered** to save the file locally on your system if desired. If the file is stored on an encrypted drive, this saves the file locally without encryption.

Note: You must have the **Copy To Clipboard/Save As** permission for every document type associated with documents that reference the file in order to use the **Save File Unaltered** option for encrypted files.

7. By default, the **Platter Locations** dialog will only show the locations where the document actually resides. Select **Show All Locations** to view locations where the document has been deleted, locations which are not yet created, or locations corresponding to committed copies of the file which are in batches and have not yet been committed.

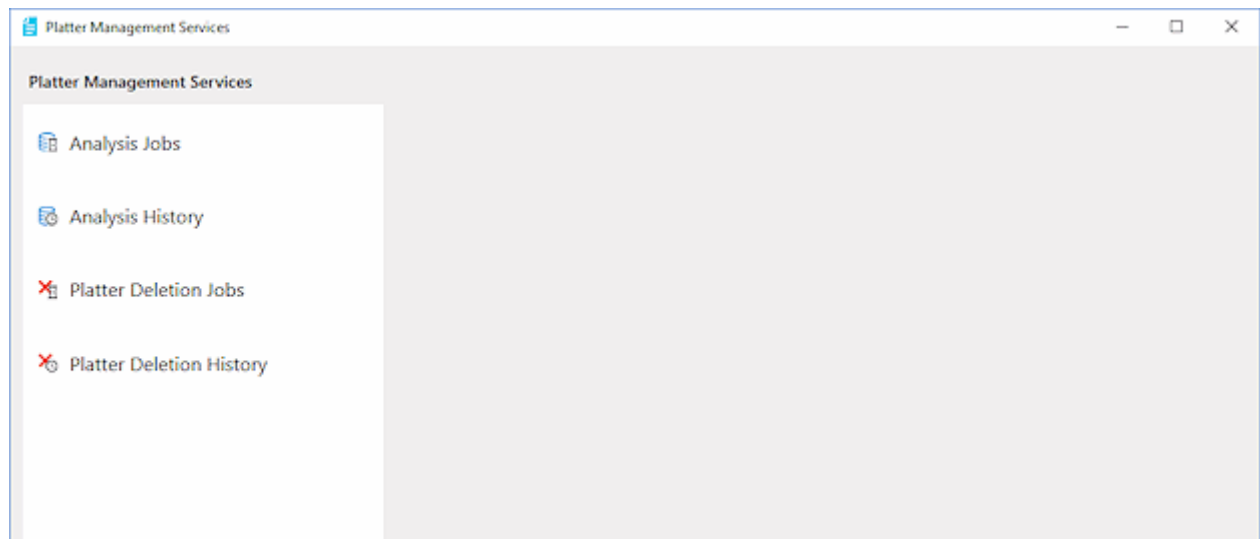
Caution: Documents should not be edited, moved, copied, deleted, or otherwise managed in the physical Disk Group folder without using the OnBase interfaces. Manipulating documents stored in OnBase without using the OnBase interfaces may cause them to become inaccessible to OnBase. The OnBase clients and Configuration module provide the ability to fully manage documents stored in OnBase, as well as providing additional security, disk management, and backup benefits.

Unity Scheduler Tasks for Platter Management

Several different types of platter management tasks are scheduled for execution using the Unity Scheduler. These tasks include analysis, incomplete commit queue processing, and incomplete delete queue processing, and platter deletion. For more information on creating tasks, see the Unity Scheduler module resource guide.

Disk Group Analysis Tasks

When an analysis job is queued in the **Client** or created by a **Rule** in **Config**, it will be added to the **Analysis Jobs** list in **Platter Management Administration**.



To execute all jobs currently available in **Platter Management Administration**, create a Disk Group Analysis Processing task in the Unity Scheduler. For more information on the Disk Group Analysis Processing task, see [Disk Group Analysis Processing on page 111](#).

Incomplete Commit Queue Processing Tasks

If the automatic commit fails upon an ad hoc (single document) import, the document is added to the Incomplete Commit Queue in **Client | Admin | Platter Management**. You can manually commit documents from this queue or they will be automatically committed once every 24 hours using **Incomplete Commit Queue Processing** task in the **Unity Scheduler**. This task is configured automatically when the **Unity Scheduler** is run. To learn more about this task, see [Incomplete Commit Queue Processing on page 115](#).

Incomplete Delete Queue Processing Tasks

If a scrub, delete, or purge action fails, the document, batch, or platter is added to the Incomplete Delete Queue in **Client | Admin | Platter Management**. You can manually retry or cancel any of the attempted deletions from this queue, or they will be automatically retried once every 24 hours using **Incomplete Delete Queue Processing** task in the **Unity Scheduler**. This task is configured automatically when the **Unity Scheduler** is run. For more information on this task, see [Incomplete Delete Queue Processing on page 162](#).

Platter Deletion Processing Tasks

Platter deletion is performed either by manually deleting the platter or through the use of platter deletion rules, which add the platter to the **Platter Deletion Jobs** queue in **Platter Management Administration**. Platters in this queue need to be manually approved for deletion. Once the deletion is approved, the platter remains in the queue until a Platter Deletion Processing task occurs. To delete all approved platters from the queue, create a Platter Deletion Processing task in the **Unity Scheduler**. For more information on configuring the Platter Deletion Processing task, see [Platter Deletion Processing on page 112](#).

Troubleshooting

Platter Management issues are reported in the Diagnostics Console. The File tab displays messages that correspond with the Web Server's attempts to access the Disk Groups and locate specific files. The Error Viewer tab reports more serious file access errors, such as the file server itself being inaccessible. The information in the File tab along with any errors displayed in the Error Viewer tab are required to troubleshoot and diagnose Platter Management issues.

See the Diagnostics Service reference guide for details on using the Diagnostics Console.

Disk Group Errors

Mount Disk

Issue: While trying to retrieve a document, the **Mount Disk** dialog is displayed, prompting the user to enter the path to the Disk Group containing the document to be retrieved. This means the Disk Group containing the document is currently offline or otherwise unavailable.

Resolution: A user with the **Platter Management** product right can enter the correct path to the Disk Group in the **Path to disk** field, or click **Browse** to locate it. If the user does not have the **Platter Management** product right to enter the path, or the Disk Group is offline or otherwise unavailable, the **Mount Disk** dialog also displays pertinent information regarding the Disk Group that cannot be mounted. Copy down this information and forward it to your system administrator for resolution.

Note: The Mount Disk error may be displayed in instances other than during document retrieval. This error occurs when the OnBase.ID file is not found in any copy. When contacting your system administrator, explain the scenario in which you encountered the error.

Platter Management Error

Issue: While trying to archive or import documents, the **Platter Management Error** dialog is displayed. This means the Disk Group that is used to store the type of document being archived is currently offline or otherwise unavailable.

Resolution: The **Platter Management Error** dialog displays pertinent information regarding the Disk Group that cannot be accessed. Copy down this information and forward it to your system administrator for resolution.

Note: The Platter Management Error may be displayed in instances other than during document retrieval or import. When contacting your system administrator, explain the scenario in which you encountered the error.

Disk Group Analysis

Issue: When processing a job with Disk Group Analysis, a job becomes stuck in the **In Progress** queue.

Resolution: The right-click menu within the **Disk Group Analysis** window contains an option for restarting the job. Right-click the volume in question and select **Restart**. Before using this option, ensure that no other analysis service is actively using the job in question.

Unable to Make File Read-Only

Issue: While trying to import documents, a **Critical Platter Management Error** is encountered. The message of the error is: **Unable to Make File Read-Only**. This error is followed by an **Index Error** that reads: **Error copying to file <file name> Index of file aborted**.

Resolution: These errors are encountered if a Disk Group copy is located on a proprietary storage device, but your database is not licensed for that storage device. To resolve this issue, make sure your database is properly licensed for the storage devices that contains your Disk Groups.

PLATTER MANAGEMENT BEST PRACTICES

The following best practice recommendations were assembled by a team of OnBase subject matter experts. They represent the accumulation of years of experience installing and configuring OnBase solutions.

The following recommendations are general in nature, and are applicable to most OnBase solutions and network environments. Depending on your solution design and your organization's needs, not all of the best practice recommendations listed below may apply to, or be recommended for, your OnBase solution.

Carefully consider the impact of making any changes, including those listed below, to your OnBase solution prior to implementing them in a production environment.

Usage

Copying Missing Files

If you run **Analyze Source** and missing files are detected you have the option to copy the missing files from a backup location. It is a best practice to select **Use Temp Path** when copying missing files. This option creates a buffer location to temporarily store the files that are being copied. This can speed up the process when copying to or from a slower media, such as a tape or CD backup.

Deleting Platters from the Disk Group

Once a copy is deleted it cannot be recovered. If there is only one copy of a platter it should not be deleted, as the documents in that copy are no longer available after deletion.

To produce a log of the files deleted, select the **Enable generation of deleted file reports** option on the **Platter Management** tab of the **Global Client Settings** in the OnBase Configuration module. This report contains the full paths to all copies of all files deleted from the Disk Groups and is stored in OnBase as **Deleted Files** under the **SYS - Platter Management Reports** Document Type. See the Configuration help files for details on selecting this option.

Exporting Platters to Disc

When exporting data to disc, you can select **Compute Export Size** to estimate the number of discs required for the selected Export, before it is produced. After the process is run, the **Estimated Export Requirements** dialog box is displayed. This dialog provides information about the estimated number of discs required for the exported data and the space used on each disc.

Document Retention and Records Management

Creating discs for backup purposes is an economical way to replicate data and physical files for disaster recovery purposes. However, if your organization has strict document retention or records management regulations that must be met, backup discs can quickly become difficult to maintain once those rules have to be applied.

It is a best practice to only use discs for the backup of volumes or Disk Groups that contain documents that are not governed by document retention or records management rules. If documents are part of a retention plan, the Disk Groups should only be configured with **Mass Storage** copy types.

Configuration

Disk Groups

It is a best practice to create separate hidden shares for each Disk Group.

Separate Disk Group locations should be created for test data during the installation or expansion of modules. This allows test data to be kept separate from production data, making the migration to production and cleanup afterwards easier.

Note: Documents should not be edited, moved, copied, deleted, or otherwise managed in the physical Disk Group folder without using the OnBase interfaces. The OnBase clients and Configuration module provide the ability to fully manage documents stored in OnBase, as well as providing additional security, disk management, and backup benefits.

Security

In order for users to be able to access the Disk Groups from OnBase, the Disk Group folders must be set with certain share/NTFS permissions, depending on a user's level of access. It is a best practice to give users or User Groups the minimum level of access required to perform the OnBase functions expected of them. In this way, if a user is able to access the Disk Group folders outside of OnBase, that user may be prevented from manually performing actions not granted in OnBase, such as editing documents.

Since security rights and permissions are unique to each operating system, make sure you are assigning the appropriate security rights to each copy of the Disk Groups you create.

Folders that contain higher security Disk Groups should not be not placed in lower security shares.

Ensure that network **Create** rights exist for all copy locations because all Core Services modules and file imports perform an immediate commit to all secondary and removable copies in the Disk Group.

Note: Refer to the **Encrypted Disk Groups** or **Distributed Disk Services** documentation for information on how to better secure files accessed outside of OnBase.

Disk Group Settings

Volume Size

It is critical that the absolute limit of the selected media is not used for the volume size. This is because space is also required on the media for the file allocation table, not just the data. If the media has a set block size, multiple small files could actually take up more space than expected, which could cause issues when going from one block size media to another. Scanning also poses special considerations when computing volume size, since scanning always finishes a batch in whatever volume it started, regardless of the volume size.

Refer to [Computing Volume Size and Splitting Volumes on page 124](#) for additional information.

Backup Copies

When creating your Disk Group copies, it is often helpful to create your backup copies last so that they are listed in the configuration dialogs as a group after all of the other copies.

It is also a best practice to create at least one of the three different types of copies for each Disk Group that you create (**Removable**, **Backup**, and **Externally Filled**).

The data contained on any volume or platter in a Disk Group can be copied at any time during the collection of data, unlike the **Write** function, which is only available in the **Backup Queue**. However, the **Copy** function is not intended as a permanent method of archiving data. Copying requires independent tracking of the data contained in a volume, especially when determining when a platter is at its maximum capacity and must be copied prior to its deletion. For this reason, creating a Disk Group with a backup copy and utilizing the **Write** function to make off-line backups is recommended.

Maximum Number of Volumes

It is a best practice to set your maximum number of volumes to be one less than the actual maximum number of volumes your Mass Storage media can hold. For example, if the Mass Storage drive can hold four gigabytes of data and you have configured your volume size to be 500,000 kilobytes, you could fit 8 volumes on the mass storage media. However, it is a best practice to configure the maximum number of volumes to be 7.

The reason for this is that if you process documents into your system using any batch processing then it is possible that a volume will need to be promoted in the middle of a job. If this occurs, the system promotes the last volume and completes the job on the next volume. If you set the maximum number of volumes to be the actual maximum, this means you will end up with one more volume online than your desired maximum number of volumes, and potentially more data than the media can hold. Also, after this job is completed, you cannot add more documents to the Disk Group until the oldest volume is deleted.

Volume Paths

The paths for each volume should be configured before the volume is created. You can enter the paths to each new volume for a copy by selecting the **Activate Platter Paths** box. By default, this option is selected when the copy is of the **Removable Media** type. Click **Platter Paths** to open the Platter Paths dialog box and enter the paths for each new volume.

Backfile Conversions

If documents are being added to the system via a backfile conversion process, those documents should be stored in separate Disk Groups from new documents. Archiving new and backfile documents together could adversely affect resource planning and inhibit the correct allocation of resources.

E-Forms Disk Groups

E-Forms should be placed in their own, unique Disk Groups. Since E-Forms in the OnBase Client can require a brief locking period during updates, automated processing and other prolonged locking functions could negatively impact the performance of E-Forms if they are using the same Disk Groups. The brief locking period does not occur in the Unity or Web Clients.

Upgrade Considerations

The following upgrade considerations have been compiled by OnBase subject matter experts. These upgrade considerations are general and applicable to most OnBase solutions and network environments and should be considered each time an upgrade is performed.

Carefully consider the impact of making any changes, including those listed below, prior to implementing them in a production environment.

For additional general information about upgrading OnBase, refer to the Upgrade Guidelines reference manual, and visit the Hyland Community at:
<https://www.hyland.com/community>.

Platter Management Upgrade Considerations

The following information should be considered or noted when upgrading Platter Management deployments. Read this information prior to upgrading your version of OnBase.

General Deployment Considerations — In addition to the previous considerations, the following should be considered with regard to general deployments:

- When upgrading Platter Management systems using incremental, parallel upgrades, be aware that many Platter Management-related components require specific software versions and builds to match and can become unusable if there is a mismatch.

KOMpliance Considerations — KOMpliance servers are no longer supported for use with OnBase as of Foundation EP1.

The following information should be considered or noted when upgrading Encrypted Disk Groups deployments. Read this information prior to upgrading your version of OnBase.

Encrypted Disk Groups Deployment Considerations — In addition to the previous considerations, the following should be considered with regard to Encrypted Disk Groups deployments:

- If changes are made to Encrypted Disk Groups during an upgrade, new encryption keys can be generated and the way encryption is handled may have been updated by the new version of the client. Due to this, after upgrading any discrepancy in encryption between the clients or the application server, or the older version of the client having older encryption keys, may cause the older version of the client to be unable to access encrypted data.

The following information should be considered or noted when upgrading Storage Integration deployments. Read this information prior to upgrading your version of OnBase.

Storage Integration Deployment Considerations — In addition to the previous considerations, the following should be considered with regard to Storage Integrations deployments:

- When upgrading OnBase or a storage integration component, for instance, Storage Integration for EMC Centera, or Storage Integration for IBM Tivoli, ensure that each component is compatible with all others.

The following information should be considered or noted when upgrading Centera integration. Read this information prior to upgrading your version of OnBase.

Centera Integration Considerations — In addition to the previous considerations, the following should be considered with regard to Centera integration:

- When upgrading OnBase from a version prior to 11, the Client needs to be upgraded as well to properly function with Centera integration.