Copyright © 1993 – 2009 EMC Corporation. All rights reserved.

Published March, 2009

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS IS.” EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date regulatory document for your product line, go to the Technical Documentation and Advisories section on EMC Powerlink.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com.

All other trademarks used herein are the property of their respective owners.
Preface

Chapter 1 The DiskXtender Advantage
Seamless extension of disk space ................................................................. 16
  Full NTFS compatibility ........................................................................... 16
  Native Windows network connectivity and security .................................. 17
  Automated file management ................................................................... 18
  Flexible support for back end storage ..................................................... 19
  Hardware scalability ................................................................................ 19
  Automated media management .............................................................. 20
  Offline media support ............................................................................ 20

Chapter 2 Architecture and Requirements
  DiskXtender architecture ................................................................. 22
  DiskXtender components ...................................................................... 24
    User machines .................................................................................... 24
    File System Manager .......................................................................... 24
    Media services .................................................................................. 25
    License Server ................................................................................ 28
    DiskXtender Search Module ........................................................... 29
  System requirements .......................................................................... 30
  Security requirements ........................................................................ 31

Chapter 3 File Management
  Supported file types .......................................................................... 36
    International character support .................................................... 37
    Path and filename length limitations ............................................ 37
    File stream support .......................................................................... 38
    Encryption ........................................................................................ 38
    Microsoft Windows offline files ................................................. 38
    Microsoft Windows DFS links .................................................. 39
  Migrating files to media ................................................................. 40
    File migration models ................................................................. 40
    Customizing file migration ......................................................... 42
  Purging files .................................................................................... 44
    Purge rules .................................................................................... 45
    Purging files as disk space is needed ........................................... 45
Chapter 4  Media Management

EMC Centera ........................................................................................................ 56
Virtual media ......................................................................................................... 57
Content-addressable storage ............................................................................... 58
Compliance through retention and audit .............................................................. 62
Replication ............................................................................................................ 63
Network-attached storage ..................................................................................... 67
Standard NAS ....................................................................................................... 67
Aggregate NAS ..................................................................................................... 67
Retained NAS ....................................................................................................... 68
Limitations for filepath lengths ........................................................................... 69
Creating the shares for NAS media ..................................................................... 70
Removable media .................................................................................................. 73
MediaStor .............................................................................................................. 73
Sun StorageTek ACSLS ........................................................................................ 75
Managing the removable media lifecycle ............................................................ 77
Tivoli Storage Manager .......................................................................................... 81

Chapter 5  Monitoring DiskXtender

Monitoring service events, errors, and warnings .................................................. 84
Monitoring file activity .......................................................................................... 84
Monitoring media .................................................................................................. 85
Media status indicators ......................................................................................... 85
Media task queue .................................................................................................. 85
Media logs ............................................................................................................. 85
Media properties ................................................................................................... 85
Monitoring licensing ............................................................................................. 86
Reports ................................................................................................................... 86
Audit logs ............................................................................................................... 87
Remote administration .......................................................................................... 87

Chapter 6  Backup and Recovery

Developing a backup strategy ................................................................................. 90
Backing up the extended drive ............................................................................. 92
Ensuring storage redundancy ............................................................................... 93
Copying removable media .................................................................................... 93
Replicating EMC Centera ...................................................................................... 93
Contents

- Backing up NAS ................................................................. 93
- Backing up TSM ................................................................. 94
- Backing up the DiskXtender server ........................................ 95
- Protecting against accidental file deletion .............................. 96

Chapter 7   Interoperability

- DiskXtender as an application back end .................................. 98
  - Documentum ApplicationXtender ......................................... 98
  - Custom integration through the DiskXtender SDK .................... 98
- High availability ................................................................. 99
  - AutoStart ........................................................................ 99
  - PowerPath ....................................................................... 99
- Replication ........................................................................... 101
- Anti-virus software interoperability .......................................... 102
- DiskXtender on VMware .......................................................... 102
  - Clustering DiskXtender on VMware .................................... 102
  - VMotion support ............................................................. 103

Index
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 DiskXtender architecture</td>
<td>22</td>
</tr>
<tr>
<td>2 File System Manager Administrator</td>
<td>25</td>
</tr>
<tr>
<td>3 MediaStor Administrator</td>
<td>27</td>
</tr>
<tr>
<td>4 Standard migration</td>
<td>40</td>
</tr>
<tr>
<td>5 Multi-target migration</td>
<td>40</td>
</tr>
<tr>
<td>6 Tiered migration</td>
<td>41</td>
</tr>
<tr>
<td>7 EMC Centera C-Clip for a DiskXtender file</td>
<td>58</td>
</tr>
<tr>
<td>8 Embedded BLOB for a file stored on EMC Centera</td>
<td>60</td>
</tr>
<tr>
<td>9 Separate CDF and BLOB for a file stored on EMC Centera</td>
<td>60</td>
</tr>
<tr>
<td>10 Tiered migration</td>
<td>68</td>
</tr>
<tr>
<td>11 DiskXtender with NAS</td>
<td>71</td>
</tr>
<tr>
<td>12 File System Manager with MediaStor</td>
<td>74</td>
</tr>
<tr>
<td>13 DiskXtender with ACSLS</td>
<td>76</td>
</tr>
<tr>
<td>14 DiskXtender with Tivoli Storage Manager</td>
<td>81</td>
</tr>
<tr>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Supported removable media types</td>
<td>19</td>
</tr>
<tr>
<td>Supported media services</td>
<td>26</td>
</tr>
<tr>
<td>Minimum and Recommended Hardware Requirements for DiskXtender</td>
<td>30</td>
</tr>
<tr>
<td>DiskXtender user groups</td>
<td>32</td>
</tr>
<tr>
<td>Product interoperability and foreign-language character support</td>
<td>37</td>
</tr>
<tr>
<td>Icons for files on the extended drive</td>
<td>44</td>
</tr>
<tr>
<td>File edit and rename capabilities by media type</td>
<td>48</td>
</tr>
<tr>
<td>File delete capabilities by media type</td>
<td>49</td>
</tr>
<tr>
<td>Types of retention</td>
<td>62</td>
</tr>
<tr>
<td>NAS media types</td>
<td>67</td>
</tr>
<tr>
<td>Supported removable media types</td>
<td>73</td>
</tr>
<tr>
<td>File system support by media type</td>
<td>79</td>
</tr>
<tr>
<td>Subsystems for the OTG file system</td>
<td>79</td>
</tr>
<tr>
<td>UDF file systems</td>
<td>80</td>
</tr>
<tr>
<td>Toolbar icons for events, warnings, and errors</td>
<td>84</td>
</tr>
<tr>
<td>Media status indicated by color</td>
<td>85</td>
</tr>
<tr>
<td>Reports</td>
<td>86</td>
</tr>
<tr>
<td>Recommended media protection methods</td>
<td>91</td>
</tr>
</tbody>
</table>
As part of an effort to improve and enhance the performance and capabilities of its product lines, EMC periodically releases revisions of its hardware and software. Therefore, some functions described in this document may not be supported by all versions of the software or hardware currently in use. For the most up-to-date information on product features, refer to your product release notes.

If a product does not function properly or does not function as described in this document, please contact your EMC representative.

Audience
This Technical Product Overview is intended for technical staff and managers, including:

◆ IT managers and IT staff
◆ Development managers
◆ Engineers
◆ System administrators

Readers of this document are expected to be familiar with the following topics:

◆ Microsoft Windows network administration
◆ Storage media and hardware device management

Related documentation
Related documents include:

◆ EMC DiskXtender Microsoft Windows Version Release 6.4 Administration Guide
◆ EMC DiskXtender Microsoft Windows Version Release 6.4 Release Notes
◆ EMC DiskXtender Search Module Release 1.1 Installation Guide
◆ EMC DiskXtender Search Module Release 1.2 Release Notes

Conventions used in this document
EMC uses the following conventions for special notices.

Note: A note presents information that is important, but not hazard-related.

CAUTION
A caution contains information essential to avoid data loss or damage to the system or equipment.
IMPORTANT
An important notice contains information essential to operation of the software.

Typographical conventions
EMC uses the following type style conventions in this document:

Normal Used in running (nonprocedural) text for:
- Names of interface elements (such as names of windows, dialog boxes, buttons, fields, and menus)
- Names of resources, attributes, pools, Boolean expressions, buttons, DQL statements, keywords, clauses, environment variables, filenames, functions, utilities
- URLs, pathnames, filenames, directory names, computer names, links, groups, service keys, file systems, notifications

Bold: Used in running (nonprocedural) text for:
- Names of commands, daemons, options, programs, processes, services, applications, utilities, kernels, notifications, system call, man pages

Used in procedures for:
- Names of interface elements (such as names of windows, dialog boxes, buttons, fields, and menus)
- What user specifically selects, clicks, presses, or types

Italic: Used in all text (including procedures) for:
- Full titles of publications referenced in text
- Emphasis (for example a new term)
- Variables

Courier: Used for:
- System output, such as an error message or script
- URLs, complete paths, filenames, prompts, and syntax when shown outside of running text

Courier bold: Used for:
- Specific user input (such as commands)

Courier italic: Used in procedures for:
- Variables on command line
- User input variables

< > Angle brackets enclose parameter or variable values supplied by the user
[] Square brackets enclose optional values
| Vertical bar indicates alternate selections - the bar means “or”
{} Braces indicate content that you must specify (that is, x or y or z)
... Ellipses indicate nonessential information omitted from the example

Where to get help
EMC support, product, and licensing information can be obtained as follows.

Product information — For documentation, release notes, software updates, or for information about EMC products, licensing, and service, go to the EMC Powerlink website (registration required) at:

http://Powerlink.EMC.com

Technical support — For technical support, go to EMC Customer Service on Powerlink. To open a service request through Powerlink, you must have a valid support agreement. Please contact your EMC sales representative for details about obtaining a valid support agreement or to answer any questions about your account.
Your comments  Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Please send your opinion of this document to:

SSGdocumentation@EMC.com
The following topics provide an introduction to and describe the benefits of EMC DiskXtender for Windows:

- Seamless extension of disk space ................................................................. 16
- Automated file management ......................................................................... 18
- Flexible support for back end storage .......................................................... 19
Seamless extension of disk space

EMC® DiskXtender® for Windows is so named because it extends the amount of space on a server’s local New Technology File System (NTFS) volume, or hard drive partition. This can either be a volume physically located on the DiskXtender server or a fibre-connected drive that has been mapped as a local drive.

DiskXtender extends the amount of space on a drive by migrating files from the drive to external storage media, while maintaining the appearance that the files are still on the drive. A drive that has been extended through DiskXtender is called an extended drive.

The management of files on the extended drive through DiskXtender is actually a two-part process. Those two parts are referred to as a move and a purge and can be performed separately or simultaneously.

In DiskXtender, a move is actually a copy. When DiskXtender moves a file to media, it is really copying the file data out to media and adding extended attribute information to the file on the drive. The file is then managed by DiskXtender, and the data resides both on the extended drive and on the media.

After file data is moved to storage media, that data can be removed, or purged, from the extended drive, which frees that space for additional files. The purging of a file removes the file data from the drive, and leaves behind a file tag on the drive. The data then resides only on the media.

The file tag serves two purposes:

- It allows the file to appear as if it still resides on the drive so that users can easily find it.
- It contains the extended file attribute information that DiskXtender needs to manage and retrieve the file from media.

To a user who retrieves files from a drive extended by DiskXtender, all files appear to be present, regardless of whether the file data is on the drive or only on storage media. When the user requests the files, DiskXtender accesses the media where the files are stored and retrieves the file data, and displays it for the user. This file retrieval process is called a fetch.

Full NTFS compatibility

Since DiskXtender uses the NTFS file system as the gateway to its remote storage management functions, all native features of NTFS are supported, including support for:

- Long filenames (up to 259 characters)
- Filenames with Unicode characters
- Folder and file-level security
- Offline files

Regardless of the media type that is being used for remote storage, full security can be applied to any file or folder on an extended drive, even if the storage media itself does not support Microsoft Windows security (for example, magneto-optical WORM or tape).
Native Windows network connectivity and security

DiskXtender does not interfere with Windows networking. Users that access an extended drive, usually through network shares, can connect by using any installed transports and protocols.

DiskXtender does not interfere with Windows security either. Users that access an extended drive are authenticated through native Windows security. The operating system manages security at all levels.
Automated file management

DiskXtender automates the migration of files to media by using a rule-based system. Rather than just migrate all files to media without distinction between the files, you can select which files should be moved to what types and pieces of media, and when those files are moved.

After file data is moved to storage media, automatic file purge options can remove the file data from the drive, and leave behind a file tag so that the file can be retrieved when necessary.

File purging can occur:

- Immediately for all files, as soon as they are moved to media
- When extended drive disk space is needed
- When the files meet other criteria, such as a certain age

If necessary, you can protect migrated files from being edited or deleted during a specified time period. This protection is called file retention, and is required in some environments to comply with government and organizational regulations. Retention is available if you are migrating files from DiskXtender to one of the following devices:

- EMC Centera®
- EMC Celerra® with the File-Level Retention (FLR) file system
- Network Appliance (NetApp) NAS device with SnapLock software

When you apply retention, the files are protected both on the extended drive and on the storage hardware device.

In some instances, you may also want to delete files completely when they are no longer of use. You can either delete files manually (for example, through Windows Explorer), or you can delete files automatically through DiskXtender by using rule-based criteria.

When you delete a file from the extended drive, the file is also deleted from any associated storage media, if the media allows it.
Flexible support for back end storage

DiskXtender supports many high-capacity storage media types, including several removable media and disk-based storage options.

Table 1 on page 19 provides details on the supported removable media types.

<table>
<thead>
<tr>
<th>Media type</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tape and tape-WORM</td>
<td>LTO, SDLT, DLT, SAIT, AIT, 9840, and 9940</td>
</tr>
<tr>
<td>DVD</td>
<td>DVD-R, DVD-RAM, and DVD-ROM</td>
</tr>
<tr>
<td>Optical and optical WORM</td>
<td>Magneto-optical, Ultra Density Optical</td>
</tr>
</tbody>
</table>

These media types are supported through a wide variety of hardware devices. For a complete list, refer to the DiskXtender for Windows Supported Device List, available on the EMC Powerlink® website.

Disk-based storage options include EMC CLARiiON®, and Celerra, as well as many other Redundant Array of Independent Disks (RAIDs) and network-attached storage (NAS) devices. Essentially, a server with a network share that is available to DiskXtender can be used as storage media. DiskXtender considers all of these shared devices to be NAS media.

DiskXtender also supports the use of an EMC Centera content-addressed storage (CAS) system, the first magnetic disk-based WORM device. DiskXtender and EMC Centera are tightly integrated to optimize file storage and retrieval performance. Several DiskXtender file migration and retention features are designed specifically to take advantage of the features available with an EMC Centera device.

DiskXtender transparently manages data movement between the extended drive and the storage media. Communication with the hardware devices that contain the storage media is established through the creation of DiskXtender media services. DiskXtender transfers files to the media provided by the media services, and sends requests for pieces of media to the media services as needed.

DiskXtender manages all functions related to the transfer of information to and from media, such as the migration and retrieval of files. The only role a media service plays is to provide access to the media so that DiskXtender can work with it. For a media service that provides access to removable media, this means that the service places the requested media into a drive or prompts the administrator of the media service to insert the appropriate piece of media. For a media service that provides access to disk-based devices, this means that the service provides access to a place where the data is written.

You can use any or all of these media types with a single DiskXtender installation.

With DiskXtender, hardware can grow with your storage needs, and you do not need to reconfigure or reformat the extended drives. DiskXtender interfaces with the software that manages the storage devices. The devices are completely independent of the extended drives they support, even though DiskXtender controls the media in those devices. If you are using removable media, you can change hardware and relocate media without affecting the files on your extended drive or the ability of DiskXtender to find files on the storage media.
DiskXtender Advantage

DiskXtender stores an internal inventory of all online and offline media in the system. This inventory system means that removable media is not dedicated to a specific hardware device. When hardware configuration or removable media locations change, the internal inventory is automatically updated so that DiskXtender always knows where media is located.

When file migration or retrieval is required, DiskXtender uses its internal inventory to automatically find the proper media for the requested file.

Automated media management

DiskXtender can automatically prepare media for file migration when it is needed, as well as reclaim space that is no longer used on some media types.

If you are using removable media, DiskXtender can automatically format, label, and assign media for file migration from a group of blank media. You can also reclaim space on removable media by compacting it when wasted space exceeds a certain percentage. When you compact a piece of media, active files on the media (current versions of written files and files not marked for deletion) are written back to the extended drive and are remigrated to another piece of eligible media. You can then reformat the compacted media so that it can be used again. Compaction optimizes media usage even if file deletions are frequent.

If you are using an EMC Centera device, DiskXtender can automatically create the "virtual" media that DiskXtender uses to simulate divisions of an EMC Centera cluster. The use of virtual media enables you to take advantage of the flexible file migration features available in DiskXtender.

If you are using DVD-R media, DiskXtender can automatically finalize the media when it is full. Finalization closes the media, which prevents the writing of any more files to the media. Finalization also increases the stability of the media so that data is better protected.

Offline media support

Offline media support is very important for large systems with limited hardware resources and large storage requirements. DiskXtender fully supports offline media. With DiskXtender, media can be online or offline. When online, users can access any file on the media. If media is taken offline and a file is requested that is not on the extended drive, the user receives an error message and the DiskXtender system administrator is notified that the requested media must be mounted.

One important benefit of DiskXtender offline media support is that the files on your extended drive are not affected by the state of the media. Unlike other products, where files disappear when media is taken offline, DiskXtender maintains file and folder information whether the media is online or offline. This enables you to take hardware devices offline for maintenance without concerns about whether DiskXtender will be able to find the files or media when the device is set online again. Users and applications can always see their files on an extended drive.

In addition, if you know in advance what media will be offline for a period of time, you can copy certain files from the media back to the extended drive. This prefetch feature ensures that files are available for user requests even when media is offline.
The following topics introduce the DiskXtender architecture and provide the minimum system requirements for installing and using DiskXtender:

- DiskXtender architecture ................................................................. 22
- DiskXtender components ................................................................. 24
- System requirements ....................................................................... 30
- Security requirements ..................................................................... 31
DiskXtender architecture

Figure 1 on page 22 illustrates the basic components of a DiskXtender for Windows system, which can be set up on several computers to avoid the bottleneck of an architecture with a single server and multiple clients.

Users save files to and retrieve files from one or more DiskXtender extended drives. The extended drives are NTFS volumes on a Microsoft Windows server. The DiskXtender File System Manager component, which is the main component of the DiskXtender system, is installed on the server.
File System Manager monitors activity on the extended NTFS volumes, and manages all functions related to the transfer of information to and from media, such as the migration and retrieval of files. Communication with the hardware devices that contain the storage media is established through the creation of DiskXtender media services. DiskXtender transfers files to the media provided by the media services, and sends requests for pieces of media to the media services as needed. The only role a media service plays is to provide access to the media so that DiskXtender can work with it.
DiskXtender components

The DiskXtender architecture consists of the following components:

- “User machines” on page 24
- “File System Manager” on page 24
- “Media services” on page 25
- “License Server” on page 28
- “DiskXtender Search Module” on page 29

User machines

All users that can connect to an NTFS volume can store and access files on a DiskXtender extended drive.

DiskXtender can manage files written to the extended drive from user machines that use NTFS or File Allocation Table (FAT) because both are Microsoft Windows native file systems. DiskXtender also supports streamed files from user machines that use a network file system (NFS), such as a UNIX/Linux file system.

File System Manager

DiskXtender File System Manager is the data mover for the DiskXtender product suite. File System Manager moves files from the extended drive to storage media, and retrieves files when they are requested.

The File System Manager program is installed on the server connected to or containing the NTFS volumes to be extended. This server is considered the DiskXtender server. When you install File System Manager, the DiskXtender service, the File System Manager Administrator interface, and a filter driver are installed.

Service

DiskXtender functions as a Windows service rather than as a user-mode application. As a Windows service, DiskXtender can continue to be active even after you log out of Windows, as long as the computer is still running.

Administrator interface

Configuration of file migration, purging, deletion, indexing, and other system options is performed by using the File System Manager Administrator interface, which is illustrated in Figure 2 on page 25.
Filter driver

The DiskXtender filter driver keeps track of all files created, requested, edited, deleted, and indexed on the extended drive. This driver ensures that all the qualified files are moved to storage media, purged, fetched, deleted, and indexed when appropriate.

When a file on the extended drive is saved or changed, the filter driver analyzes the file to determine if action must be taken.

The filter driver analyzes all files, including those not managed by DiskXtender. If there are frequently changing files (such as email files) on the extended drive, the filter driver must monitor those files. This can cause a reduction in system performance. As a result, the extended drive should be reserved for files that should be managed by DiskXtender.

Media services

Communication with the hardware devices that contain the storage media is established through the creation of DiskXtender media services. DiskXtender transfers files to the media provided by the media services, and sends requests for pieces of media to the media services as needed.

DiskXtender manages all functions related to the transfer of information to and from media, such as the migration and retrieval of files. The only role a media service plays is to provide access to the media so that DiskXtender can work with it.

For a media service that provides access to removable media, this means that the service places the requested media into a drive or prompts the administrator of the media service to insert the appropriate piece of media.

For a media service that provides access to disk-based devices, this means that the service provides access to a place where the data is written.
Table 2 on page 26 describes the media services that are supported by DiskXtender, as well as the media types supported by the media service.

### Table 2: Supported media services

<table>
<thead>
<tr>
<th>Media service</th>
<th>Abbreviated name</th>
<th>Media types supported through the media services</th>
</tr>
</thead>
</table>
| DiskXtender MediaStor | MediaStor | • Magneto-optical (MO)  
• Ultra Density Optical (UDO)  
• MO WORM  
• UDO WORM  
• Tape  
• Tape-WORM  
• DVD-R  
• DVD-RAM  
• DVD-ROM |
| EMC Centera | EMC Centera | “Virtual” media defined in DiskXtender to simulate divisions of the EMC Centera cluster |
| Network-attached storage | NAS | “Virtual” media defined in DiskXtender that correspond to shares on a NAS device |
| IBM Tivoli Storage Manager | TSM | “Virtual” media defined in DiskXtender to simulate divisions of the disk on the TSM server |
| Sun StorageTek Automated Cartridge System Library Software (ACSLS) | ACSLS | Tape and tape-WORM |

**MediaStor**

DiskXtender MediaStor™ is a media service program that is provided automatically with the DiskXtender product suite. MediaStor provides comprehensive drive and library management capabilities for retrieving, mounting, and dismounting removable media in a variety of hardware devices.

MediaStor functions as a Microsoft Windows service and can be configured through an Administrator interface, as illustrated in Figure 3 on page 27.
EMC Centera

The EMC Centera media service provides access to an EMC Centera content-addressed storage (CAS) system, the first magnetic disk-based WORM device.

When you configure an EMC Centera media service in DiskXtender, you create a connection between DiskXtender and the access nodes of an EMC Centera cluster. EMC Centera media in DiskXtender is considered virtual, meaning that a piece of media in DiskXtender does not correspond to a physical piece of media, such as a tape cartridge. Instead, the virtual media is designed to simulate divisions of an EMC Centera cluster. Creation of EMC Centera media in DiskXtender enables you to take advantage of the flexible file migration features available in DiskXtender.

DiskXtender and EMC Centera are tightly integrated to optimize file storage and retrieval performance. Several DiskXtender file migration and retention features are designed specifically to take advantage of the features available with an EMC Centera device. “EMC Centera” on page 56 provides additional details.

Network-attached storage

NAS media in DiskXtender are network shares on disk-based storage devices. These shares can be located on a server hard drive or on any network appliance that provides share-level access to storage, such as a CLARiiON or Celerra device.

Each DiskXtender installation can have only one NAS media service. However, you can create as many pieces of NAS media for that media service as you want, and each piece of media can write to a different share on a different device.

“Network-attached storage” on page 67 provides additional details on the use of NAS with DiskXtender.
IBM Tivoli Storage Manager

If you are using TSM, you can leverage the storage management capabilities of TSM with DiskXtender. When you configure a TSM media service in DiskXtender, files on the extended drive can be moved to a TSM server. TSM can subsequently move the files to storage devices that are managed by the TSM server.

TSM media in DiskXtender is considered virtual, meaning that a piece of media in DiskXtender does not correspond to a physical piece of media in the TSM system, such as a tape cartridge. Instead, the virtual media is designed to simulate divisions of the larger repository (the TSM server). Creation of TSM media in DiskXtender enables you to take advantage of the flexible file migration features available in DiskXtender.

The TSM server manages the actual physical removable media, so that tasks like formatting, labeling, and copying media are performed by TSM rather than by DiskXtender.

“Tivoli Storage Manager” on page 81 provides additional details on the use of TSM with DiskXtender.

Details on the supported versions of the TSM server and client products are listed in the EMC Information Protection Software Compatibility Guide available on the Powerlink website.

Sun StorageTek ACSLS

If you have already invested in ACSLS, you can use DiskXtender to migrate files from a Microsoft Windows server to tape media in libraries managed by the ACSLS server. ACSLS is a UNIX-based device management product that manages Sun StorageTek tape libraries and provides device-sharing capability between applications.

A SCSI cable connects the DiskXtender server and one or more drives in the Sun StorageTek library. When you configure an ACSLS media service in DiskXtender, you designate the connected drives as the drives that should be used by DiskXtender. Other servers cannot access that drive.

Certain pieces of media in the ACSLS system are assigned to DiskXtender by using ACSLS.

When DiskXtender requires a particular piece of media, DiskXtender requests that media from ACSLS. ACSLS retrieves the media and places it in the drive connected to the DiskXtender server. DiskXtender then communicates directly with the drive, and initiates all media-related tasks without any involvement from ACSLS.

“Sun StorageTek ACSLS” on page 75 provides additional details on the use of ACSLS with DiskXtender.

Details on the supported versions of the ACSLS and LibAttach products are listed in the EMC Information Protection Software Compatibility Guide available on the Powerlink website.

License Server

DiskXtender licensing information is managed by the EMC Xtender Solutions® License Server program. The License Server program is included on the DiskXtender installation CD and can be installed on a DiskXtender server, or on a separate computer that is visible to the DiskXtender server through the network.

The License Server program also manages licensing information for several other EMC products, including EMC Documentum® ApplicationXtender® and EMC EmailXtender®.
The computer on which you install License Server depends on the environment:

- If License Server manages only a DiskXtender license for a single DiskXtender installation, then it can be safely installed on the DiskXtender server without any significant impact on performance.
- If License Server manages a DiskXtender license for multiple DiskXtender installations, then you may want to install it on a separate computer that is accessible to all of the DiskXtender servers.
- If License Server manages licenses for both DiskXtender and multiple ApplicationXtender clients, then it should be installed on a separate computer to avoid any impact on DiskXtender server performance.

The DiskXtender Search Module is optional software that works exclusively with DiskXtender for Windows release 6.2 and later. The DiskXtender Search Module software enables you to index files that are stored on one or more extended drives, create search queries, and then view files returned by the search query.

The DiskXtender Search Module includes two primary components:

- **Index and Search Engine (ISE)** — The ISE manages content indexing and is installed on a separate server from the DiskXtender server. A single ISE server can index files from as many as 10 DiskXtender servers. Each DiskXtender server should manage no more than five extended drives.

- **User interface** — The user interface provides a way to search a collection of indexes for files managed by DiskXtender, and then to view the search results. It also enables you to perform several important administrative tasks on the ISE, such as index preparation tasks and the addition of index file storage.

The user interface can be installed on the ISE server. It can also be installed on a different computer, so that you can connect remotely to perform searches and administrative tasks.

**Note:** The DiskXtender Search Module is not intended for end-user searches of data. Only users with administrative privileges on the ISE server or on the domain can view search results. Search capabilities should only be allowed to select individuals, such as a security officer or IT manager who has the authority or job responsibility for the retrieval of the company’s data.

You can install the DiskXtender Search Module along with DiskXtender in a new environment. You can also install the DiskXtender Search Module in an environment where DiskXtender is already managing files.

The ISE can index new files that are saved to the extended drive, as well as files that were on the extended drive prior to the DiskXtender or DiskXtender Search Module installation.
System requirements

The Windows servers on which you install DiskXtender and MediaStor should meet the requirements listed in Table 3 on page 30.

Table 3  Minimum and recommended hardware requirements for DiskXtender

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor(^a)</td>
<td>1.3 GHz</td>
<td>2.8 GHz</td>
</tr>
<tr>
<td>Memory</td>
<td>1 GB</td>
<td>2 GB</td>
</tr>
<tr>
<td>Free space on the system drive</td>
<td>200 MB</td>
<td>20% free</td>
</tr>
<tr>
<td>Total size of the extended drive</td>
<td>100 MB</td>
<td>10 GB</td>
</tr>
<tr>
<td>Operating system</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Windows 2003 Standard or Enterprise Edition with SP2 (x64)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Windows Storage Server 2003 (x64)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Windows Server 2008 Standard or Enterprise Edition with SP1 (x64)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\(^a\) DiskXtender is supported on x86 platforms running a supported version of the Windows operating system, including Intel and AMD x86 processors. Neither Itanium processors nor Windows operating systems for Itanium-based architectures are supported.

The DiskXtender installation guide provides in-depth details on system requirements.

The latest Windows operating system versions, service packs, and hot fixes that are certified for use with DiskXtender are listed in the EMC Information Protection Software Compatibility Guide available on the Powerlink website.
Security requirements

DiskXtender should always be installed in a trusted Microsoft Windows domain and on a dedicated server to maximize a secure deployment. In addition, the DiskXtender installation should be protected from access from unauthorized users. Local administrators and users on the DiskXtender server should be limited to highly trusted individuals.

DiskXtender and its components provide several mechanisms to ensure the security of the DiskXtender system. However, each environment is unique and may provide unforeseen security risks. All security issues that are reported will be given a high priority, with a goal of addressing the issue within 30 days.

The following sections discuss the security mechanisms available with DiskXtender.

Service account security requirements

The user account that DiskXtender uses to log on as a service must be a member of the local Administrators group on the DiskXtender server. This account must also have the Log on as a service privilege. Because DiskXtender uses the account entered during installation to log on to the DiskXtender service, this privilege is added to that account during installation.

The service account must have full access rights to all files in all media folders in order to manage the files. If the service account does not have access to the files, it assumes that there are no files to process. There are no error messages or other indications that DiskXtender is not managing the files.

Depending on the environment, the following additional requirements may apply:

- If you are using the MediaStor media service, then you must add the DiskXtender service account to the MsAdministrators group on the MediaStor server.
- If you are planning to index files by using the DiskXtender Search Module, then you must add the DiskXtender service account to the DxIndexers group on the ISE server.
Controlling access to the DiskXtender configuration

To assist in the prevention of unauthorized users from connecting to DiskXtender servers and configuring the system, the user groups listed in Table 4 on page 32 are created on the DiskXtender server during installation.

<table>
<thead>
<tr>
<th>Group name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DxAdministrators</td>
<td>Members of the DxAdministrators group can log onto the DiskXtender server, either locally or by using a Remote Administrator installation, and perform all functions except for editing audit log configuration settings.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>To manage the DiskXtender service (start, pause, and stop the service, and configure service startup settings), a user must be a member of both the local Administrators group and the DxAdministrators group.</td>
</tr>
<tr>
<td></td>
<td>If the Explorer Add-ons are installed, DxAdministrators can perform the following tasks:</td>
</tr>
<tr>
<td></td>
<td>• Purge files</td>
</tr>
<tr>
<td></td>
<td>• Set retention</td>
</tr>
<tr>
<td></td>
<td>• Perform privileged deletes</td>
</tr>
<tr>
<td></td>
<td>• Enable/disable Direct Read</td>
</tr>
<tr>
<td></td>
<td>All members of the local Administrators group are added to this group during DiskXtender installation.</td>
</tr>
<tr>
<td>DxUsers</td>
<td>Members of the DxUsers group can view the DiskXtender configuration when they log onto the DiskXtender server, either locally or by using a Remote Administrator installation, but they cannot change any settings. In addition, DxUsers cannot view the audit log or view or edit the audit log configuration.</td>
</tr>
<tr>
<td></td>
<td>If the Explorer Add-ons are installed, DxUsers can run file reports and view file properties.</td>
</tr>
<tr>
<td></td>
<td>All members of the local Administrators group and all members of the local Users group are added to this group during DiskXtender installation.</td>
</tr>
<tr>
<td>DxSecurityAdmins</td>
<td>Members of the DxSecurityAdmins group can view and configure audit log settings on the DiskXtender server. The DiskXtender administration guide provides additional information on viewing and configuring audit logs.</td>
</tr>
<tr>
<td></td>
<td>The DiskXtender service account is added to the DxSecurityAdmins group automatically during File System Manager installation.</td>
</tr>
<tr>
<td>DxMonitors</td>
<td>Members of the DxMonitors group can view the DiskXtender configuration when they log onto the DiskXtender server (either locally or by using a Remote Administrator installation), but they cannot change any settings. DxMonitors members also can view the audit log file on the DiskXtender server, but they cannot change audit log settings.</td>
</tr>
</tbody>
</table>

**Note:** On the MediaStor server, the groups are MsAdministrators, MsUsers, MsSecurityAdmins, and MsMonitors.

To add or remove users from these groups, use Microsoft Windows group management functions. When DiskXtender is installed in a Microsoft clustering or AutoStart™ environment, changes or additions to the security groups must be configured on each of the servers in the cluster or AutoStart domain.
Auditing system activity

DiskXtender audit logs provide a secure, access-controlled means for monitoring change events to the DiskXtender service, and whether each event succeeds or fails. The audit log enables you to monitor important DiskXtender events, including:

- Addition, editing, and deletion of configuration objects (extended drives, media folders, media groups, rules, and so on)
- Media management tasks
- Service stops and starts

Audit logging is automatically enabled, and the DiskXtender service account is automatically added to the DxSecurityAdmins group, during File System Manager installation. Similarly, MediaStor audit logging is automatically enabled during installation when the MediaStor service account is added to the MsSecurityAdmins group.

The File System Manager Administrator enables you to configure which events are logged, set a maximum log file size, and change the location where the log file is stored. You can also enable logging of auditing events to the Windows event log in addition to the DiskXtender audit log.

The performance impact caused by audit logging is minimal.

If you use external auditing software on the extended drive, however, there may be a more significant performance impact. Auditing software typically adds a filter driver to the server to monitor access to the file system. This filter amplifies file operation overhead, causing performance degradation. As a result, the use of external auditing software on the DiskXtender server and the extended drive is not recommended.
The following topics provide more information on managing files on a DiskXtender extended drive:

- Supported file types........................................................................................................ 36
- Migrating files to media ................................................................................................... 40
- Purging files ..................................................................................................................... 44
- Fetching files .................................................................................................................... 47
- Editing files ...................................................................................................................... 48
- Deleting files .................................................................................................................... 49
- Indexing and searching for files.................................................................................... 52
- DiskXtender file management through Windows Explorer ...................................... 54
File Management

Supported file types

DiskXtender supports a wide variety of file types. Because DiskXtender does not need to open a file in order to manage it, DiskXtender can manage most file types that can be saved on a Microsoft Windows NTFS volume. However, DiskXtender is designed to serve as an archiving tool for fixed or unstructured data. As a result, adherence to the following guidelines ensures optimal system performance.

The most common file types used with DiskXtender include but are not limited to:

- Microsoft Office files (.doc, .ppt, .xls, and so on)
- Adobe Acrobat files (.pdf)
- Text files (.txt)
- HTML files (.htm or .html)
- XML files (.xml)
- ZIP archives (.zip)
- Image files, such as JPEGs (.jpg), TIFFs (.tif), bitmaps (.bmp), and GIFs (.gif)

Note: The DiskXtender Search Module can index a majority of the common file types in this list. “Supported file types for indexing” on page 53 provides more information.

Files that are frequently accessed or changed could result in the production of lock files or temporary files. A lock file is a file produced by an application to prevent write access when it is already open by another user. A large number of such files can clog the DiskXtender system or inadvertently fill the DiskXtender Recycler if it is enabled. Therefore, the following file and data types are not recommended for use with DiskXtender:

- Frequently accessed files, such as email files or files in user home directories or temporary directories

IMPORTANT

If you must manage these types of files with DiskXtender, then you should use a media type that allows renames and provides faster performance, such as NAS.

- Data that is part of a database
- Application files for programs installed on the extended drive

Note: Installing applications on or running applications from the DiskXtender extended drive is not recommended.

The following file types are not supported by DiskXtender:

- Macintosh files
- Personal Folder files (.pst)

If the sixth character in a filename is a tilde and the eighth character is either null or a period (for example, filen~2.doc), then you can save the file to the extended drive, but DiskXtender does not move the file to media. This typically occurs in files with filenames that have been automatically shortened to an 8.3 format.
DiskXtender can manage files with Unicode characters in either the filename or the file data. However, characters may display incorrectly if the correct language code pages are not installed. In addition, the application that displays DiskXtender logs and reports is not Unicode compliant. Filenames in logs and reports may display incorrectly, even though the file data remains intact.

Some applications used with DiskXtender do not provide the same level of foreign language character support. Table 5 on page 37 lists supported applications with these limitations.

<table>
<thead>
<tr>
<th>Product</th>
<th>Foreign-language character support</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoStart</td>
<td>Supports only ASCII characters.</td>
</tr>
<tr>
<td>NetWorker® PowerSnap™</td>
<td>Supports file system backup if file names and directory names are ASCII characters.</td>
</tr>
</tbody>
</table>

**Note:** If you use the DiskXtender Search Module to index and search for files on a DiskXtender extended drive and the files include ANSI character encoding, such as Big5 (Chinese) or Shift-JIS (Japanese), then the corresponding code page must be installed and set as the default code page on the ISE server. If a different code page is set as the default on the ISE server, then perform the steps in the EMC DiskXtender Search Module Release 1.2 Release Notes to enable proper indexing and search of the ANSI-encoded files.

You should verify international character support statements for all applications installed on the DiskXtender server before you configure file migration.

When you save or edit a file on the extended drive, the full path and filename can total as many as 259 UTF-16 characters. The full path and filename include the following components:

```
Drive:\Directory1\Directory2\Filename.Extension
```

where *Drive* is the assigned volume drive letter, *Directory1* and *Directory2* are optional folders on the drive, *Filename* is the name of the file, and *Extension* is the file extension.

**Note:** Japanese path and filenames are limited to 145 characters or less.

DiskXtender does not prevent users from saving a file to the extended drive when the character count for the path and filename exceeds 259 characters. However, files with excessive path and filenames may not be migrated to media, depending on the type of media and the file system with which it is formatted.

Most types of media and media file systems support at least the same number of characters as DiskXtender. However, when writing to media that is formatted with the UDF file system, DiskXtender supports a shorter path and filename of only 127 characters.
Most NAS file systems support filepaths of 259 UTF-16 characters. However, if DiskXtender is writing to a share on the NAS device, the character count of the full filepath on the device is included in the maximum number of characters allowed. In other words, the total character count includes the path and filename on the extended drive and the full path to the share on the device.

### File stream support

File streams contain the data that is written to a file and give more information about a file than attributes and properties. For example, you can create a stream that contains search keywords or the identity of the user account that creates a file.

The NTFS file system uses file streams to store private data. Because NTFS supports file streams, many applications now take advantage of file streams to store their data.

DiskXtender can manage files with file streams as long as the DiskXtender media supports file streams. All DiskXtender media types support file streams except for some NAS devices. In general, file streams are supported on NAS devices that use Common Internet File System (CIFS) or Server Message Block 2.0 (SMB). If a NAS device is using a different protocol, then consult the device manufacturer for guidance on whether file streams are supported.

DiskXtender support for file streams ensures that you can protect all application data in files, not just the primary data. File streams are moved and fetched along with the primary file data. In addition, file streams can be restored from storage media, along with primary file data, for disaster recovery purposes.

**Note:** You cannot directly read files with streams from media by using the Direct Read feature in DiskXtender. You can set the Direct Read attribute for these files. However, when the file is requested, it is fetched to the extended drive instead of being read directly from the media. In addition, the Direct Read attribute is removed.

If a NAS device configured with DiskXtender does not support file streams, then the file is not moved to media. In addition, a warning message is listed in the event logs to notify you that the file could not be moved to media.

### Encryption

DiskXtender can manage encrypted files on the extended drive as long as the files are not encrypted with an on-the-fly encryption (OTFE) method, also called real-time encryption. This type of encryption prevents DiskXtender—specifically the DiskXtender service account—from gaining access to the files to manage them.

### Microsoft Windows offline files

DiskXtender supports the offline files feature available in several Windows operating systems. When users access the extended drive, they can configure files or folders on the extended drive as offline files. This enables users to access the files when their workstations are not connected to the network. When the workstations reconnect to the network, any changes that were made to the files are updated on the extended drive.

When you configure a purged file as an offline file, the file is fetched. DiskXtender continues to migrate, fetch, index, purge, and otherwise manage files that are configured as offline files. The files are updated on media and on the ISE server, if necessary, when they are synchronized back to the extended drive and are no longer offline.

**Note:** When you rename an offline file and the file contains file streams, then the file streams are lost when you reconnect to the network and update the file on the extended drive. This issue occurs regardless of whether DiskXtender is installed on the server.
Microsoft Windows DFS links

DiskXtender is supported in a Windows Distributed File System (DFS) environment. However, DiskXtender manages only the files that are physically located on the server where it is installed. It does not manage files on other servers that are connected to it by DFS links. For example, the following configurations are supported:

- The DFS link is on a server where DiskXtender is not installed (Server A), and the link points to an extended drive on a server where DiskXtender is installed (Server B).
  
  Users can use the DFS link on Server A to access the files on Server B, even if the files have been purged.
  
  DiskXtender manages only the files on Server B.

- The DFS link is on an extended drive on a DiskXtender server (Server A), and the link points to another server (Server B).
  
  Users can use the DFS link on Server A to access the files on Server B.
  
  The DiskXtender installation on Server A manages all of the files that are saved locally to its extended drive. However, it does not manage the files on Server B.

CAUTION

DFS is supported only in DFS nonreplication mode. Attempts to use DiskXtender with DFS replication enabled might cause data loss.
Migrating files to media

The term file migration refers to the function of moving files from a local hard drive to one or more pieces of storage media.

In DiskXtender, a move is actually a copy. When DiskXtender moves a file to media, it is really copying the file data out to media and adding extended attribute information to the file on the drive. The file is then managed by DiskXtender, and the data resides both on the extended drive and on the media.

You can migrate files to media through DiskXtender by using one of three file migration models:

- **Standard migration** — Each file is migrated once from the extended drive to a piece of media, as shown in Figure 4 on page 40.

- **Multi-target migration** — Each file is migrated from the extended drive to multiple targets (pieces, and even different types of media), as shown in Figure 5 on page 40.

Multi-target migration provides improved data availability and reliability. In the event that one of the pieces of media is not available, a file can be retrieved from another piece of media in a different target.
**Tiered migration** — With tiered migration, also called hierarchical storage management (HSM), each file is migrated twice: from one extended drive to another extended drive, and then from that extended drive to tape media, as shown in Figure 6 on page 41.

To accomplish this through DiskXtender, media folders on the second extended drive are configured as *Aggregate NAS media*. The files from the first extended drive are migrated to the Aggregate NAS media. DiskXtender then moves the files from the Aggregate NAS media to tape media.

When files are saved to a media folder on the first extended drive that contains a media group with Aggregate NAS media, DiskXtender does not allow you to rename files or folders on the first extended drive. This restriction mimics the behavior of the second extended drive (the Aggregate NAS media), because the second extended drive is writing to tape, which also does not allow file or folder renames.

The restrictions of Aggregate NAS media are designed to ensure that files and file tags on both extended drives remain synchronized, and that the files on the subsequent tape media are not orphaned.

Tiered migration *is only* supported through the use of the Aggregate NAS media type and tape media. DiskXtender does *not* support tiered migration from one extended drive to another media type (such as EMC Centera) before a final migration to tape. Migration from Aggregate NAS to media other than tape (such as EMC Centera or optical) is also *not* supported.
Customizing file migration

DiskXtender automates the migration of files to media by using a rule-based system. You can customize this rule-based system very specifically to determine which files are moved, what media they are moved to, and when. This customization is accomplished through the File System Manager Administrator by:

- Organizing files on the extended drive into media folders
- Grouping media into media groups and assigning it to media folders
- Configuring move rules that identify which files should be migrated
- Scheduling a window of opportunity when file migration can occur

Media folders

Media folders help to organize files on the extended drive. These folders are created as physical folders (or subfolders) on the extended drive, and can be viewed as such through Windows Explorer.

You can create a media folder by using a folder that already exists on the extended drive. Alternatively, you can create a new physical folder on the drive for the media folder.

Files on the extended drive can be stored in a single media folder, or they can be divided into multiple media folders. The creation of separate media folders enables you to segregate the data on both the extended drive and the storage media.

When a file is written to a piece of media, the directory structure on the media mirrors the extended drive directory structure. The root media folder, however, does not appear on the storage media. For example, if the Reports media folder is located at the root of extended drive E, then E:\Reports\Accounts.doc on the extended drive is stored as Accounts.doc on the media.

Media groups

Media groups are specific groupings or pools of media that have been assigned to a media folder. Files in the media folder are written to media in the media groups for the media folder.

Media groups provide several options that control the way files are written to the media in the media group. For example, you can specify whether files are written to each piece of media sequentially or randomly:

- With the sequential media fill method, each piece of media is filled with files based on the order in which the media is listed in the File System Manager Administrator. This fill method optimizes file retrieval performance and is designed for removable media.
- With the random media fill method, files are written to media as the media is available. This fill method optimizes file migration performance and is designed for NAS, EMC Centera, and TSM media.

It is also through media groups that you can configure automated labeling and compaction for removable media, as well as automated virtual media creation for EMC Centera.

A special kind of media group, called a multi-target group, enables implementation of the multi-target migration model. A multi-target media group is designed solely to contain media targets, which are two, three, or four standard media groups that contain the media to which you want to write files. You cannot assign individual pieces of media to the multi-target group, and there are no options or automated media management features. The options and automated media management features must be configured at the standard media-group level.
When using multi-target media groups, you can define an expiration policy for each target media group. When a file meets the expiration criteria for a target media group, it is deleted from the media in the group. However, the file remains on media in other target media groups until it meets the expiration criteria for those groups. The expiration policies enable you to reclaim space on some pieces of media while leaving files active on other pieces of media.

**Move rules**

Move rules contain the criteria that DiskXtender follows when choosing which files to move to a particular media group.

There are two types of move rules:

- **Inclusive** — Creating an inclusive move rule specifies which files should be moved, and which target group of media (either a standard or multi-target media group) will be used to store them.

- **Exclusive** — Creating an exclusive move rule specifies which files should not be moved to media.

You must create at least one inclusive move rule to move files to media.

You can configure how each rule selects files to be moved or excluded from movement based on the location of the file (media folder or subfolder), extension, attributes, and size. You can also configure the media group to which the move rule points, as well as an age delay for moving files, preventing DiskXtender from moving them until a specified time period has elapsed after each file was created, last accessed, or last written to (edited).

If you are using EMC Centera, Celerra with the FLR file system, or a NetApp NAS device with the SnapLock software, move rules can also be used to set retention for qualifying files. When a file qualifies for a move rule that contains a retention period, you cannot edit or delete the file until the retention period expires.

By default, files qualify for move rules when they are saved to the extended drive. If the move rule contains age delay criteria, then the file is qualified for move rules during a **background scan**.

A background scan is a scan of the extended drive. This scan is performed so that the files on the drive can be qualified against the rules (including purge, delete, and index rules) for each media folder. Background scans allow DiskXtender to verify that all files on the extended drive that need to be managed are being managed.

By default, background scans begin automatically at midnight each night and run only once in a 24-hour time period. However, you can change the time and frequency at which background scans occur to maximize system performance. You can also force DiskXtender to perform a background scan any time one is needed by right-clicking the extended drive and selecting Force Background Scan.

**Scheduling file migration**

When files qualify for migration based on move rules, those files are written to the move list for a media group. The move list is a list of files that need to be migrated to the media in the media group.

The move list is only processed, and files are only moved to media, when the Move Files to Media schedule is active. The Move Files to Media schedule specifies a time period during which file migration can take place.

By default, the Move Files to Media schedule is active from 8 p.m. to 9 a.m. However, you can adjust the schedule to maximize system performance. File migration can negatively impact file retrieval performance, so it should occur during the times of least activity.

The Move Files to Media schedule must be configured for each extended drive.

---

**Migrating files to media**
Purging files

When DiskXtender moves files, it really copies the files to storage media. In other words, the file data exists on both the media and on the extended drive.

When DiskXtender purges a file, it removes the file data from the extended drive and leaves behind a file tag on the extended drive. A file tag contains information about the file, including name, size, age, retention period (if applicable), and other attributes.

Purging files frees space on the extended drive, while maintaining the appearance that the files are still on the drive. Table 6 on page 44 provides details on file icons for unmanaged, fetched, and purged files.

<table>
<thead>
<tr>
<th>File type</th>
<th>Icon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unmigrated and fetched file</td>
<td></td>
</tr>
<tr>
<td>Purged file (file tag) in Windows Vista and Windows Server 2008</td>
<td></td>
</tr>
<tr>
<td>Purged file (file tag) in earlier Windows versions</td>
<td></td>
</tr>
</tbody>
</table>

A purged file is still accessible, and to a user machine, appears to reside on the extended drive. When the user requests the file, DiskXtender performs the following actions:

1. Accesses the media where the file is stored.
2. Retrieves the file data.
3. Displays it for the user.

When a file has been migrated to a single piece of media, a file tag consumes between 0 bytes and 1 cluster of disk space. (On Microsoft Windows NTFS systems, a cluster of disk space averages approximately 4 KB, although the size depends on a number of variables.) When a file has been migrated to multiple pieces of media through multi-target migration, then a file tag is likely to consume 1 cluster of disk space.

Because space and file retrieval requirements vary, DiskXtender provides several different ways to purge files from the extended drive, enabling you to be very specific as to when files are purged from the extended drive.

Files cannot be purged from the extended drive until they are moved to media and indexed, if indexing is enabled. However, once a file is moved to media, you can choose whether to automatically purge that file from the extended drive:

- Immediately after it has been moved
- When extended drive space is low
- During the next background scan (after the file qualifies for a purge rule)

You can also select specific files and purge them manually by using the DiskXtender Explorer Add-ons.
There may even be some files that you do not want to purge at all. The purge options you choose are likely determined by a number of factors, including:

- The type of storage media you use
- How much space you have on the extended drive
- How often files are accessed
- How long files are normally active

For example, if the files on the extended drive are accessed frequently for a certain number of days after they are created, you should wait to purge the files until they are no longer needed.

---

### Purge rules

A purge rule contains the instructions that DiskXtender follows when choosing which files to purge from the extended drive and when.

Purge rules are necessary if you want to purge files as disk space is needed or during background scans.

As with move rules, there are two types of purge rules:

- **Inclusive** — An inclusive purge rule enables you to specify which migrated files should be purged from the extended drive and when.
- **Exclusive** — An exclusive purge rule enables you to specify which moved files you do not want DiskXtender to purge.

You can configure how each rule selects files to be purged or excluded from purging based on the location of the file (media folder or subfolder), extension, attributes, and size. You can also configure an age delay for purging files, which prevents those files from being purged until a specified time period has elapsed after the file was created, last accessed, or last written to (edited).

---

### Purging files as disk space is needed

You can set up purge rules so that DiskXtender purges files only when disk space is needed. The following process occurs for each file that is managed by DiskXtender:

1. When files qualify for a purge rule (during a background scan), DiskXtender adds them to the purge list.
2. As additional files are written to the extended drive and the amount of used space on the extended drive reaches a certain percentage (the purge start watermark), DiskXtender begins purging the files that appear on the purge list.
3. DiskXtender continues to purge files until the percentage of used space is reduced to an acceptable level (the purge stop watermark).

You can customize the purge watermarks for each extended drive. By default, the purge start watermark is set to 95 percent, and the purge stop watermark is set to 90 percent.

Because the purge list is processed only for as long as is necessary to free up space to the purge stop watermark, you can also configure the priority for files added to the purge list. Priorities can be used to ensure that certain files, such as larger files or files that are accessed less frequently, are purged first (when disk space is needed), which optimizes the purge process.
The purging of files in this way ensures that file data remains on the extended drive until purging to recover space on the extended drive is absolutely necessary. Maintaining file data on the extended drive can improve performance because it helps minimize fetch requests.

### Purging files during background scans

Files qualify for purge rules during a background scan. You can set up the purge rules so that DiskXtender purges files as soon as they qualify for the purge rules. This purging option helps to maintain a high volume of free space on the extended drive.

Note: Files may be purged before a background scan takes place (regardless of purge rule settings) if disk space is needed before the next background scan starts.

### Purging files immediately after migration

You can purge files immediately after they are moved to media by using a move rule option. You may want to use this purge option to target certain files for movement to media and immediate purge.

**IMPORTANT**

Even if you plan to purge files immediately after they are moved by using the move rule option, you should still configure purge rules. If you do not configure purge rules and the purged files are fetched, the files may not be purged again.

### Purging files during DVD-R finalization

If you use DVD-R media, you cannot purge files until the media they are written to is finalized. When you finalize the media, you can choose to purge all files that have been written to that media.

If you do not choose to purge files as a function of finalization, the data for those files remains on the extended drive until the files qualify for configured purge rules. Then it is the selections made in the purge rules that determine when the files are purged from the extended drive.
Fetching files

If a user attempts to access a file on the extended drive that has been migrated to media and purged, the file is retrieved from the media and copied back to the extended drive. The user can then open the file on the extended drive. The retrieval of a purged file from media is called a *fetch*.

If the environment is a multi-target migration environment, purged files are fetched from the first target media group that is listed under the multi-target group. You can change the media priority from which DiskXtender fetches the file by changing the order in which the standard media groups appear under the multi-target group.

When purge rules are configured, fetched files are qualified against the purge rules again during the next background scan, and purged again as appropriate based on purge rule settings.

If you want to prevent users from fetching files from media during a certain time period each day, you can disable the Allow Fetches From Media schedule. This schedule can be configured for each extended drive.

Prefetch

To reduce read requests from media during high traffic times, you can anticipate file retrieval needs and *prefetch* frequently used files. During a prefetch, DiskXtender retrieves files from storage media and writes the file data to the extended drive.

There are two ways to prefetch files through DiskXtender:

- If you know that you will need specific files, you can select the files by setting up a prefetch request through the Prefetch Request Wizard.
- If you want to temporarily remove a piece of media from a device (for example, to perform maintenance), you can prefetch all files from the piece of media by assigning a Prefetch media task to the media.

Direct Read

The DiskXtender Direct Read feature allows a purged file to be opened directly from the media when requested, rather than being fetched back to the extended drive and opened from there.

Direct Read is strongly discouraged in most DiskXtender environments. In select situations, Direct Read can ease the strain on system resources caused by fetching certain files back to the extended drive. However, Direct Read requests can be as much as three times slower than normal fetch requests.

The DiskXtender administration guide provides details on when to use Direct Read and how to enable it.
Editing files

To keep the files and file structures on the extended drive synchronized with the files on the media, DiskXtender prohibits certain edit and rename operations on the extended drive for migrated files and folders that contain migrated files.

These restrictions depend on the type of media you use and, for removable media, the type of file system the media is formatted with. If the media does not allow the edit or rename, then DiskXtender must enforce the same restriction on the extended drive to maintain synchronization.

Table 7 on page 48 provides details for each type of media and file system.

<table>
<thead>
<tr>
<th>Media type</th>
<th>File system</th>
<th>Edit/rename file</th>
<th>Rename directory</th>
<th>Set attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>DVD-R</td>
<td>UDF (sequential)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>DVD-RAM</td>
<td>UDF (overwritable)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>OTG (OSS)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>DVD-ROM</td>
<td>UDF (read-only)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>EMC Centera (active retention)</td>
<td>Not applicable</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EMC Centera (no retention or expired retention)</td>
<td>Not applicable</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Magneto-optical (MO)</td>
<td>UDF (overwritable)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>OTG (OSS)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>MO WORM</td>
<td>UDF (overwritable)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>OTG (OSS)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>NAS (Standard)</td>
<td>NTFS</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>NAS (Aggregate)</td>
<td>NTFS</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>NAS (Retained)</td>
<td>NTFS, Mixed mode</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Tape</td>
<td>OTG (TSS)</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tape-WORM</td>
<td>OTG (TSS)</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TSM</td>
<td>Not applicable</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>UDO</td>
<td>UDF (overwritable)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>OTG (OSS)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>UDO-WORM</td>
<td>UDF (overwritable)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>OTG (OSS)</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
</tbody>
</table>

If you attempt to perform an edit or rename when it is not allowed on the extended drive, then a message appears to notify you that the action cannot be performed.

Chapter 4, “Media Management,” provides more information on supported media types and file systems.
Deleting files

In certain situations, you may not want to keep files on the extended drive after a period of time. Unless retention has been set for a file, you can delete the file from the extended drive. There are two ways to delete files from the extended drive:

- Manually (for example, through Windows Explorer)
- Automatically by using DiskXtender delete rules

When you delete a file from the extended drive, DiskXtender attempts to delete the file from media (if the file has been migrated to media).

If DiskXtender cannot delete the file from media, the file is marked for deletion. It still exists on the media, but it becomes an orphaned file and is no longer recognized or tracked by DiskXtender. The deleted files are not actually removed from the media until the media is compacted and reformatted.

DiskXtender success in deleting files from media depends on the type of media that is used. For removable media, the type of file system the media is formatted with also impacts file delete capabilities.

Table 8 on page 49 provides details on whether you can delete files from the extended drive or media.

<table>
<thead>
<tr>
<th>Media type</th>
<th>File system</th>
<th>Deletion is possible on the drive</th>
<th>Deletion is possible on the media</th>
</tr>
</thead>
<tbody>
<tr>
<td>DVD-R</td>
<td>UDF (sequential)</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>DVD-RAM</td>
<td>UDF (overwriteable)</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>OTG (OSS)</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>DVD-ROM</td>
<td>UDF (read-only)</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>EMC Centera (active retention)</td>
<td>Not applicable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EMC Centera (no retention or expired retention)</td>
<td>Not applicable</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Magneto-optical (MO)</td>
<td>UDF (overwriteable)</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>OTG (OSS)</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>MO WORM</td>
<td>UDF (overwriteable)</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>OTG (OSS)</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>NAS (Standard)</td>
<td>NTFS</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>NAS (Aggregate)</td>
<td>NTFS</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Tape</td>
<td>OTG (TSS)</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Tape-WORM</td>
<td>OTG (TSS)</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>TSM</td>
<td>Not applicable</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>
### File Management

If you attempt to delete a file that is under retention, then a message appears to notify you that the file cannot be deleted.

**Note:** If you enable the DiskXtender Recycler, files that you manually delete from the extended drive are placed in the Recycler rather than being deleted from media. Files that are deleted by delete rules or by using EMC Centera privileged deletes are **not** placed in the Recycler. “Recycler” on page 50 provides details.

Chapter 4, “Media Management,” provides more information on media types and file systems.

#### Delete rules

A delete rule contains the instructions that DiskXtender follows when choosing which files to delete from the extended drive and from storage media, if applicable. Delete rules also contain an exclusion option that allows you to identify files that should not be deleted.

**Note:** Delete rules do not prevent files from being manually deleted by users accessing the extended drive. The rules only impact automatic deletion of files by DiskXtender. The file retention feature is intended to prevent files from being deleted by users.

Files are qualified against delete rules and then subsequently deleted during background scans.

You can configure how each rule selects files to be deleted or excluded from deletion based on the location of the file (media folder or subfolder), extension, attributes, and size. You can also configure an age delay for file deletion, which prevents files from being deleted until a specified time period has elapsed after the file was created, last accessed, or last written to (edited).

#### Recycler

The DiskXtender Recycler functions similarly to the Windows Recycle Bin, but affects only files on a drive extended through DiskXtender. There is one Recycler for each extended drive.

When you enable the DiskXtender Recycler and a user deletes a file from the extended drive, the file is placed in the Recycler instead of being permanently deleted. This occurs for files that are managed by DiskXtender (files that have qualified for movement to media), and files that are **not** managed by DiskXtender (files that do not qualify for movement to media).

By using the File System Manager Administrator interface, you can then restore files from the Recycler if necessary, or delete them permanently if they are no longer needed. A restored file retains all of its migration information, if it was migrated to media. You do not need to re-migrate the restored file to media.

---

**Table 8  File delete capabilities by media type (page 2 of 2)**

<table>
<thead>
<tr>
<th>Media type</th>
<th>File system</th>
<th>Deletion is possible on the drive</th>
<th>Deletion is possible on the media</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDO</td>
<td>UDF (overwritable)</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>OTG (OSS)</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>UDO-WORM</td>
<td>UDF (overwritable)</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>OTG (OSS)</td>
<td>✔️</td>
<td></td>
</tr>
</tbody>
</table>

a. This operation is not allowed if the media is in a DVD-RAM drive.
IMPORTANT

The Recycler is not a substitute for regular backups of the extended drive. It is intended only for short-term storage of deleted files to provide rapid recovery when an accidental deletion takes place. As a result, the Recycler is located on the extended drive, and it factors into the total amount of space on the extended drive. To avoid filling the drive with deleted files, empty the Recycler on a regular basis. You can schedule the Recycler to empty automatically, or you can manually empty the Recycler as needed.

You can exclude certain files from being placed in the Recycler when they are deleted from the extended drive. Instead, the files are deleted permanently when they are deleted from the extended drive.

These exclusions are intended to save space on the extended drive by preventing files from being placed in the Recycler when you are certain that they will never need to be restored.

You can exclude files based on the location or name of the file. In addition, you can specify whether files of a certain migration status (migrated, purged, or fetched) are excluded from the Recycler. Certain files, like Windows and shell temporary files, database lock files, and utility files, are excluded by default.

Note: Files deleted according to delete rules or by using EMC Centera privileged deletes are not placed in the Recycler.

Because the DiskXtender Recycler resides on the extended drive, the disk space used by the Recycler factors into the total available disk space for the extended drive. You should empty the Recycler on a regular basis to help maintain an adequate amount of space on the extended drive. When you empty the Recycler, the files in the Recycler are permanently removed from DiskXtender.

You can empty the Recycler either manually when needed or on a scheduled basis. If you schedule the Recycler to be emptied, you can choose whether to empty the entire Recycler or to remove only files that meet certain age criteria, such as files that were deleted more than seven days ago.
Indexing and searching for files

The DiskXtender Search Module software enables you to index files stored on an extended drive, create search queries, and then view files returned by the search query.

Indexing files

The DiskXtender server and the ISE component of the DiskXtender Search Module work together to identify files that should be indexed and then to index them, respectively. Indexing can be enabled for one or more extended drives on a DiskXtender server.

DiskXtender index rules enable you to identify which files you do—and which files you do not—want to index. You can choose files for indexing (or exclusion from indexing) based on file location, name, type, size, attributes, and age. You can index new files that are saved to the extended drive, as well as files that are already being managed by DiskXtender.

Files on the extended drive are evaluated against index rules when they are saved to the drive if the real-time moves feature is enabled. They are saved when they are added, edited, renamed, or moved. They are also evaluated against rules during a background scan.

Qualifying files are written to the Index Transaction Log (ITL). There is one ITL for each extended drive with indexing enabled. The ITL is processed, and files are submitted to the ISE for indexing, when the index schedule begins. To maximize system performance, you should schedule indexing for a time when there is a minimum of activity on the network, the DiskXtender server, and the ISE server.

As the ISE indexes files on the ITL for an extended drive, the index information is grouped into an index collection for the extended drive. The index collection is stored on the ISE server.

If files are edited or deleted on the extended drive, the ISE updates the corresponding index files in the index collection so that they remain current with the files on the extended drive. These updates occur along with new indexing activity, according to the indexing schedule.

In the unlikely event that the files on the extended drive are not synchronized with the indexes on the ISE—such as in a disaster recovery scenario—you can schedule a resynchronization process. This resynchronization process ensures that:

- There is corresponding index information on the ISE for all files on the extended drive that are marked as indexed.
- There are no orphan indexes on the ISE for files that have been deleted from the extended drive.

Searching for files

Once files are indexed, you can search for the files by using the DiskXtender Search Module user interface. There are two options for building a search query:

- Build complex queries including Boolean operators (such as AND, OR, and NOT) and proximity operators (which limit results based on the location of search terms within a file in relation to each other).
- Build simple queries by using natural language prompts for search terms. Natural language prompts enable you to easily search for an exact phrase, for all words in a list, or for at least one of the words in a list. They also enable you to search for files that do not have any of the words in a list.
Search results appear in a table in the user interface with details about the search query and the files themselves. You can view an excerpt of a file in the results list, or you can open a file in its Microsoft Windows-associated application.

If the search returns a significant number of results, you can sort the results. Alternatively, you can further limit the number of results by adding search criteria to the query or by filtering the results by filename, path, or date.

Exporting search results enables you to save them in a file. The file can then be imported into a spreadsheet program for additional analysis of the results.

If you know you will need to run a query on a regular basis, you can save the query.

The ISE can index the following file types:

- Microsoft Word
- Microsoft RTF
- Microsoft Excel
- Microsoft PowerPoint
- Microsoft Visio

**Note:** To index Visio files, you must install the Visio IFilter 2003 Add-in on the ISE server. Download the add-in from the Microsoft website, and install it before you begin indexing files.

- HTML
- JPEG (Exchangeable Image File Format, or EXIF, markers only)
- Adobe PDF
- Text files

**Note:** The ISE cannot index text files unless they either contain at least several hundred characters, or a carriage return or line feed at the end of each line.

- TIFF (metadata only)
- XML
- ZIP

**Note:** The ISE only indexes supported file types within the ZIP file.

The ISE supports the indexing and search of files with Unicode characters in the filename, file metadata, and file data. If the files include ANSI character encoding, such as Big5 (Chinese) or Shift-JIS (Japanese), then the corresponding code page must be installed and set as the default code page on the ISE server.

If a different code page is set as the default on the ISE server, then perform the steps in the EMC DiskXtender Search Module Release 1.2 Release Notes to enable proper indexing and search of the ANSI-encoded files.
DiskXtender file management through Windows Explorer

The DiskXtender Explorer Add-ons utility enables you to perform DiskXtender file and folder management functions from Windows Explorer, rather than from the File System Manager Administrator.

You can access the Explorer Add-ons by using either a wizard or by right-clicking files in Windows Explorer to access the DiskXtender shortcut menu.

The Explorer Add-ons connect to the extended drive through Windows Explorer so that users without a full installation of DiskXtender can perform the following tasks:

- View DiskXtender-related information about a file, including its retention period and migration status, as well as information about the media to which the file has been migrated
- Set Direct Read for a file
- Purge a file
- Change the retention setting for a file
- Delete a retained file from EMC Centera (Privileged Delete)

You can perform a task on one file at a time, or you can select multiple files and perform the task on all of them simultaneously.

The Explorer Add-ons also provide a user fetch notification feature. When a user with Explorer Add-ons installed requests a file that must be fetched from media and the retrieval takes more than a few seconds, a progress message indicates that file retrieval is taking place. This situation occurs most often when a requested file exists on a piece of media that must be mounted in a drive.

The Explorer Add-ons are installed automatically on the DiskXtender server. However, you can also install them on a separate computer. Release 6.3 and Release 6.4 of the Explorer Add-ons can connect to a DiskXtender 6.4 server.

Release 6.3 supports the following 32-bit operating systems:

- Microsoft Windows XP Professional with Service Pack 3
- Microsoft Windows Vista with Service Pack 1

Release 6.4 supports the following 64-bit operating systems:

- Microsoft Windows 2003 Standard or Enterprise Edition with Service Pack 2 (x64)
- Microsoft Windows Server 2008 Standard or Enterprise Edition with Service Pack 1 (x64)
- Microsoft Windows XP Professional with Service Pack 3
- Microsoft Windows Vista with Service Pack 1
The following topics provide details on the storage media to which DiskXtender migrates files:

- EMC Centera................................. 56
- Network-attached storage................ 67
- Removable media............................ 73
- Tivoli Storage Manager .................... 81
When you install DiskXtender, the EMC Centera SDK is installed automatically on the DiskXtender server to enable communication between DiskXtender and an EMC Centera cluster.

When you create an EMC Centera media service in DiskXtender, you specify the connection string that the EMC Centera SDK uses to enable DiskXtender to connect to an EMC Centera cluster. The connection string includes information about the EMC Centera access nodes, as well as the Pool Entry Authorization (.pea) file that contains the profile information that should be used for the DiskXtender connection. DiskXtender connects with the access nodes by using a TCP/IP connection.

EMC Centera security is based on pools and application profiles:

- An application pool, or "virtual" pool, is a logical area on an EMC Centera device where applications can store their data. Virtual pools enable you to logically separate data on an EMC Centera device. This is particularly useful if there are multiple applications with different security needs that write data to an EMC Centera device.

- Access profiles provide access to one or more EMC Centera pools. Pools grant capabilities to applications that are accessing EMC Centera by using the profile. For DiskXtender, the profile must have the Write, Read, Delete, and Query capabilities. To allow privileged deletes of retained files, the profile should also have the Privileged Delete capability.

- A .pea file, which is generated while creating or updating an access profile, is a clear-text, XML-formatted, nonencrypted file that can be used by system administrators to communicate and distribute authentication credentials to application administrators.

Each EMC Centera cluster can have multiple virtual pools and multiple access profiles.

The EMC Centera online help provides information on pools, access profiles, and .pea files, which should be configured by an EMC Centera technical representative.

There should be a single .pea file for each media service. You cannot specify multiple .pea files for a single media service. If the virtual pool is being replicated to another EMC Centera cluster, the .pea files for the virtual pools and access profiles on the two clusters are merged. This merged .pea file, which enables access to both pools with a single profile, should be configured by an EMC Centera technical representative.

If you have multiple, separate pools and access profiles, each pair with its own corresponding .pea file, then you can create multiple EMC Centera media services. Multiple media services enable you to further separate data that you are writing through DiskXtender.

If you do not specify a .pea file when you create an EMC Centera media service, then DiskXtender uses the Anonymous profile to connect to EMC Centera.

Note: The Anonymous profile is disabled in CentraStar® 3.1 and later. If CentraStar 3.1 or later is installed on the EMC Centera cluster, you must use an access profile when you create a media service in DiskXtender. If you are using an earlier release of CentraStar with DiskXtender and you upgrade to 3.1 or later, you can continue to use the Anonymous profile.
EMC Centera media is virtual, meaning that a piece of media defined in DiskXtender does not specifically correspond to a physical piece of media (like a tape cartridge). The virtual media is designed to simulate divisions of an EMC Centera cluster.

The use of virtual media instead enables you to take advantage of the flexible file migration features available in DiskXtender.

Each piece of virtual media can contain as much as 256 GB of file data and metadata, and can store up to 100,000 files. This is an either/or limit. It is possible that you can fill a piece of EMC Centera media with 100,000 files, but remain well under the 256 GB size limit.

When you create a piece of virtual media, the 256 GB of space is not reserved on EMC Centera. Space is used on EMC Centera only when a file is migrated from DiskXtender.

Note: Because space is not reserved on EMC Centera for virtual media, if you meet the limit of 100,000 files before you meet the limit of 256 GB, the size of the piece of media is limited to the size required for the 100,000 files. In other words, the difference between the total size of the 100,000 files and 256 GB is not wasted space on EMC Centera.

The size limit for EMC Centera media is imposed so that finding a file associated with a piece of media does not take an inordinate amount of time. When either threshold is reached, the media is considered full and cannot receive any more files, although files can be retrieved from the media when necessary. Full media appears with a blue label in the File System Manager Administrator.

You can create as many pieces of virtual media as you need. You are limited only by the total amount of space available on the EMC Centera.

When a piece of virtual media is created in DiskXtender, a corresponding EMC C-Clip™ for the media is created on EMC Centera. Once the C-Clip is created, the content address (CA) of the C-Clip is sent back to DiskXtender and is stored in the Microsoft Windows registry on the DiskXtender server.

When DiskXtender migrates a file to a piece of EMC Centera media, a C-Clip for the file is created on the EMC Centera device. Metadata about the piece of virtual media associated with the file is stored with the file on the EMC Centera device.

In addition, DiskXtender creates a special C-Clip on the EMC Centera cluster daily at midnight (EMC Centera cluster time). This new C-Clip contains a list of all media C-Clips currently on the system. One C-Clip is created for each EMC Centera media service. The CA for the C-Clip is stored in the DiskXtender event log when the C-Clip is created. If a disaster occurs, an EMC Customer Support Representative can retrieve the C-Clip to develop a list of media to restore to DiskXtender.

There are two ways to create virtual EMC Centera media through DiskXtender:

- **Automatically through the media group** — Media is created automatically either when free space in the media group falls below a certain number of megabytes or when the number of available pieces of media falls below a certain level. The media is also automatically allocated to the extended drive and added to the media group.

- **Manually through the media service** — Use this method to create individual pieces of media. Then allocate the media to the extended drive and add it to a media group to make it available for file migration. This option is not recommended for most environments.
If you no longer need the files that have been written to a piece of EMC Centera virtual media, you can run a Format media task on the media to clear the files from the media. The EMC Centera Garbage Collection feature then reclaims the space made available by the deleted files.

**Note:** The Format task may take a significant amount of time to complete for EMC Centera media.

---

**Content-addressable storage**

With content-addressable storage (CAS), EMC Centera ensures that applications, such as DiskXtender, no longer have to track the physical location of stored information. Instead, by using the CentraStar software operating environment, EMC Centera creates a unique identifier, based on the attributes of the content, that applications use for retrieval.

The unique identifier is called a content address (CA). The CA uniquely represents the object and its associated metadata, and is required to retrieve the object.

The following topics provide details on how DiskXtender writes files to EMC Centera media, as well as how to customize file migration between DiskXtender and EMC Centera.

**How DiskXtender writes files to EMC Centera**

When DiskXtender writes a file to EMC Centera, a CA for the file (BLOB) is generated and stored in an XML file with standardized metadata from the DiskXtender system. The XML file is called a C-Clip Descriptor File (CDF).

**Note:** You can add custom metadata to CDFs by using DiskXtender media groups. This custom metadata can be used to enhance EMC Centera Seek and Chargeback Reporter reports.

Another CA for the CDF is generated, and then DiskXtender stores the CDF and the file data in a package on the EMC Centera cluster. This complete package, which contains both file data and metadata, is called a C-Clip and is illustrated in Figure 7 on page 58.
The CA for the CDF is returned to DiskXtender and stored for the file. When the file is purged from the extended drive, this information can be used to retrieve the file data from EMC Centera.

EMC Centera Storage Strategies

Data can be stored on an EMC Centera device by using one of two storage strategies:

- **Storage Strategy Capacity** is designed to maximize the storage capacity of the cluster by taking advantage of single-instance storage. With single-instance storage, duplicate copies of a file are not stored on the cluster. Only a single copy of a file is stored.

- **Storage Strategy Performance** is designed to maximize file storage and retrieval performance at the cost of single-instance storage. With this storage strategy, smaller files with identical content may be stored multiple times. This is because it is faster to store duplicates than it is to perform the data comparison necessary to eliminate duplication. However, single-instance storage is still used to exclude duplicates of larger files. This is because the data comparison is equal in speed to or faster than the amount of time necessary to store the file itself.

Consult with an EMC Centera technical representative to decide which storage strategy is appropriate for your environment. Only qualified EMC Centera service personnel can change the storage strategy for a cluster.

**Note:** DiskXtender also works with both EMC Centera data protection mechanisms; Content Protection Mirrored (CPM) and Content Protection Parity (CPP). The EMC Centera protection mechanism (CPM or CPP) is transparent to DiskXtender.

DiskXtender options to tune CAS

DiskXtender provides media service options that enable you to customize the way files are stored to EMC Centera, and therefore maximize performance:

- **Collision avoidance** — Collision avoidance ensures that a unique CA is created for each file stored on EMC Centera, even if the file is a duplicate of another file stored on the cluster. If the file is edited and re-migrated, then a different unique CA is created.

  This feature is designed to prevent the unlikely event where the same CA is created for different files. If the files are purged and you attempt to fetch the second file, the data for the first file with the CA is returned instead. The data for the second file is irretrievable.

  Collision avoidance should not be used in most environments because it prevents the primary benefit of single-instance storage, which is the elimination of duplicate content so that only a single copy of each file is stored. It should be used only in environments where even the most remote possibility of data loss is unacceptable, or in environments where single-instance storage is forbidden, usually due to legal regulations.

  **Note:** If you enable collision avoidance, each file is stored uniquely, even if you are using Storage Strategy Capacity (single-instance storage).

- **Embedded BLOBs** — You can set a threshold for embedding small BLOBs (file data) in the CDF. Embedding file data in the CDF can decrease read and write times, since the overhead required to manage two objects (CDF and BLOB) is greater than the overhead required to manage a single object. You can embed files of up to 100 KB in the CDF.
Figure 8 on page 60 illustrates an embedded BLOB, while Figure 9 on page 60 illustrates a separate CDF and BLOB.

To maximize the performance benefits of this feature, files smaller than 100 KB (the maximum value for the option) should be embedded in the CDF.

If the EMC Centera is configured for Storage Strategy Capacity (single-instance storage), the embedding of BLOBs for files smaller than 100 KB will not allow you to realize the benefits of the storage strategy for these files. This is because the file content is embedded in the CDF. If you embed the BLOBs for files smaller than 100 KB, then single-instance storage is applied only to files larger than 100 KB.

**Note:** The total file size (all streams and the stream tags) must be less than the embedded BLOB threshold before the BLOB is embedded in the CDF.
**Client-side ID calculation**—The Client-side ID (hash) calculation option enables you to control whether the EMC Centera API calculates the CA for a piece of data before the data is sent to the EMC Centera cluster. If the calculation results in the determination that duplicate data exists on the EMC Centera cluster, the duplicate data is not sent.

Client-side ID calculation can improve performance and maximize storage efficiency under the following conditions:

- Files are larger than 10 MB in size.
- Identical data is likely to be sent to EMC Centera.
- You are using Storage Strategy Capacity (single-instance storage).

Client-side ID calculation is not beneficial under the following conditions:

- File data is embedded in the CDF (in other words, when you set an embedded BLOB threshold of greater than zero).
- Files are small (less than 10 MB).
- You are using Storage Strategy Performance or collision avoidance and files are stored uniquely even if they are identical.

**Note:** If you are using CentraStar 3.0.2 or later, or 3.1.1 or later, additional configuration steps are required on the EMC Centera device to enable client-side ID calculation. Contact an EMC Centera technical representative for assistance in enabling this feature if you are using one of the specified CentraStar versions.

**Garbage Collection**

When a file is deleted from the DiskXtender extended drive, a delete transaction is issued and flushed to the target storage device. Delete transactions can flush every minute, depending on what other transactions have been initiated.

When EMC Centera receives a delete transaction from DiskXtender, the CDF is deleted from the EMC Centera device, and the BLOB is left there (orphaned). CDFs not under retention can be deleted from any type of EMC Centera device.

If the EMC Centera Garbage Collection process is enabled, then the BLOBs with deleted CDFs are removed from the EMC Centera device and space is recovered. The file data for deleted files is removed from the EMC Centera device and is not recoverable. If Garbage Collection is disabled, however, then the BLOBs with deleted CDFs remain on the EMC Centera device and occupy space.

**Garbage Collection and the DiskXtender Recycler**

If the DiskXtender Recycler is enabled, files are placed in the Recycler when they are deleted from the extended drive. A delete transaction is sent to the EMC Centera cluster when the file is deleted from the Recycler.

When a significant number of delete transactions are sent to the EMC Centera cluster, the completion of those transactions may take a long time. During that time, file fetches may be delayed or even canceled due to timeout issues. **Do not** empty the Recycler when users are most likely to access the system. Or, if the Recycler is disabled, **do not** delete a significant number of files from the extended drive when users are most likely to access the system.
Compliance through retention and audit

EMC Centera is designed to facilitate compliance with externally driven regulations and internal governance requirements through its retention and audit features, including the features discussed in the following topics.

File retention

EMC Centera can protect stored data through its retention feature, which is complemented by the DiskXtender retention feature. Through DiskXtender, you can apply a retention period automatically to files that qualify for move rules. You can also apply retention to and extend retention periods for specific files by using the DiskXtender Explorer Add-ons utility.

Once DiskXtender applies a retention period to a file, the file cannot be edited or deleted from the extended drive until the retention period expires. (If you edit a retained file, you must save the file with a new filename.)

If you have an EMC Centera GE or EMC Centera CE+ device, the file is also protected on the EMC Centera device.

If you have an EMC Centera Basic Edition and you apply retention through DiskXtender, the file is protected on the extended drive but is not protected on the EMC Centera device.

Table 9 on page 62 lists the retention options for files written to EMC Centera through DiskXtender.

<table>
<thead>
<tr>
<th>Type of retention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fixed retention period</td>
<td>A specific period of time during which file retention is enforced.</td>
</tr>
<tr>
<td>Retention class</td>
<td>A symbolic representation of a retention period. When the retention class is defined, you specify a name and a retention period (in days). You can edit the retention period for a retention class by changing the class definition, thereby changing the retention period for a group of files. Note: If you have an EMC Centera CE+ device, you can only extend the retention period definition for a retention class. The list of retention classes and their definitions in DiskXtender is refreshed every time the EMC Centera media service is refreshed. This occurs approximately every two minutes. The list is stored and updated locally on the DiskXtender server (in addition to the definition on the EMC Centera device). This enables retention enforcement on the extended drive even if the EMC Centera device is unavailable. Even though you can configure retention classes of less than one day on the EMC Centera cluster, you cannot use those retention classes in DiskXtender. Retention classes of less than one day are not listed in the DiskXtender interface.</td>
</tr>
<tr>
<td>Infinite retention</td>
<td>Retention that can never expire.</td>
</tr>
</tbody>
</table>

If you set global retention on the EMC Centera device and you configure a different retention period through DiskXtender, the DiskXtender retention period applies. This is true even if the DiskXtender retention period is zero days (no retention). Therefore, when you set a retention period of zero days through DiskXtender, the file is not protected on the EMC Centera device, even if EMC Centera is configured for a global retention period of one or more days.

DiskXtender always applies a retention period to files written to EMC Centera, even if the retention period is zero days (no retention). You cannot automatically apply the global retention period set on the EMC Centera device to files on the extended drive.
To match the global retention period on EMC Centera with the retention set on files on the extended drive, specify the same retention setting in DiskXtender as on EMC Centera.

**Privileged delete**

If you have an EMC Centera Basic or EMC Centera GE, you can delete retained files by using privileged deletes. To delete retained files on a CE+ device, contact an EMC Centera technical representative.

To perform privileged deletes through DiskXtender, use the Privileged Delete option in the Explorer Add-ons utility.

*Note:* When you perform a privileged delete, and the DiskXtender Recycler is enabled, the file is permanently deleted. It is *not* placed in the DiskXtender Recycler.

When you delete a retained file through DiskXtender, you must enter an audit string. You can then view audit information by performing an EMC Centera query.

*Note:* Consider the compliance regulations followed by your company before performing a privileged delete.

**Audited delete**

When you delete a file that is stored on EMC Centera, metadata about the deleted file remains on the cluster. This metadata is called a *reflection* or *tombstone*.

Through DiskXtender, you can provide an audit string that is included in the reflection. An EMC Centera query then enables you to search for the reflection and view the audit string.

If retention has never been set for the file, or if the retention period for the file has expired, the audit string can be provided automatically by DiskXtender through the media service. The audit string enables you to identify the data as deleted DiskXtender data.

If the file is still under retention (and you are therefore performing a privileged delete through the Explorer Add-ons utility), then you must provide a custom audit string through the utility.

If you provide an audit string through the media service but you delete the file by using a privileged delete, the audit string entered for the privileged delete is used instead of the media service audit string.

An EMC Centera query enables you to search for deleted data and view the audit string. The EMC Centera documentation provides instructions on how to do this.

**Replication**

The EMC Centera replication feature protects against data corruption and loss by automatically copying data from one EMC Centera cluster to another. As an EMC Centera cluster acquires new content from an application, the replication mechanism ensures that this new content is automatically and transparently transferred across a WAN or LAN to a designated EMC Centera in another location.

Replication is used on an ongoing basis to keep two or more EMC Centera clusters synchronized with new content. In a typical replication setup, the EMC Centera clusters are geographically separate to ensure disaster recovery or to distribute the content for access from another location. For example, a company may replicate to a second EMC Centera cluster to enable recovery from the loss of the primary EMC Centera or to avoid multiple requests for the same content across a WAN connection.
The majority of EMC Centera environments with replication are configured for unidirectional replication. With unidirectional replication, one EMC Centera cluster updates another cluster with its content. For example, if content is written to cluster A, then unidirectional replication transfers the content to cluster B so that it is located on both clusters. However, if content is written directly to cluster B, the content is not transferred to cluster A. As a result, there may be additional content on cluster B that does not exist on cluster A.

The EMC Centera online help provides additional information on replication. Replication should be configured by an EMC Centera technical representative.

Replication and DiskXtender files

The replication process itself is transparent to DiskXtender. In other words, after DiskXtender migrates files to EMC Centera, the files are replicated from the source cluster to the target cluster without any DiskXtender involvement.

Replication failover

In past releases, DiskXtender supported three types of DiskXtender file behavior when the source EMC Centera cluster failed:

- Read-only failover
- Read/write failover
- No failover

Due to concerns about possible data loss, however, only read-only failover and no failover are now supported. The following sections provide details on the supported configurations, as well as an explanation of the concerns surrounding read/write failover.

Read-only failover

When the source EMC Centera cluster fails, DiskXtender automatically attempts to set the failed media service online again. If DiskXtender is unable to set the media service online, the EMC Centera SDK provides a read-only connection to the target (replica) cluster after a brief pause. With read-only failover, files can be read from the target cluster, but additional files cannot be written to the target cluster.

Once the source cluster is set online again, DiskXtender automatically resumes normal read/write activity with the source cluster.

This scenario enables users to fetch files that have already been migrated and purged, even when the source cluster fails. However, new file migration activity (from new files that qualify for migration, as well as edits to and deletes of files that have already been migrated) must wait until the source cluster comes back online.

To enable this behavior, include the connection information for only the source cluster in the media service connection string, and select the Enable Read-Only Replica Failover checkbox when configuring the media service.

Losing the read-only connection to the replica

If the DiskXtender service restarts or if the media service is set offline while DiskXtender is connected to the target, then the connection to the target fails, and the media service is set offline. Purged files cannot be fetched until the source cluster is set online again.

This is because DiskXtender passes the connection string to the EMC Centera SDK, and the connection string includes only addresses from the source cluster. If the source cluster is offline, then no connection can be made—not even to the target cluster. The address information for the target cluster is passed to DiskXtender only after a successful connection to the source cluster.
If the source cluster is offline for an extended period of time, contact EMC Customer Service. A Customer Support Representative can configure the environment to establish a read/write connection to the target cluster, and to ensure that files are replicated back to the source cluster once it is set online.

**Read/write failover**
Read/write failover, where DiskXtender both reads files from and writes files to the target cluster if the source cluster fails, is no longer supported due to concerns about possible data loss. If a failover occurs and files are written to the target cluster, then the files are not replicated back to the source cluster in a unidirectional replication environment, which includes the majority of replication environments. As a result, if the target cluster is removed from the environment, then the files that were written only to the target cluster are lost.

**No failover**
You can configure DiskXtender so that no failover to the target cluster occurs. In other words, files can neither be read from nor written to the target cluster. Both file fetches and file migration are disabled. Users can only access migrated files that were fetched prior to the failover.

To enable this behavior, include the connection information for only the source cluster in the media service connection string, and clear the Enable Read-Only Replica Failover checkbox when configuring the media service.

DiskXtender continues to attempt to set the media service back online until it is successful. Until then, the media service and its media remain offline.

**Replicate Delete**
If you use EMC Centera replication and you delete file data from an extended drive, you can choose whether the file data is deleted from only the source cluster or from all eligible clusters (including both the source cluster and all target clusters).

When you delete file data from the extended drive and the EMC Centera Replicate Delete feature is enabled, the file is deleted from the source cluster. The delete transaction is then placed in a queue, and eventually carried out on the target clusters. Replicate Delete is also known as delete propagation.

When you enable Replicate Delete, the file data on all replicated clusters remains more closely synchronized.

---

**Note:** When Replicate Delete is disabled, content deleted from the source cluster is not deleted from the target. This may be appropriate in some circumstances, but will result in uneven capacity utilization.

**Synchronous deletion**
DiskXtender also enables you to control delete propagation to the target EMC Centera clusters.

If you need deletions to occur almost simultaneously on both the source and target clusters, you can configure synchronous deletion through DiskXtender. When synchronous deletion is enabled, DiskXtender processes each file deletion on all eligible clusters.

**Note:** If one or more of the clusters is not available, then the file deletion fails and an error occurs. When DiskXtender synchronous deletion is enabled, all eligible clusters must be available for a deletion to succeed.
Enable synchronous deletion through DiskXtender only if the timing of delete transaction processing on the target clusters is important. Synchronous deletion may result in performance degradation when you delete files from the extended drive. This is because DiskXtender must process the deletion on all eligible clusters instead of on just the source cluster.

If the timing of delete transaction processing on the target clusters is not important, enable only the EMC Centera Replicate Delete feature. This enables EMC Centera to process the deletion as system resources are available.

To configure synchronous deletion through DiskXtender, use the **Enable synchronous deletes on replicated Centeras** option, which is available on the **Options** tab of the **Service Properties** dialog box.

If you enable synchronous deletion through DiskXtender, you should enable EMC Centera Replicate Delete as well. Enabling both features provides additional assurance that the file is deleted on all eligible clusters. This is because EMC Centera may be able to delete the file even if DiskXtender is unable to do so.
Network-attached storage

DiskXtender considers network attached storage (NAS) media to be any media available through a connection to a share on a network, including:

- A network share on a standard disk-based storage device, such as CLARiiON, Celerra, Symmetrix®, or other RAID and NAS devices.
- RAID devices are storage devices that contain several high-capacity magnetic drives and manage storage of data to those drives in a way that is seamless to the user.
- NAS devices use an operating system (like Microsoft Windows) to function as the file system control that tracks the location of files within the NAS device.
- A shared folder on a server on the network.
- A shared media folder on another DiskXtender extended drive. The second extended drive must be located on a separate DiskXtender server. You cannot migrate files from a media folder on one extended drive to a location on the same extended drive.

NAS media is considered virtual media because it does not correspond directly to a specific piece of media (like a tape cartridge). However, it does correspond to a specific location (the share) on a magnetic drive.

When DiskXtender writes to NAS media, it is essentially copying files over the network from the extended drive to the shared location.

DiskXtender does not impose a limit on the size of NAS media. The size of each piece of NAS media depends on the size of the partition on which the share is located.

When you connect DiskXtender to a share on a NAS device by creating a piece of NAS media, you must choose the type of media you are creating. Table 10 on page 67 lists the available options.

<table>
<thead>
<tr>
<th>NAS media type</th>
<th>Type of share</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Standard NAS&quot; on page 67</td>
<td>Standard NAS share on a disk-based storage device or server on the network</td>
</tr>
<tr>
<td>&quot;Aggregate NAS&quot; on page 67</td>
<td>Media folder on another DiskXtender extended drive as part of tiered migration</td>
</tr>
<tr>
<td>&quot;Retained NAS&quot; on page 68</td>
<td>Standard share on a retention-capable NAS device</td>
</tr>
</tbody>
</table>

Standard NAS

Standard NAS media can be created for any network share on any type of disk-based device, like a RAID or a NAS device, or a server drive on the network.

DiskXtender treats standard NAS media like any normal read/write magnetic media. There are no restrictions on editing or deleting files, or renaming files or folders.

Aggregate NAS

Aggregate NAS is designed to be used in a tiered migration environment, in which you are aggregating files before moving them (a second time) to tape. Files are migrated from one DiskXtender extended drive to another extended drive, and then from the second extended drive to tape, as shown in Figure 10 on page 68.
To accomplish this through DiskXtender, media folders on the second extended drive are configured as Aggregate NAS media on the first DiskXtender server. The files from the first extended drive are migrated to the Aggregate NAS media. The DiskXtender installation on the second server then moves the files to tape media.

When files are saved to a media folder on the first extended drive that contains a media group with Aggregate NAS media, DiskXtender does not allow you to rename the files or the folders in which they reside. This behavior mimics the behavior of the second extended drive (the Aggregate NAS media), because the second extended drive is writing to tape, which also does not allow file or folder renames.

The restrictions of Aggregate NAS media are designed to ensure that files and file tags on both extended drives remain synchronized, and that the files on the subsequent tape media are not orphaned.

Note: DiskXtender does not restrict you from using the second extended drive to write to media other than tape. However, Aggregate NAS media restricts file and folder renames, operationally imitating extended drives that write to tape media.

Retained NAS

Some NAS devices can be configured to contain variable retention volumes, including a Celerra Network Server with the File Level Retention (FLR) file system and Network Appliance (NetApp) NAS devices with SnapLock software.

With these retention-capable volumes, you can set retention on files written to the volumes. Through DiskXtender, you can apply a retention period automatically to files that qualify for move rules that write to these volumes.

When DiskXtender applies a retention period to a file, the file cannot be edited or deleted from the extended drive until the retention period expires. You also cannot change the retention period that has been applied to a file until the original retention period expires.
When the file is moved to media, the retention period you set through DiskXtender move rules is passed to the retained NAS device. As a result, the file is also protected on the NAS device until the retention period expires.

Because retention periods are passed from DiskXtender to the retained NAS, do not configure retention through the NAS device. Instead, configure retention through DiskXtender.

**Note:** You cannot create a piece of retained NAS media unless you are using a supported device: either Celerra with FLR or NetApp with SnapLock. If you select the Retained NAS option when creating NAS media for a share that does not reside on a supported device, then DiskXtender automatically converts the media to the Standard NAS media type.

To write to a retention capable device share without using retention, use the Standard NAS option when creating the NAS media that corresponds to the share.

**Limitations for filepath lengths**

There is a limit to the total length allowed for a path and filename on both the extended drive and on NAS media.

When you save or edit a file on the extended drive, the full path and filename can total as many as 259 UTF-16 characters.

Most NAS file systems support filepaths of 259 UTF-16 characters. (Review the NAS device documentation for specific support information.) However, if DiskXtender is writing to a share on the NAS device, the character count of the full filepath on the device is included in the maximum number of characters allowed. In other words, you must consider the absolute path of the file on the device. To do this, total the character count of the path and filename on the extended drive and the full path to the share on the device.

For example, assume that there is a share called `\Server\Share` for the `\Server\Directory1\Directory2\Directory3` location on a NAS device. Assume also that `\MediaFolder\File.doc` is on the extended drive writing to a piece of NAS media for `\Server\Share`. The character count for the media derives from `\Server\Directory1\Directory2\Directory3\File.doc` and not from `\Server\Share\File.doc`.

**What happens when the filepath length exceeds the limit**

If the character count for the media path exceeds the maximum allowed by the media file system, then the file is not migrated to media. Also, a warning is written to the DiskXtender event logs. This warning continues to appear in the logs every time the file is qualified against the move rules during a background scan.

To avoid exceeding the maximum path length, ensure that the path from the NAS media share is equivalent to the absolute path. Do not create a share with a short name for a deep subfolder.

**Length limitations when restoring files from media**

Take filepath character counts into consideration when restoring files from media. The file restore may fail in the following scenario:

1. DiskXtender successfully migrates the file to media.
2. You remove the media from the media group.
3. You re-add the media to a media group in a different media folder, and the new media folder has a higher character count.

4. The combined character count of the file on the media and the new media folder exceeds the maximum allowed.

File restore may also fail if you are creating a piece of NAS media. This occurs if the share already contains files, and the character count for the filepath exceeds the maximum allowed.

If the file restore fails, a warning is written in the DiskXtender event logs.

---

**Creating the shares for NAS media**

Before you add the NAS media service in the File System Manager Administrator, prepare the shares that will be identified as NAS media.

**NAS share requirements**

The shares for NAS media should meet the following requirements:

- The shares should **not** be located at the root of the storage device. Create shares for either folders or partitions on the device.
- The shares should be visible over the network to the DiskXtender server.
- The absolute filepath (in other words, the full filepath on the device plus the filepath of any files on the extended drive) must not exceed the maximum number of UTF-16 characters supported by both DiskXtender and the device. “Limitations for filepath lengths” on page 69 provides details.
- Only the DiskXtender service account and any accounts required for backups should have full access to the share that corresponds to a piece of NAS media. No other user accounts or applications should have write access to the share. “NAS share security” on page 72 provides details on why this is necessary.
- If you use Celerra FLR, the share should be located on a Celerra disk.
- If you use a NetApp device with SnapLock, the share should be located on a drive that has been specified as a SnapLock drive.
- If you set up tiered migration, the DiskXtender administration guide provides the steps to prepare the DiskXtender installation with the media folder that will serve as a piece of Aggregate NAS media.

**Deciding how many shares to create**

Each DiskXtender installation can have only one NAS media service. However, you can create as many as 256 pieces of NAS media for that media service, and each piece of media can write to a different share on a different device, as illustrated in Figure 11 on page 71.
**Figure 11** DiskXtender with NAS

**Note:** You can create more than 256 pieces of NAS media, but no more than the maximum will be online at the same time. You cannot write files to or read files from the media that DiskXtender does not set online at initialization.

Even if the NAS media service is writing to a single device, you should create several partitions and shares so that you can create multiple pieces of NAS media. This is important for the following reasons:

- DiskXtender performance improves when the system can write to and read from multiple media at once. Focusing all system activity on a single piece of media can cause a performance bottleneck.
- You can take advantage of the flexible file migration features available in DiskXtender. You can migrate data from multiple media folders to different locations (pieces of media) by using customized migration rules.
Media Management

◆ More files remain available if an error or other system problem occurs. If a piece of media becomes inaccessible (for example, as a result of a failed transaction), the files on other pieces of media remain accessible while the inaccessible media is offline.

The number of media you should create depends on your environment and your tolerance for system downtime. For assistance in determining how many pieces of NAS media to create, contact EMC Professional Services.

NAS share security

Only the DiskXtender service account and any accounts required for backups should have full access to the share that corresponds to a piece of NAS media. No other user accounts or applications should have write access to the share.

⚠️ CAUTION
This restriction is critical to protect the data that DiskXtender manages.

If a user saves, edits, or deletes a file directly on the NAS share instead of through the extended drive, the files and file tags on the extended drive are not synchronized with the files on media. If this occurs, users will receive Access Denied errors when attempting to open those files from the extended drive.

If the file is renamed directly on the media, the file data (or file tag, if the file is purged) on the extended drive becomes orphaned.

If you ever change the account that DiskXtender uses to log on as a service, you also need to change the access permissions to any network shares that are being used as NAS media.
Removable media

Table 11 on page 73 provides details on the high-capacity, removable media types that DiskXtender supports.

<table>
<thead>
<tr>
<th>Media type</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tape and tape-WORM</td>
<td>LTO, SDLT, DLT, SAIT, AIT, 9840, and 9940</td>
</tr>
<tr>
<td>DVD</td>
<td>DVD-R, DVD-RAM, and DVD-ROM</td>
</tr>
<tr>
<td>Optical and optical WORM</td>
<td>Magneto-optical, Ultra Density Optical</td>
</tr>
</tbody>
</table>

These media types are supported through a wide variety of hardware devices. For a complete list, refer to the DiskXtender for Windows Supported Device List available on the Powerlink website.

All of the media types in Table 11 on page 73 are supported through the MediaStor media service. If you have already invested in StorageTek ACSLS, you can use the ACSLS media service in DiskXtender to migrate files from Windows computers to tape media managed by the ACSLS server.

There are a number of steps you must take to lead a piece of removable media through its lifecycle in DiskXtender. These steps include formatting and labeling the media, as well as compacting the media to reclaim wasted space and maximize storage efficiency. DiskXtender provides several features to automate the media lifecycle and simplify the media management process.

The following topics provide more information on managing removable media through DiskXtender:
- “MediaStor” on page 73
- “Sun StorageTek ACSLS” on page 75
- “Managing the removable media lifecycle” on page 77

MediaStor

MediaStor provides comprehensive drive and library management capabilities for retrieving, mounting, and dismounting removable media in a variety of hardware devices. MediaStor is provided automatically with the DiskXtender product suite.

MediaStor supports standalone drives and libraries that use the following interfaces:
- SCSI
- Fibre Channel
- iSCSI (IP over SCSI)

The DiskXtender for Windows Supported Device List provides a list of the adapters you can use to connect hardware devices to the MediaStor server.

MediaStor must be installed on a server attached to the hardware devices that contain the media to use for extended storage, as illustrated in Figure 12 on page 74.
Media Management

Figure 12 File System Manager with MediaStor

MediaStor should be installed on a dedicated Windows server to maximize system performance.

If necessary, a single MediaStor installation can manage devices on behalf of multiple File System Manager installations. Alternatively, a single File System Manager installation can connect to multiple MediaStor installations, each managing one or more hardware devices.

In the MediaStor Administrator, a wizard leads you through the steps to add hardware devices to the configuration so that you can manage them and the media within them.

You can perform the following device and media management tasks by using MediaStor:

- Inventory a device
- Insert and eject media
- Move media from one shelf to another
- Allocate and deallocate media to extended drives
- Reserve library drives for media tasks, moves and fetches, or both
- Set a device offline so that you can perform maintenance or troubleshoot problems
- (Tape libraries only) Specify automatic drive cleaning options so that cleaning cartridges are mounted based on one of the following criteria:
  - Number of motion hours (read, write, or read and write) of data tapes in the drive
  - Number of times data tapes have been mounted in the drive
  - Cleaning requests from the drive
Two additional device management utilities are installed with MediaStor and are available from the MediaStor Program menu:

- Jukebox Manager provides an additional interface to inventory and manage the media in a library.
- SCSI Manager provides an interface to issue SCSI commands to monitor and troubleshoot SCSI and iSCSI devices.

ACSLS is a UNIX-based device management product that manages Sun StorageTek tape libraries and provides device sharing between applications. For ACSLS to communicate with DiskXtender, Sun StorageTek LibAttach must be installed on the DiskXtender server. LibAttach translates Windows-based product commands from DiskXtender into a syntax that the UNIX-based ACSLS understands.

The ACSLS server is connected to the device controller for one or more Sun StorageTek tape libraries. ACSLS controls the picker arm for each library device and manages retrieval of media within the library.

However, to allow device sharing, Sun StorageTek constructs some of the library devices in a way that allows individual applications to communicate directly with particular drives in a library. To enable this communication for DiskXtender, you connect the DiskXtender server and one or more drives in the Sun StorageTek library by using a SCSI cable, as illustrated in Figure 13 on page 76.
When you configure an ACSLS media service in DiskXtender, you designate the connected drives as the drives that should be used by DiskXtender. Other servers cannot access that drive.

Certain pieces of media in the ACSLS system are assigned to DiskXtender by using ACSLS.

When DiskXtender requires a particular piece of media, DiskXtender requests that media from ACSLS. The ACSLS system retrieves the media and places it in the drive connected to the DiskXtender server. DiskXtender then communicates directly with the drive, and performs all media-related tasks without any involvement from ACSLS.
Understanding the components of an ACSLS library

In a Sun StorageTek library managed by ACSLS, two or more Library Storage Module (LSM) devices can be connected by using a pass-through connection. When two or more LSM devices are connected, they are called an Automated Cartridge System (ACS).

In DiskXtender, an ACS, which contains one or more LSMs, is considered a library. When an LSM is set offline, the media within that LSM is still online in DiskXtender.

Note: If an error appears indicating that the library (in other words, the ACS) is offline when DiskXtender tries to mount a piece of media in an LSM, clear the error state. This will bring the media back online even if the LSM is offline.

Managing the removable media lifecycle

The following steps outline the required lifecycle phases for a piece of blank, removable media in DiskXtender.

The steps assume that the media service is already configured in DiskXtender to provide access to the hardware device.

1. Insert the media into the hardware device and inventory it, if necessary.
   Once the media is inventoried, it can be recognized by DiskXtender.

2. Allocate the media to an extended drive.
   When you allocate media, the media is assigned for use only by that extended drive.

3. Ensure that the media is formatted with a supported file system and labeled:
   • If the media is blank, format and label the media.
   • If the media has already been formatted with a supported file system, label the media.
   • If the media has been formatted with a file system that is not supported, reformat the media and then label it.

   The formatting of media verifies the integrity of a piece of removable media, and makes it available for use with system hardware. It prepares the media for file writes by creating the specified file system on the media. When you label a piece of media, you assign a name and serial number to the media so that DiskXtender can track it.

   There are several ways to format and label media in DiskXtender. The most efficient method depends on the status of the media and the number of pieces of media that need to be formatted and labeled:
   • You can format and label multiple pieces of unformatted media at once by using the Media Prepare Manager.

   Note: The Media Prepare Manager is available only for media in a library configured through the MediaStor media service.

   • You can format and label a single piece of unformatted media by assigning the Format and Label media tasks to the media.
You can format but not label a single piece or multiple pieces of unformatted media, assign a Format media task to the media. You can then enable automatic labeling of the media through a media group, or you can label the media individually later by assigning a Label media task.

You can label a single piece of blank media by assigning a Label media task.

You can set up automatic labeling and addition of blank media to a media group automatically through the media group settings.

4. **Add the media to a media group.**

   This is the final step in preparing a piece of media for file migration.

5. **Migrate files to the media by configuring move rules that point to the media group and setting the Move Files to Media schedule.**

   When the media is full, files are no longer written to the media. However, the media remains in the media group so that users can continue accessing files on the media. Full media appears with a blue label in the File System Manager Administrator.

6. **(Optional) To reuse the media, compact and reformat the media.**

   When media is compacted, files on the media are copied back to the extended drive and then re-migrated to a new piece of media. The media is also automatically removed from the media group. You can then reformat the media and reuse it.

   Compaction can happen automatically (based on media group automation settings) when the amount of wasted space on the piece of media exceeds a specified percentage. You can also assign a media task to compact a piece of media when necessary.

7. **(DVD-R only) To stabilize DVD-R media once it is full, finalize the media.**

   Finalization is also required before you can purge files that have been migrated to the DVD-R media.

   Finalization can happen automatically (based on media group settings) when the media is full, or you can assign a media task to finalize the media when necessary.

8. **(Optional) If you no longer need the files that have been migrated to the media, or if you want to move the files to a different piece or type of media, remove the media from the media group. There are two ways to remove media from a media group:**

   - To copy the files on the media back to the extended drive and move the files to other media, compact the media. The media is automatically removed from the media group during compaction.
   - To remove the files on the media from the extended drive altogether, remove the media from the media group.

9. **(Optional) Deallocate the media from the extended drive, and delete it from the media service.**

10. **(Optional) Remove the media from the hardware device.**
Media file systems

DiskXtender can write files to and read files from removable media that is formatted with either the OTG file system or the UDF file system. Table 12 on page 79 lists the file systems that DiskXtender supports for each type of media.

<table>
<thead>
<tr>
<th>Media type</th>
<th>Supported file systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>DVD-R and DVD+R</td>
<td>UDF</td>
</tr>
<tr>
<td>DVD-RAM</td>
<td>• OTG</td>
</tr>
<tr>
<td></td>
<td>• UDF</td>
</tr>
<tr>
<td>Magneto-optical (MO)</td>
<td>• OTG</td>
</tr>
<tr>
<td></td>
<td>• UDF</td>
</tr>
<tr>
<td>MO WORM</td>
<td>• OTG</td>
</tr>
<tr>
<td></td>
<td>• UDF</td>
</tr>
<tr>
<td>Tape</td>
<td>OTG</td>
</tr>
<tr>
<td>Tape-WORM</td>
<td>OTG</td>
</tr>
<tr>
<td>UDO (UDO1, UDO2)</td>
<td>• OTG</td>
</tr>
<tr>
<td></td>
<td>• UDF</td>
</tr>
<tr>
<td>UDO WORM (UDO1 WORM, UDO2 WORM))</td>
<td>• OTG</td>
</tr>
<tr>
<td></td>
<td>• UDF</td>
</tr>
</tbody>
</table>

Note: DVD-ROM can only be read by DiskXtender if it is written by using the UDF file system. DVD-ROM must be created in another system. DiskXtender cannot write to DVD-ROM.

OTG file systems

OTG file systems are installed with DiskXtender and are optimized for DiskXtender media performance. Table 13 on page 79 lists the two subsystems for the OTG file system and the media types that support them.

<table>
<thead>
<tr>
<th>Subsystem</th>
<th>Media types</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSS (Optical Storage Subsystem)</td>
<td>• MO</td>
</tr>
<tr>
<td></td>
<td>• MO WORM</td>
</tr>
<tr>
<td></td>
<td>• UDO</td>
</tr>
<tr>
<td></td>
<td>• UDO WORM</td>
</tr>
<tr>
<td></td>
<td>• DVD-RAM</td>
</tr>
<tr>
<td>TSS (Tape Storage Subsystem)</td>
<td>• Tape</td>
</tr>
<tr>
<td></td>
<td>• Tape-WORM</td>
</tr>
</tbody>
</table>

OTG file systems are sequential, which means that files are written contiguously from the beginning to the end of each piece of media, with single-seek read and write access. As a result, runtime overhead is very low and data is sequentially organized, which enhances overall performance.

When you edit a file that has been written to media formatted with an OTG file system, DiskXtender does not "go back" to edit the file data on the media. Instead, when a file is edited, the file is written as a new file to the next blank area on the media, and the file tag on the extended drive is updated to point to the new file. The
old file data remains on the media, but is orphaned. The only exception to this is when a file is renamed on rewritable media. In that case, the file trailer on the media, where the filename is kept, is updated to reflect the new filename.

When you delete a file that has been written to media that has been formatted with the OTG file system, the file and its data are only deleted from the extended drive. They are *not* removed from the media. Deleting the file on the extended drive removes the file tag, which contains the location information for the file on the media. Without the file tag, DiskXtender can no longer track that file on the media (even though the data is still there), and the file on the media is orphaned.

**UDF file systems**

DiskXtender meets the specifications (version 2.01) laid out for the UDF (Universal Disk Format) file system by the Optical Storage Technology Association (OSTA), a nonprofit international trade association. For more information on OSTA, refer to the OSTA website, www.osta.org.

UDF is intended to enable file interchange between different operating systems.

There are two types of UDF file systems: overwritable and sequential. Table 14 on page 80 lists the two UDF file systems and the media types that support them.

<table>
<thead>
<tr>
<th>UDF file system</th>
<th>Media types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overwritable</td>
<td>• MO</td>
</tr>
<tr>
<td></td>
<td>• UDO</td>
</tr>
<tr>
<td></td>
<td>• DVD-RAM</td>
</tr>
<tr>
<td>Sequential</td>
<td>• DVD-R</td>
</tr>
<tr>
<td></td>
<td>• DVD+R</td>
</tr>
<tr>
<td></td>
<td>• MO WORM</td>
</tr>
<tr>
<td></td>
<td>• UDO WORM</td>
</tr>
</tbody>
</table>

By using the overwritable UDF file system, DiskXtender writes files to any available location on the media and can overwrite and delete files.

By using the sequential UDF file system, DiskXtender writes files in sequential order on the media, and does not edit files. Instead, DiskXtender adds edited files as new files to the next blank space on the media (functioning much like the OTG file system described above). In addition, when you delete a file that has been written to media formatted with the UDF sequential file system, the file and its data are only deleted from the extended drive and are *not* removed from the media. Deleting the file on the extended drive removes the file tag, which contains the location information for the file on the media. Without the file tag, DiskXtender can no longer track that file on the media (even though the data is still there), and the file is orphaned.

*Note:* When writing to media that is using the UDF file system, DiskXtender supports a shorter path and filename than the extended drive supports. DiskXtender supports 259 UTF-16 characters on the extended drive, but only 127 UTF-16 characters when writing files to media with the UDF file system.
If you use IBM Tivoli Storage Manager (TSM) as a data storage or data backup system, you can migrate files on a DiskXtender extended drive to the TSM server. TSM can subsequently move the files to storage devices managed by the TSM server.

After you create a TSM media service in DiskXtender to create the connection between DiskXtender and a TSM server, you must create virtual TSM media. The virtual media does not correspond to a physical piece of media in the TSM system, such as a tape cartridge. Instead, the virtual media is designed to simulate divisions of the larger repository (the TSM server) and corresponds to a filespace on the TSM server. The maximum size of a piece of virtual TSM media is 256 GB. This enables you to take advantage of the flexible file migration features available in DiskXtender.

The TSM server manages the actual physical removable media in the storage device attached to the TSM server. Tasks like formatting, labeling, and copying media in the storage device attached to the TSM server are performed by TSM rather than by DiskXtender.

To use TSM as a DiskXtender media service, the TSM Backup/Archive Client must be installed and configured appropriately on the DiskXtender server. DiskXtender then communicates with the TSM server by using an RPC connection, as illustrated in Figure 14 on page 81.

![Diagram of DiskXtender with Tivoli Storage Manager](GEN-000944)
The following topics provide more information on the DiskXtender functions that enable you to monitor, diagnose, and troubleshoot the system:

- Monitoring service events, errors, and warnings....................................................... 84
- Monitoring file activity................................................................................................... 84
- Monitoring media ........................................................................................................... 85
- Monitoring licensing ..................................................................................................... 86
- Reports .............................................................................................................................. 86
- Audit logs..................................................................................................................... 87
- Remote administration .................................................................................................. 87
Monitoring service events, errors, and warnings

DiskXtender provides built-in utilities for monitoring service events, errors, and warnings. The Event Viewer contains a listing of all DiskXtender events, errors, and warnings. This information is also logged to event logs. Errors and warnings are logged automatically, while DiskXtender must be configured to log other events.

The Event Viewer and event logs provide a quick look at DiskXtender activities. Logs can help identify and solve potential problems during runtime that might otherwise become critical problems if ignored.

If you receive an error, the DiskXtender error lookup feature enables you to quickly translate the error codes provided.

A visual indicator appears in the Administrator window when a warning or error occurs. The Event Viewer icon on the toolbar changes from an informational icon to a triangular caution symbol to indicate a warning or an exclamation point to indicate an error, as illustrated in Table 15 on page 84.

In addition, the number of errors and warnings since the service was last started is listed in the status bar at the bottom of the Administrator.

For further notification, you can configure automatic communication of warnings and errors through email alerts.

<table>
<thead>
<tr>
<th>Event Viewer toolbar icon</th>
<th>Toolbar icon for warnings in the Event Viewer</th>
<th>Toolbar icon for errors in the Event Viewer</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Information" /></td>
<td><img src="image" alt="Warning" /></td>
<td><img src="image" alt="Error" /></td>
</tr>
</tbody>
</table>

Monitoring file activity

You can monitor statistics in the File System Manager Administrator for the number of files that are pending migration, purge, and indexing. You can also monitor statistics that indicate how many files have already been migrated, purged, deleted, and submitted for indexing. These statistics enable you to verify that these file activities are occurring.

**Note:** Indexing statistics are only available if you use the DiskXtender Search Module and you enable indexing for the extended drive.
Monitoring media

The following topics provide information on the DiskXtender options available to monitor media and clear errors when they occur.

Media status indicators

The label for each piece of media automatically changes color in the tree view of the Administrator depending on its status, as listed in Table 16 on page 85.

<table>
<thead>
<tr>
<th>Media color</th>
<th>Media status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Black</td>
<td>Online</td>
</tr>
<tr>
<td>Green</td>
<td>Online but with a task pending, in progress, or suspended</td>
</tr>
<tr>
<td>Blue</td>
<td>Full</td>
</tr>
<tr>
<td>Red</td>
<td>Error</td>
</tr>
<tr>
<td>Yellow</td>
<td>Offline</td>
</tr>
</tbody>
</table>

Media task queue

If you assign media tasks to multiple pieces of media, you can monitor the status of the tasks by using the Media Task Queue Manager.

If necessary, you can stop or abort a media task that is currently in progress.

You can also remove pending tasks for a piece of media from the media task queue. When all tasks are deleted from a piece of media, the media is removed from the media task queue.

Media logs

DiskXtender maintains a log of activity for each piece of media. These logs are useful for viewing task-processing information and error codes/status for failed tasks.

Media properties

The Media Properties dialog box enables you to view detailed information about a piece of media, including the type, file system, location, number of files, amount of free and used space, number of file reads, writes, and errors, and the status of a media task, if one is in progress.
Monitoring licensing

As files are added to the extended drive for DiskXtender to manage, you should regularly monitor the DiskXtender license to ensure that you do not exceed the capacity allotted by the license.

If you exceed the storage capacity of the license, a 90-day grace period commences. You must update the license with additional storage capacity before the grace period expires. Otherwise, file migration is disabled. Contact the EMC Licensing Support team for assistance with updating the license.

You can monitor license usage for a single DiskXtender installation from the File System Manager Administrator. The License Server Administrator enables you to monitor total license usage by all DiskXtender installations.

You should also regularly review the License Server event logs to ensure that the License Server service and the licenses it manages are healthy and available to the DiskXtender servers that rely on them.

Reports

The DiskXtender reporting feature is a useful tool for tracking system statistics. Table 17 on page 86 lists the reports available in DiskXtender.

<table>
<thead>
<tr>
<th>Report name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extended Drive Information</td>
<td>Displays information about the extended drives you select, including properties and assigned media. Full reports also display additional information, including schedule information, metadata export statistics, move statistics, and fetch statistics.</td>
</tr>
<tr>
<td>Media</td>
<td>Includes information on the selected media, either as a summarized list or a detailed description of properties. Information displayed in the detailed report includes location information, total used/free space, and read/write/mount statistics.</td>
</tr>
<tr>
<td>Media Files</td>
<td>Provides information about the files on the selected pieces of media. Note: You can also run a file report for a selected group of files rather than for a piece of media by using the Explorer Add-ons.</td>
</tr>
<tr>
<td>Media Services</td>
<td>Provides information on the media services configured on the selected DiskXtender servers.</td>
</tr>
<tr>
<td>Media Tasks</td>
<td>Displays a list of media tasks that are pending, are in progress, or that have failed for selected media on the selected extended drives.</td>
</tr>
<tr>
<td>Product Registry Information</td>
<td>Provides a complete listing of all information contained in the Microsoft Windows registry about the DiskXtender service on the selected servers.</td>
</tr>
</tbody>
</table>
Audit logs

An audit log is a secure log file that functions independently of the existing DiskXtender logs (event and warning logs) and Windows system logs.

The purpose of the audit log is to provide a secure, access-controlled means for monitoring "change" events to the DiskXtender service, and whether each event succeeds or fails.

An audit log enables you to monitor important DiskXtender events, including:

- Addition, editing, and deletion of configuration objects (extended drives, media folders, media groups, rules, and so on)
- Media management tasks
- Service stops and starts

Audit logging is automatically enabled when you install or upgrade DiskXtender. You can control access to the audit log and its configuration settings by managing the membership of the DiskXtender security groups on the DiskXtender server.

The performance impact caused by audit logging is minimal. However, you can disable the audit log, if necessary.

You can also clear the audit log, or export the audit log to a tab-delimited text file so that the data can be moved into a spreadsheet or database application for additional analysis.

Remote administration

You can administer a DiskXtender installation or a MediaStor installation from the servers on which the components are installed, and from remote computers.

On servers where the components are installed, you can use the Administrator interface that is installed with the components. If there are multiple DiskXtender installations in the environment, you can administer all of them from the Administrator interface on a single DiskXtender server. The same is true for MediaStor.

On a remote computer where neither component is installed, you can install a Remote Administrator. A Remote Administrator installation provides you with the Administrator interface and the registration capability to attach remotely to one or more networked DiskXtender or MediaStor servers.

You can provide full read/write access to the DiskXtender installation, or you can provide read-only access. With read-only access, a user with a Remote Administrator installation can monitor DiskXtender but not change any settings.

Note: You can also remotely administer DiskXtender and MediaStor by using a Windows Terminal Services client.
The following topics provide details on backing up the DiskXtender system:

- Developing a backup strategy ................................................................. 90
- Backing up the extended drive ................................................................. 92
- Ensuring storage redundancy ................................................................. 93
- Backing up the DiskXtender server ......................................................... 95
- Protecting against accidental file deletion ........................................... 96
Developing a backup strategy

DiskXtender is an archival product that stores the primary copy of a file on storage media. Because it is the primary copy of a file that resides on storage media in DiskXtender, not a backup copy of a file, it is important to establish a comprehensive backup process to make a copy of the file. This copy can be used to recover the data if it is lost.

A comprehensive backup strategy enables you to restore individual files, or even the full DiskXtender system, in the event of problems or an entire system shutdown. The strategy should protect the three basic components of the DiskXtender system:

- The extended drive, from both the accidental deletion of individual files and the more complete destruction or corruption of the entire volume
- The DiskXtender server, including the DiskXtender installation
- The hardware devices and storage media to which files are migrated

The DiskXtender administration guide discusses the considerations for implementing a regular backup process for each one of these components. It also provides guidelines for the necessary tools that are available to every DiskXtender installation for backup and restore procedures.

However, each DiskXtender environment is unique. Different hardware devices, network configurations, existing tools outside of DiskXtender, and business needs all contribute to the infinite variety of configurations that are available. It is important to take all of these variables into consideration when developing a backup strategy for your environment.

Some of the procedures discussed will not be appropriate in every environment. Additional backup procedures may even be necessary, depending on your configuration. The goal of the content in the administration guide is to provide you with the background to evaluate your own system and determine any additional points of possible failure so that you can design a strategy that meets your specific needs. If necessary, EMC Professional Services staff can assist you in choosing the appropriate backup software for your environment and developing a custom backup solution for you.

The following best practices are recommended for backing up the DiskXtender system:

- Use qualified backup software to back up each extended drive and the system drive on the DiskXtender server.
  Qualified backup software is listed in the *EMC Information Protection Software Compatibility Guide* on the Powerlink website.
- Use the Registry Log Wizard to change the location in which the DiskXtender registry backup is saved. The new location should be on a network drive that is backed up regularly.
- Enable the DiskXtender Recycler so that you can restore files that have been accidentally deleted from the extended drive.
- Ensure that there is an additional copy of the secondary storage to which you are migrating files through DiskXtender. Table 18 on page 91 provides details for each type of storage.

### Table 18  Recommended media protection methods

<table>
<thead>
<tr>
<th>Type of storage</th>
<th>Recommended protection method</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMC Centera</td>
<td>Enable EMC Centera replication to another EMC Centera cluster.</td>
</tr>
<tr>
<td>NAS</td>
<td>Use qualified backup software to back up the NAS device.</td>
</tr>
<tr>
<td>Removable media (tape or optical)</td>
<td>Create copies of each piece of media by using the DiskXtender Copy Media Manager, or configure multi-target migration to another type of media.</td>
</tr>
<tr>
<td>TSM</td>
<td>Follow recommended TSM backup practices.</td>
</tr>
</tbody>
</table>

**Note:** Ensuring high availability of the DiskXtender system through the use of Microsoft clustering or AutoStart is discussed in the DiskXtender installation guide. Replicating the extended drive through products like RepliStor®, Symmetrix Remote Data Facility (SRDF®), or MirrorView™ is also covered in the DiskXtender installation guide.
Backing up the extended drive

Most backup applications, including all of the applications supported for use with DiskXtender, are capable of backing up a file on the extended drive and its metadata, including the extended attributes (EAs) that DiskXtender uses to store migration information. If a file is restored to the extended drive without its extended attributes, then DiskXtender treats the file as a new file and migrates it again.

When backup software is EA-aware, backup performance is improved. This is because the backup software can back up file tags for managed files on the extended drive.

**Note:** Even if the backup software you are using is capable of successfully backing up file tags, you may want to back up a full version of each file before it is migrated and purged to ensure that there is a full copy of each file available in one of your backup sets.

DiskXtender also supports several snapshot backup applications, such as Microsoft Windows 2003 Volume Shadow Copy Services (VSS) and NetWorker SnapImage™ Module for Microsoft Windows. Qualified snapshot backup software, which is EA-aware, takes a snapshot of the extended drive at a certain point in time. A backup application such as NetWorker can then create a backup that reflects the state of the drive at the time of the snapshot. So, if a snapshot backup begins at 8 P.M. and a file changes at 8:30 P.M. while the backup is still in progress, then the change to the file is not included in the snapshot backup that started at 8 P.M. It must be included in the next backup set.

When backup software is not EA-aware, such as IBM Tivoli Storage Manager, file tags are backed up as zero byte files, and the migration information for a file is not captured. Therefore, if you restore a zero-byte file from backup, the file is re-migrated, and data loss can occur. To prevent this situation, you must include the full file data in each backup. Purged files must be read from media so that they can be included in the backup. This slows system performance and requires more disk space for the backup set.

If you use backup software that does not support EAs, there are specific steps you must take to minimize the performance impact and ensure that you do not encounter data loss by restoring incomplete files.

The DiskXtender metadata export feature can be used to supplement backups from software that is not EA-aware. Metadata exports capture the file migration information that cannot be captured by backup software that is not EA-aware.

If necessary, EMC Professional Services staff can assist you in choosing the appropriate backup software for your environment and developing a custom backup solution for you.
Ensuring storage redundancy

The following topics provide recommendations for ensuring redundancy of the media to which files on the extended drive are migrated.

Copying removable media

To back up all removable media types supported by the MediaStor (tape or optical) and Sun StorageTek ACSLS media services (tape), you can create a copy of each piece of media. Copy media are media that are being used as copies, or backups, of original media on the extended drive. If an original piece of media becomes unreadable, the copy of the media can be promoted to original status (after the original is removed from the system).

Copy media has the same label as the original it corresponds to, but it has a unique serial number. However, as soon as the copy is promoted to original, the serial number on the copy is changed to match the serial number that was on the original.

DiskXtender provides two ways to create copy media:

- The Copy Media Manager enables you to create copies of multiple pieces of media at one time.
- The Label Copy media task enables you to create a copy of a single side of a single piece of media, or if you need to copy from a standalone drive to a library drive or vice versa, or between two stand-alone drives.

If necessary, you can even create and maintain off-site copies of original media for disaster recovery.

When the Update Copy Media schedule for an extended drive is active, DiskXtender evaluates each copy against its original to determine whether any updates should be made to the copy. DiskXtender searches for the number of sectors written, and knows how much of the media it has left to copy. If updates are required, DiskXtender updates the copy. When DiskXtender updates a piece of copy media, it copies the data from the original media to the copy. In other words, files are not fetched to the extended drive during a copy update.

If the copy is of DVD media and the original is finalized, DiskXtender automatically finalizes the copy as soon as the update of the copy is complete.

If a piece of original media becomes corrupt, you may be able to repair the media by using a Check Disk media task. However, if you cannot repair the media, you can replace the original with the copy by promoting the copy to original status.

Replicating EMC Centera

The EMC Centera replication feature protects against data corruption and loss by automatically copying data from one EMC Centera cluster to another. As an EMC Centera cluster acquires new content from an application, the replication mechanism ensures that this new content is automatically and transparently transferred across a WAN or LAN to a designated EMC Centera in another location. “Replication” on page 63 provides additional information on replication.

Backing up NAS

Use dedicated backup software to back up files on the NAS device shares configured as NAS media in DiskXtender. Because the full file data (and not file tags) are stored on the shares, the extended attribute restrictions that apply to backing up the extended drive do not apply to backing up NAS.

Full and incremental backups of the NAS shares should be performed on a regular basis according to your company’s recommended backup policies.
IMPORTANT
Only the DiskXtender service account and any accounts required for backups should have full access to the share that corresponds to a piece of NAS media. No other user accounts or applications should have write access to the share.

Backing up TSM
Follow recommended TSM procedures to back up the TSM system, including the TSM server and client configuration, as well as the media to which the TSM server ultimately writes.

Multi-target migration
Regardless of the type of media you are using, you can ensure redundancy of files on media by migrating files on the extended drive to multiple pieces of media with the DiskXtender multi-target migration feature. With multi-target migration, you can migrate a single file to different pieces, and different types, of media at the same time.
Backing up the DiskXtender server

In addition to backing up the files on the extended drive, you should perform regular backups of the rest of the DiskXtender server, including the system drive and the DiskXtender configuration itself, which is stored in the Microsoft Windows registry. The following topics provide details.

You should also record the following information in a document dedicated to backup and restore procedures:

- The name of the servers on which DiskXtender is installed
- The version of the operating system on the DiskXtender servers
- The size and drive letter of each partition
- The volume serial number for each partition (extended drive)

This information is necessary to restore the server in the event of a total system failure.

Backing up the system drive

Use a dedicated backup tool to back up the system drive on the DiskXtender server according to your company’s backup policy.

Backing up DiskXtender registry settings

To back up the DiskXtender configuration for either File System Manager or MediaStor, you need to back up the DiskXtender settings that are stored in the Microsoft Windows registry. The Registry Log Wizard, available in both the File System Manager Administrator and the MediaStor Administrator, enables you to do this.

For virtual media such as TSM and EMC Centera, the registry log backup is especially important because virtual media is defined through the File System Manager configuration. In the event of system failure, it is most efficient to restore that configuration to access and restore, if necessary, files on the media.

The registry log is automatically updated every hour. DiskXtender saves one registry log per server per day for each of the last seven days. The registry log file with the most recent (hourly) updates is named DiskXtender.rlog (for File System Manager) or MediaStor.rlog (for MediaStor). The registry log file for each of the last seven days is named DiskXtender_mm_dd_yyyy.rlog or MediaStor_mm_dd_yyyy.rlog, respectively, where mm_dd_yyyy represents the date the file was created.

By default, the registry log is saved to a folder in the DiskXtender installation directory. You should designate a different location in which to store the registry log files by using the Registry Log Wizard. The registry log should be stored at a network location. In addition, you should archive the registry log files as you would any other backup data for disaster recovery.

**Note:** Each DiskXtender installation creates its own registry log file. You cannot restore a registry log file from one server to another server in order to move or reuse a DiskXtender configuration. The server to which you are restoring a registry log file must have the same name as the server from which the registry log file was generated. In addition, you must restore a registry log file to a DiskXtender installation that is using the same release as the one that was used to create the registry log file.
Protecting against accidental file deletion

You can prevent users from accidentally deleting files from the extended drive by controlling access to the files, setting the read-only attribute for the files, or by setting retention on the files.

For environments where these methods are not appropriate, however, you can enable the DiskXtender Recycler, which allows you to restore files that have been accidentally deleted. You may also be able to restore files from backup sets if you use a qualified backup tool.

Preventing users from deleting files

Microsoft Windows provides several options to control access to and protect files on an NTFS volume. To protect files from unauthorized access by users, you can create network shares on the extended drive for certain media folders, and then restrict the users who can access the shares. You can also specify security at the file and folder level on the extended drive. Alternatively, you can set the Read-only attribute on a file to prevent it from being edited or accidentally deleted. The Microsoft Windows documentation provides details on these security options.

If the files on the extended drive are critical enough that they require absolute protection, then you can prevent users from deleting the files by setting retention on the files. File retention is available when you migrate files to either EMC Centera or a share on a supported NAS device with retention software installed.

Enabling the DiskXtender Recycler

The DiskXtender Recycler for each extended drive functions similar to the Microsoft Windows Recycle Bin, but only affects files on a drive extended through DiskXtender.

The DiskXtender Recycler is designed to protect against accidental deletion of files on the extended drive. When a user deletes a file from the extended drive and the Recycler is enabled, the file is placed in the Recycler instead of being permanently deleted. You can then restore files from the Recycler, if necessary.

Note: Files deleted according to delete rules or by using EMC Centera privileged deletes are not placed in the Recycle Bin.
The following topics provide details on DiskXtender interoperability with other products:

- DiskXtender as an application back end ............................................................ 98
- High availability .................................................................................................. 99
- Replication .......................................................................................................... 101
- Anti-virus software interoperability ................................................................. 102
- DiskXtender on VMware .................................................................................. 102

Details on the supported versions of these products are listed in the *EMC Information Protection Software Compatibility Guide* available on the Powerlink website.
DiskXtender as an application back end

Installing DiskXtender enables you to extend the capacity of drives that serve as the primary repository for files generated by mission-critical applications, ApplicationXtender. You can also customize integration with DiskXtender by using the DiskXtender SDK.

Documentum ApplicationXtender

Documentum ApplicationXtender electronically stores, organizes, and manages documents, files, and other business-critical information. ApplicationXtender then provides fast, security-controlled access to the files from Microsoft Windows or web-based clients.

You can use DiskXtender to extend the storage capacity of the ApplicationXtender document storage server.

ApplicationXtender can connect to a DiskXtender extended drive by using Windows shares or Distributed Component Object Model (DCOM).

The DiskXtender administration guide provides details on configuring DiskXtender to store ApplicationXtender documents.

Custom integration through the DiskXtender SDK

The DiskXtender SDK provides application developers with client access to DiskXtender administration and event notification capabilities.

The DxDmClient application programming interface (API) provides a programming interface to DiskXtender administrative functionality by using RPC. Through the API, you can issue DiskXtender server management calls, including calls to create and manage the following items:

- Media services
- Extended drives
- Media
- Media groups
- Rules
- Reports
- Schedules
- Metadata exports and registry log configuration

This direct integration capability enables application developers to customize the way their application files are stored and managed in DiskXtender.

The DiskXtender SDK requires DiskXtender for Windows and Microsoft Visual Studio version 6.0 (for C and C++ development) or Microsoft Visual Studio .NET. Both Unicode and ANSI character sets are supported.

The DiskXtender API reference guide provides additional details on installing and using the DiskXtender SDK.
High availability

You can use Microsoft clustering, AutoStart, or EMC PowerPath® to maximize DiskXtender availability in a nonstop business environment.

Microsoft clustering

The DiskXtender File System Manager component can be installed in a Microsoft clustering environment on as many as eight nodes. The shared storage drives in the cluster, which are connected to each cluster node, are the drives that you extend through DiskXtender.

The DiskXtender installation can be either active or passive on a cluster node. An active installation is a standard DiskXtender installation with the Administrator interface, the DiskXtender service, an active filter driver, and one or more extended drives that are connected to all cluster nodes. A passive installation is a full DiskXtender installation where the DiskXtender service and the filter driver are not active. A passive installation becomes an active installation if an active installation fails over to the node with the passive installation.

An active DiskXtender installation can fail over to either another active DiskXtender installation or a passive DiskXtender installation.

The DiskXtender installation guide provides additional details on configuring DiskXtender in a cluster.

AutoStart

The DiskXtender File System Manager component can also be installed in an AutoStart domain. DiskXtender can write to an EMC Centera cluster or NAS shares when it is installed in an AutoStart domain. The DiskXtender installation must be active on all nodes on which it is installed in the domain.

The nodes in the AutoStart domain can be either local or remote.

If the nodes are local, then the extended drives are connected to all nodes. When a failover occurs, control of the extended drives on the failed node moves to an activeDiskXtender installation on a standby node.

If the nodes are remote, then SRDF is used to replicate the extended drives in one location to the extended drives in another location. When a failover occurs, the AutoStart node alias no longer points to the failed node. Instead, it points to the replicated extended drive on the DiskXtender installation in a remote location.

The DiskXtender installation guide provides additional details on configuring DiskXtender in an AutoStart domain.

PowerPath

PowerPath for Windows provides automatic failover and dynamic multipath load balancing for the I/O components in a SAN that connect a DiskXtender server and the PowerPath supported device it is using as an extended drive:

- **Automatic failover** — PowerPath enhances availability by eliminating the I/O path as a point of failure. It can compensate for failure of any of the I/O components, including HBAs, the interface or interface port, or the Fibre Channel hub or switch.

- **Load balancing** — PowerPath also tries to maintain maximum performance and reduce management through dynamic load balancing. It uses all paths at all times by distributing I/O requests to a logical device across all available paths.
Supported PowerPath devices include but are not limited to Symmetrix and CLARiiON.

**Note:** PowerPath and DiskXtender integration is also supported in a Microsoft cluster or in an AutoStart domain.

To use DiskXtender with PowerPath, you should install PowerPath on the DiskXtender server, which is connected to a switch by using at least one Fibre Channel HBA. A minimum of two HBAs are recommended.

A PowerPath supported storage device, such as Symmetrix or CLARiiON, is also connected to the switch through a single connection point, and serves as the extended drive for the DiskXtender server.

Depending on the level of fault tolerance required, you can also include multiple switches.
Replication

You can replicate files on the DiskXtender extended drive from one server to another by using one of the following EMC replication products:

- RepliStor can replicate files on a Windows server.
- SRDF can replicate files on a Symmetrix device.
- MirrorView can replicate files on a CLARiiON device.

General Microsoft Windows replication with RepliStor

RepliStor provides high availability and continuity through real-time data replication for Microsoft Windows data across LAN and WAN environments.

RepliStor can replicate files from an extended drive on one DiskXtender server to an extended drive on another DiskXtender server. If the source server becomes unavailable, the target server can begin receiving and managing DiskXtender file requests.

The DiskXtender installation on the target server can be passive and serve only as a replication target. The DiskXtender installation can also be active with additional extended drives that are receiving files and migrating them to media.

RepliStor does not replicate DiskXtender extended attributes or file tags. Instead, RepliStor replicates the actual file. Remember this when you determine the amount of disk space necessary on the target server. You might want the target server to have an active installation so that you can configure file migration and purging on the target server as well.

To minimize unnecessary replication, RepliStor does not forward any file modifications that result from migrating, purging, or fetching a file.

The DiskXtender installation guide provides additional details on system architecture and requirements, as well as how to install and manage DiskXtender with RepliStor.

Replicating an extended drive on a CLARiiON or Symmetrix device

MirrorView is a limited-distance, remote mirroring facility for Celerra configurations with CLARiiON backend storage systems. MirrorView maintains copies of data on CLARiiON devices at different locations.

SRDF enables you to maintain multiple, host-independent, mirrored copies of data on a Symmetrix device. The Symmetrix systems can be in the same room or in different locations.

If the DiskXtender extended drive is on a CLARiiON or Symmetrix device, you can use MirrorView or SRDF, respectively, to create and maintain remote replicas of the extended drive from a device at a primary data center to another device at a disaster recovery site.

With either MirrorView or SRDF, DiskXtender is installed and actively managing files on the server at the primary data center. DiskXtender is also installed on the server at the disaster recovery site. However, the service is stopped. In other words, DiskXtender is passive at the disaster recovery site. If a failure occurs at the primary data center, you can manually fail over to the disaster recovery site. When the primary data center comes back online, you can restore operations there.
Interoperability

The DiskXtender installation guide provides additional details on system architecture and requirements, as well as how to install and manage DiskXtender with MirrorView.

Anti-virus software interoperability

If you plan to use anti-virus software to scan the files on the extended drive, you should install the software directly on the DiskXtender server. This enables DiskXtender to allow the anti-virus software to directly read purged files from media to scan them, rather than recalling the files to the extended drive and scanning them there.

The *EMC Information Protection Software Compatibility Guide*, available on the Powerlink website, provides a list of anti-virus software that is supported with DiskXtender.

Instructions for configuring DiskXtender and the anti-virus software to maximize scan performance are provided in the DiskXtender administration guide.

DiskXtender on VMware

You can install DiskXtender File System Manager on a VMware ESX Server. VMware enables you to create multiple virtual machines to maximize and consolidate your current hardware and enhance security. Virtual machines are completely isolated from the host server and from other virtual machines. If a virtual machine crashes, all others are unaffected.

You can install File System Manager on as many as four virtual machines that are running on a single VMware ESX Server. In addition, as a best practice, each File System Manager installation should manage no more than four extended drives, for a total of 16 extended drives managed on one VMware server. Otherwise, performance problems may occur.

The DiskXtender installation guide provides additional details on system architecture and requirements, as well as how to install and manage DiskXtender on VMware.

Clustering DiskXtender on VMware

You can install File System Manager on VMware virtual machines that are clustered with Microsoft clustering. VMware supports cluster environments of as many as two nodes. DiskXtender can run actively on both nodes (active/active), or it can run actively on one node and passively on another (active/passive).

The clustered VMware virtual machines can be running on either the same VMware ESX Server, which is called “cluster in a box” in the VMware documentation, or they can be running on two different VMware ESX Servers, which is called “cluster across boxes” in the VMware documentation. You can also configure DiskXtender in a cluster environment with one VMware virtual machine and one physical server (that is not a VMware server), as long as the two servers are connected to shared storage.

DiskXtender can run active/active or active/passive regardless of the cluster configuration. If DiskXtender is running active/passive, then the active installation can be on either a virtual machine or on a physical server.

Regardless of the cluster configuration, each DiskXtender installation should manage no more than three extended drives, for a total of six extended drives shared by the cluster. Otherwise, performance problems may occur.
You can install DiskXtender in a VMware environment that includes VMotion. VMotion moves live, running virtual machines—including virtual machines with a DiskXtender installation—from one host to another while maintaining continuous service availability.

When this move happens, users continue to access files by using the same virtual machine name.

The DiskXtender and VMware environment should not include Microsoft clustering. VMotion does not currently support migration of applications clustered using Microsoft clustering.

The VMware and VMotion documentation provide system requirements and installation instructions for VMotion.
A
access node, EMC Centera 56
access profile, EMC Centera 56
account, service 94
ACSLS. See Sun StorageTek ACSLS
Aggregate NAS 41, 67
anonymous profile (EMC Centera) 56
anti-virus scans 102
API
DiskXtender 98
EMC Centera 56
application file support 36
application pool, EMC Centera 56
ApplicationXtender 28, 98
architecture, system 22, 29
audit logs 33, 87
audit string for file deletes 63
audited delete 63
automation, media 42
AutoStart 91, 99

B
background scan
description 43
purging during 46
backup
DiskXtender configuration (registry settings) 90, 95
DiskXtender server 95
EMC Centera 63 to 66, 93
extended drive 90, 92
media 91, 93 to 94
NAS 93
removable media 93
snapshot 92
strategy 90
BLOBs, embedding in the CDF 59

C
C-Clip, EMC Centera
file 58
media 57
CDF (C-Clip Descriptor File) 58, 59
Celerra 18, 19, 67, 69
Centera. See EMC Centera
characters, international 37, 53
Chargeback Reporter and Seek 58
CLARiiON 19, 67, 101
client machines 24
client-side ID calculation 61
collision avoidance 59
clear, enabling for media status 85
compact media 78
compliance through retention 18
content address (CA), EMC Centera
file 58, 59
media 57
Content Protection Mirrored (CPM) 59
Content Protection Parity (CPP) 59
content-addressable storage (CAS) 58
copy media 93

database file support 36
delete rules 18, 50
deleting
audited 63
files 18, 49
files automatically 50
files on replicated EMC Centera devices 65, 66
including audit strings 63
retained files 63
DFS links 39
Direct Read 47
DiskXtender Search Module 29, 52
supported file types 36, 53
Documentum ApplicationXtender 28, 98
driver, filter 25
DVD
finalization 20, 46
supported types 73
DxAdministrators 31
Index

E
editing files 48
embedded BLOB threshold 59
EMC Centera 19, 56 to 66
  access nodes 56
  anonymous profile 56
  Basic Edition 62
  client-side ID calculation 61
  collision avoidance 59
  Compliance Edition (CE) 62
  Compliance Edition Plus (CE+) 62
  connecting with DiskXtender 56
  data protection 59
  embedded BLOB threshold 59
  Garbage Collection 58, 61
  Governance Edition (GE) 62
  metadata 58
  overview 27
  PEA file 56
  privileged delete 63
  profile 56
  replication 63 to 66, 93
  replication failover 64
  reports 58
  retention 62
  Seek and Chargeback Reporter 58
  single-instance storage 59
  storage strategies 59
  synchronous deletes 65, 66
  virtual media 57
  virtual pool 56
  encryption 38
  error log 84
  event log 84
  Explorer Add-ons 44, 54
  extended attributes (EAs) 92
extended drive
  backup 90, 92
  deleting files from 49
  editing files on 48
  folders 42
  indexing and searching for files 29, 52
  migrating files from 40 to 43
  purging files from 44
  renaming files on 48
  replication 91, 101
  report 86
  requirements 30
  scan 43
  shares 96
  supported file types 36

F
failover
  AutoStart 99
  cluster 99, 102
  EMC Centera replication 64
  FAT compatibility 24
fetch
  before files are needed 47
  notification 54
  overview 16, 47
file deletion 49
file edit 48
file migration
  customizing 42
  definition 40
  models 40 to 41
  monitoring 84
  purging after 46
  rules 43
  schedule 43
file rename 48
file restore 69
file retention. See retention
file stream support 38
File System Manager 22, 24
file systems
  FAT, client 24
  NFS, client 24
  NTFS, client 24
  OTG 79
  supported 79
  UDF 80
file tag 16, 44
file types
  supported for indexing 36, 53
  supported on the extended drive 36
filename length 37, 69
filter driver 25
finalizing media 20, 46, 78
FLR file system, Celerra 18
folder, media 42
foreign language support 37, 53
format media
  EMC Centera 58
  tape and optical 77

G
Garbage Collection, EMC Centera 58, 61
GUI
  DiskXtender 24
  DiskXtender Search Module 29, 52
  MediaStor 26

H
hardware device
  management tasks 74
  support 73
hierarchical storage management (HSM) 41, 68
high availability 91, 99, 102, 103

I
Index and Search Engine (ISE) 29, 52
index rules 52
Index Transaction Log (ITL) 52
indexing
  architecture 29
  how it works 52
<table>
<thead>
<tr>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitoring 84</td>
</tr>
<tr>
<td>supported file types 36, 53</td>
</tr>
<tr>
<td>international character support 37, 53</td>
</tr>
<tr>
<td>inventory media 77</td>
</tr>
<tr>
<td>iSCSI device support 73</td>
</tr>
</tbody>
</table>

**J**

Jukebox Manager 75

**L**

label media 77

language support 37, 53

length, filename 37, 69

LibAttach 75

licensing 28, 86

logs

- audit 33, 87
- events, errors, and warnings 84
- media 85

**M**

Macintosh file support 36

magneto-optical (MO) media support 73

media

- automation 42
- backup 91, 93 to 94
- color indicator 85
- copy 93
- deleting files from 49
- EMC Centera 57
- fill method 42
- logs 85
- monitoring status 85
- NAS 67 to 72
- NAS, security 94
- offline 20
- removable (tape, optical) 73 to 80
- report 86
- statistics 85
- supported file systems 79
- TSM 81

media folders 42

media groups

- metadata 58
- multi-target 94
- overview 42

media service

- ACSLS 75 to 77
- EMC Centera 56 to 66
- MediaStor 73 to 75
- NAS 67 to 72
- overview 19, 25
- report 86
- TSM 81

MediaStor

- architecture 73 to 74
- device management 74
- device support 73
- GUI 26

overview 26

requirements 30

service 26

memory requirements 30

metadata

- EMC Centera 58
- export, DiskXtender 92
- Microsoft clustering 91, 99, 102

migration of files. See file migration

MirrorView 91, 101

monitoring

- DiskXtender events 84
- file activity 84
- licensing 86
- security 87

move rules 43

multi-target migration 40, 42, 94

**N**

NAS 67 to 72

- Aggregate NAS 67
- backing up 93
- media, security 94

overview 27

- Retained NAS 68
- retention 18
- security 70, 72
- share requirements 70 to 72

- types 19

NetApp (Network Appliance) with Snaplock 18, 69

NetWorker SnapImage 92

NFS file system support 24

node, EMC Centera 56

NTFS compatibility 16, 24

**O**

off-line

- files 38
- media 20

operating system 30, 54

optical media support 73

OTG file systems 79

**P**

path length requirements 37, 69

Pool Entry Authorization (.pea) file 56

pool, virtual (EMC Centera) 56

PowerPath 99

prefetch 20, 47

privileged delete 54, 63

privileges, security 31

processor requirements 30

profile (EMC Centera)

- anonymous 56
- virtual pool 56

propagation of deletes on EMC Centera 65, 66

PST file support 36

purging

after DVD-R finalization 46
after migration 46
automatically 18
based on disk space 45
during a background scan 46
methods 44
monitoring 84
overview 16, 44
recalling files 47
rules 45
watermark 45

Q
query, search 52

R
random media fill method 42
Read-only file attribute 96
recall of purged files 47
Recycler 50, 50 to 51, 61, 63, 90, 96
reformat media 78
registry log/backup 90, 95
remote administration 87
renaming files 48
replication
   EMC Centera 63 to 66, 93
   extended drive 91, 101
   of file deletes on EMC Centera 65, 66
RepliStor 91, 101
reports
   DiskXtender 86
   EMC Centera 58
requirements
   architecture 22, 29
   DiskXtender 30
   file types 36
   filename length 37, 69
   hardware device 73
   security 31
restoring
   deleted files 50 to 51
   files from media 69
retained NAS 18, 68
retention 18, 50, 62, 68, 96
reuse media 78
rules
   delete 50
   index 52
   move 43
   purge 45

S
scan
   anti-virus 102
   background 43
   schedule, file migration 43
   SCSI Manager 75
   SDK
      DiskXtender 98
      EMC Centera 56
Search Module, DiskXtender. See DiskXtender Search Module
searching for files 29, 52
security
   audit logs 33
   DiskXtender configuration 31 to 32
   extended drive 96
   file 16 to 17
   NAS media 70, 72, 94
   service account 31
Seek and Chargeback Reporter 58
sequential media fill method 42
service
   DiskXtender 24
   MediaStor 24
   service account 94
   shares
      extended drive 96
      NAS media 70 to 72
SnapImage 92
Snaplock software on NetApp 69
snapshot backups 92
SRDF (Symmetrix Remote Data Facility) 91, 101
statistics
   file activity 84
   media 85
   reports 86
status
   file activity 84
   licensing 86
   media 85
Storage Strategy (EMC Centera)
   Capacity 59
   Performance 59
streams, file 38
stub file 16
Sun StorageTek ACSLS 28, 75 to 77
supported
   file systems 79
   hardware devices 73
Symmetrix 67, 101
synchronization
   between EMC Centera devices 63
   of file deletes on replicated EMC Centera devices 65, 66
T
tape media support 73
Terminal Services, Windows 87
tiered migration 41, 68
troubleshooting
   logs 84
   media 85
TSM (IBM Tivoli Storage Manager)
   as backup software 92
   backing up 94
   media service details 81
   media service overview 28
U
UDF file system 79, 80
Ultra Density Optical (UDO) media support 73
Unicode compliance 37, 53
user interface
    DiskXtender 24
    DiskXtender Search Module 29, 52
    MediaStor 26
user machines 24
utility
    Explorer Add-ons 54
    Jukebox Manager 75
    SCSI Manager 75
V
virtual pool, EMC Centera 56
virtualization, server 102
virus scan 102
VMotion 103
VMware 102
Volume Shadow Copy Services (VSS) 92
W
warning log 84
watermark, purge 45
Windows Terminal Services 87