

An IT Briefing produced by



E-Discovery Considerations for Lotus Notes Domino Organizations



Sponsored By:



E-Discovery Considerations for Lotus Notes Domino Organizations

By David Ferris



BIO

David Ferris is a Senior Analyst at San Francisco-based Ferris Research. He wrote the first syndicated column in the computer industry and has since written hundreds of articles and bulletins and co-authored three books. His focus is on messaging technologies, compliance, content control, archiving, e-discovery, and data leak protection.

This *IT Briefing* is based on a Sherpa/TechTarget Webcast, “E-Discovery Considerations for Lotus Notes Domino Organizations.”

This TechTarget *IT Briefing* covers the following topics:

- Introduction 1
- Federal Rules of Civil Procedure (FRCP) 1
 - Traditional Discovery 1
 - E-Discovery. 1
- Preparing for E-Discovery 2
 - Why Prepare? 2
 - Key Steps for Lotus Notes Domino IT Support 3
- Let Sherpa Software Be Your E-Discovery Guide 4
 - Quickly Respond to Requests with Discovery Attender® 5
 - Proactively Prepare Data with Mail Attender® 5
 - Take Preparedness One Step Further with File Attender® 6
 - Successfully Navigate E-Discovery with Sherpa Software 8

Copyright © 2008 Sherpa Software. All Rights Reserved. Reproduction, adaptation, or translation without prior written permission is prohibited, except as allowed under the copyright laws.

About Sherpa Software Solutions

Sherpa Software Solutions provides extensive e-mail management, archiving, policy enforcement, and content filtering capabilities. The company is addressing issues relating to storage management, content discovery, and compliance. For more information visit www.sherpasoftware.com.

About Ferris Research

Ferris Research is a consulting firm offering information services, reports, white papers, webinars, and a daily news blog, blog.ferris.com. Established in 1990, its research team has decades of experience in its core competencies, and its clients include 300 of the world’s largest organizations.

About TechTarget *IT Briefings*

TechTarget *IT Briefings* provide the pertinent information that senior-level IT executives and managers need to make educated purchasing decisions. Originating from our industry-leading Vendor Connection and Expert Webcasts, TechTarget-produced *IT Briefings* turn Webcasts into easy-to-follow technical briefs, similar to white papers.

Design Copyright © 2004–2008 TechTarget. All Rights Reserved.

For inquiries and additional information, contact:
Dennis Shiao
Director of Product Management, Webcasts
dshiao@techtargt.com

E-Discovery Considerations for Lotus Notes Domino Organizations

Introduction

Domino administrators in IT departments have become key players in corporate litigation due to the development of electronic discovery (e-discovery) procedures over the last several years. IT administrators must become knowledgeable about e-discovery, so they can provide required information as quickly, efficiently, and cost-effectively as possible. In order to better understand e-discovery, it is essential to understand the process of litigation in the United States and how U.S. rules have changed to account for electronic discovery. It is also imperative for IT departments in larger organizations—and some smaller ones as well—to prepare systems and policies in advance to meet potential demands in the new electronic litigation environment.

Federal Rules of Civil Procedure (FRCP)

The process of litigation in the United States is governed by a set of formal rules known as the Federal Rules of Civil Procedure. These rules were initially created in 1938 and now number 86 in all. Many other countries around the world follow similar procedures. The FRCP can be found at <http://www.law.cornell.edu/rules/frcp/>.

Traditional Discovery

Discovery is the process by which litigants come to understand the content of a case from both points of view. This process is desirable for a variety of reasons. First, it helps legal counsel understand the strengths and weaknesses of each side. Second, when cases are shown to be uneven, one side has a greater incentive to settle. This minimizes the court's burden of cases that lack merit. Third, when cases deserve the attention of the court, discovery enables the two parties to polish their arguments, knowing there will be no surprises and there is a significant chance that justice will prevail. The three traditional methods of discovery are:

- Paper documents
- Depositions (formal recorded interviews under oath)
- Interrogatories (formal questions in writing with answers certified as accurate and honest)

The details of discovery are enumerated in Rule 26 of the FRCP.

E-Discovery

About 20 years ago, the nature of discovery began to change. During the Iran-Contra scandal in the Reagan administration, Oliver North learned that e-mail records do not disappear when the Delete button is pressed and that they can still be used as evidence in court. By 2004, asking for and digging up electronically stored information had become routine in the discovery process. These requests are often extremely time-consuming, disruptive, and expensive for IT departments to satisfy. They are typically time sensitive and high priority, and also often technically difficult. It may be necessary to search through old backup tapes with archaic electronic formats, or tapes may be damaged or missing. In some cases, lawyers use electronic discovery as a predatory tactic that makes the process inordinately burdensome, sometimes with costs that grossly exceed the cost of settling the dispute in the plaintiff's favor. These predatory legal tactics may result in grossly unfair resolutions.

Amendments to the Federal Rules of Civil Procedure

The FRCP was amended to account for e-discovery in December 2006. Six rules were updated: 16, 26, 33, 34, 37, and 45; two changes are particularly significant. First, a provision regarding electronically stored information (ESI) was added. This provision makes all electronic documents subject to discovery, including: e-mails, instant messages, word processing documents, spreadsheets, CRM databases, NSF files, and information stored in RAM. For the last few years, e-mail has been by far the most important ESI. Second, "meet-and-confer" sessions were established.

In these meetings, which usually occur early in a lawsuit, the two parties exchange information on their ESI. They discuss what can reasonably be provided to the other party and what would be unreasonably burdensome. They work out an agreement on what will be produced and a schedule. This agreement is written up in a “discovery plan” that is submitted to the court for approval. Meet-and-confer procedures are defined in Rule 26(f).

A discovery plan specifies what electronically stored information will be reproduced, in what format, by what dates. It also discusses the use of specialists to produce information that is difficult to obtain and whether some information can be withheld because it is proprietary or privileged. Issues that are either contentious or idiosyncratic are written up in very specific detail. Both parties must be frank and cooperative throughout the entire process. If the court determines that either party is being evasive in disclosing information or is exaggerating the difficulty of obtaining information, it may impose sanctions, especially in the case of large, sophisticated IT organizations.

E-Discovery Deadlines

Several deadlines for the e-discovery process were established in the FRCP. Specifically, both parties must have:

- A Rule 26(f) meet-and-confer session within 2 to 3 weeks of initiation of the lawsuit
- A discovery plan delivered to the court within 14 days of the meet-and-confer session
- All ESI delivered as specified in the discovery plan
- An initial ESI within 14 days of the meet-and-confer session
- A Rule 16 scheduling conference with time deadlines for the overall lawsuit (of which discovery is just a part) within 120 days of initiation of the lawsuit

Preparing for E-Discovery

It is important for most corporations to prepare for e-discovery for many reasons. Small organizations not engaged in regulatory businesses have little need to prepare in advance because the likelihood of lawsuits involving e-discovery is relatively low. But medium-sized and large organizations engaged in as few as one or two lawsuits a year, as well as small

companies engaged in regulatory businesses like healthcare or financial services, most certainly need to be prepared.

Why Prepare?

With advance planning, a company can have the right tools and procedures in place to review and produce relevant material quickly and accurately, using fewer resources.

The pitfalls of *not* preparing for e-discovery are:

- If a company is unprepared when a lawsuit occurs, especially if the company is the defendant, it will probably not have enough time to get ready for the meet-and-confer. The company will be unable to determine adequately either what relevant information it has to provide to the other company or what it needs to obtain.
- The company is likely to commit to unrealistic deadlines; failing to meet those deadlines will make the company look irresponsible to the court.
- Being unaware of the existence of information or unable to obtain it will make the company appear uncooperative.
- The FRCP rules are designed to encourage both parties to act rationally and to settle at an early stage if that is reasonably appropriate. This will be difficult if the company does not have readily available all the information it needs to assess realistically the merits of the case.
- Electronic discovery leads to the production of very large numbers of documents that must be reviewed carefully. Lack of advance preparation may necessitate the use of numerous staff, often high-priced lawyers, to review excessive numbers of documents under duress at considerable expense.
- While companies are required to give frank and full disclosure, they are not required to give information that the other party has not requested. Inadequate preparation may lead companies to raise their risk profile by giving away unnecessary or proprietary information, such as marketing or hiring plans, because they lacked time to evaluate the information properly.
- Companies often retain many versions of documents and may be required to provide explanations of the changes. A good retention, deletion,

and archiving policy can ensure that only clearly necessary and sufficient documentation is kept.

- If the lawsuit occurs after IT systems within the company have been substantially altered, it can be very difficult and time-consuming to resurrect old data that may be vital to the case.

Key Steps for Lotus Notes Domino IT Support

A company can take several key steps to develop an IT environment that will enable it to review and produce information efficiently in the event of a lawsuit.

Initially, corporate management must recognize that IT has an important role in supporting e-discovery. Specifically, IT needs to:

- Identify the electronic information that is relevant to the case, where it is stored, who controls it, the formats in which it is stored, and the associated archiving backup and recovery processes
- Advise on the accessibility of the data and the reasonableness of e-discovery requests submitted by the other party on short notice
- Be prepared to participate in the meet-and-confer session if requested
- Produce the information that is required to satisfy an e-discovery request

Develop Policies

IT needs to have policies in place for retaining, deleting, and archiving corporate information. Many organizations archive everything; that is usually a mistake. Keeping unnecessary information can increase both a company's risk profile and the burden of weeding out irrelevant material. Once a company has decided what should be archived, it must determine how long to keep it. While some materials must be kept indefinitely, others can be disposed of after certain periods of time. Eliminating material that is no longer necessary can further reduce both a company's risk profile and the amount of time and effort required to search for relevant data in the event of a lawsuit. Also, some laws require information to be deleted after a specified period of time.

Document the IT System

IT should document the company's entire IT system. A network map is an important piece of this docu-

mentation. It is a large schematic picture that identifies all the services on the network, including geographic locations, data communications links, applications, data and information repositories, and so on. This is especially useful in preparing for meet-and-confer sessions. A description of all corporate archiving, backup, and disaster recovery systems is another important piece of the documentation. This identifies where systems are, the types of information stored, storage formats, backup and archiving schedules, and retention and destruction policies. This must also include backup procedures adopted by individual users. Because such policies take time to develop and implement, they have to be prepared in advance.

It is also essential for IT to make sure that it has a legal hold on corporate information, so that employees cannot permanently delete relevant information in the event of a lawsuit. IT must further ensure that all information is handled confidentially, especially regarding intellectual property, hiring plans, marketing plans, and private client and employee data.

Identify Key People

IT should identify the key people in the e-discovery process. For each domain within the electronically stored information network, IT must identify the people involved in developing and maintaining that part of the network. It should document the names, titles, and contact information for all individual business users, system administrators, records managers, and backup and restoration managers within the corporation. This is difficult to do in a short amount of time, so it is important to document this information in advance and keep it up to date.

It is also beneficial to designate a point person within IT who is responsible for dealing with e-discovery requests. This individual acts as a liaison between internal and external legal staff and the line-of-business users involved with the case. He or she also develops and maintains the IT documentation necessary for e-discovery responsiveness. If invested with the necessary authority, this person will be able to respond quickly and effectively.

Install E-Discovery Support

IT should install an e-discovery support tool. Software vendors have invested heavily in developing products for this market during the last few years. Sherpa in particular has useful tools to help IT

departments satisfy e-discovery requests rapidly and accurately. They can assist IT in producing requested information in a timely way while reducing the amount of time that IT and legal staff need to spend sifting through electronically stored information to determine its relevance to a case. This helps IT control the costs of e-discovery, especially when the billable time of high-priced lawyers is minimized. Sherpa's system also helps IT coordinate the workflow of different individuals and departments involved in the e-discovery process.

Prepare Key Questions

IT must also be prepared to ask a number of key questions of the opposing party in order to deal effectively with the e-discovery process.

- Ask the other party what data they have in every possible format, including: e-mails, instant messages, data at rest, BlackBerry PIN messages, and even loose paper files. Do not limit questions to information already known to be relevant, because they may present unanticipated items.
- Ask about the custodians of the relevant data, including individuals, administrators, and line of business users. They are required to be frank and may name unexpected sources.
- Ask about archiving, backup, and recovery processes that they have in place for the relevant electronically stored information. Ask about the frequency of these procedures, what is stored and where, in what medium and format.
- Ask what policies and systems are in place regarding deletion and retention of ESI, and also what types of relevant ESI are actually being deleted in accordance with policy. Useful information may be there, and the onus is on them to tell the truth knowledgeably. Ask about relevant time periods to minimize the extent of the search. Ask where the data is located, whether on PCs, servers, or backup tapes. They know far more about their own IT environment and must be proactive in disclosure. If they are evasive or uncooperative, it will reflect badly on them and can result in significant and well-publicized sanctions. Ask them also to describe their litigation hold processes.
- Ask them what information they believe is relevant but inaccessible or unreasonably burdensome to obtain. This, too, may reveal unanticipated categories

of information that are worth pressing to acquire. Perhaps the data is not really as difficult to obtain as they believe or your own company may be willing to bear the costs.

- Ask whether e-mail communications have been restored for senior executives. The answer is always yes. This deflates a common defense against producing information: saying that backups are only used for disaster recovery because they are too hard to restore.
- Ask about search tools at their disposal that can be used to satisfy the discovery requests and whether they have had any major changes in their systems as a result of upgrades, mergers, or acquisitions that impact their ability to produce older data. Within this category, find out whether they are using existing systems with Lotus Domino or have migrated from Exchange to Domino.
- Ask what the company's litigation hold process is, both in general and for this particular lawsuit.

Further Information

Ferris Research has produced several reports on the topic of e-discovery that may be of interest. These are available at www.ferris.com and include:

- Best Practices for E-Discovery: The IT Perspective
- E-mail Archiving: Best Practices
- Archiving of Electronic Information: Key Laws and Regulations

Also available at the Ferris Web site are the Ferris Research blog and information about the company's for-fee information services. For further information, contact david.ferris@ferris.com.

Let Sherpa Software Be Your E-Discovery Guide

It is no longer a question of if you will be involved in a lawsuit, but rather a question of when. Being faced with finding relevant information in terabytes of storage can be a Mount Everest-like challenge. Why go at it alone? Sherpa Software solutions can easily discover, manage, and archive Electronically Stored Information (ESI) to answer the e-discovery requests you are facing today and give you the tools that will proactively prepare your information for the future.

Quickly Respond to Requests with Discovery Attender®

Whether you are subpoenaed to produce documentation or HR is conducting an internal investigation, locating information for a document discovery request can be very costly, extremely time consuming and disruptive to an organization. Many times, these requests are made under stringent deadlines that pose many challenges to an organization trying to search large amounts of evidentiary material that can be widely dispersed throughout the enterprise.

Keys to a successful Lotus Notes discovery are complete and consistent results, and preserving data integrity. Discovery Attender for Lotus Notes provides dedicated keyword searching and results management for Lotus e-mail and documents (including attachments). It gives administrators immediate access to content by performing searches on messages, attachments, and files (.doc, .pdf, .xls, and the like) that are stored in Domino server databases, local databases, instant message logs, and common file storage areas. Discovery Attender can search e-mail files either collectively or individually with customizable criteria such as keywords, date ranges, users, and much more.

Searching Lotus Notes e-mail is particularly problematic, especially within large organizations. Discovery Attender's design takes into account the large volume of data and widespread networks that may need to be searched, as well as the limitations in the time a Lotus Notes scheduled process can execute. Discovery Attender operates from within the native Lotus Notes environment in order to leverage its inherent, highly-scalable capabilities. When multiple servers need to be searched, Discovery Attender distributes processing across the environment, with search criteria and results managed centrally.

Figure 1 shows an easy-to-use interface to enter criteria/parameters and execute searches.

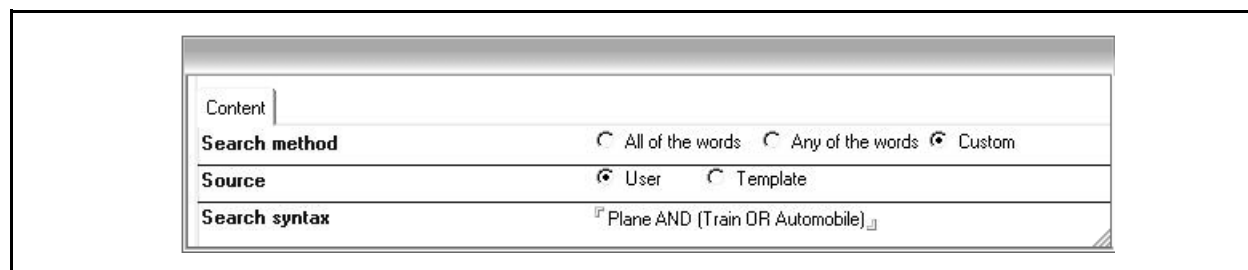


Figure 1

Once searches are complete, Discovery Attender offers capabilities for deduplication, redaction, and annotation to further cull review sets. And, because outside legal teams are often involved in discovery requests, results can be optionally exported into non-native formats that can be viewed by parties outside the Lotus Notes environment.

Figure 2 illustrates how results are ranked by relevancy and sorted by multiple, user-customized criteria.

Discovery Attender can effectively save time, secure evidence, and reduce litigation support costs by enabling IT, litigation support, and legal teams to immediately gain access to content and efficiently search, locate, and review data for document discovery requests.

Proactively Prepare Data with Mail Attender®

The key to discovery preparedness is to have ongoing retention and archiving policies established so information is already harvested, secured, and centralized prior to an EDD (Electronic Data Discovery) request. Mail Attender for Lotus Notes is a Domino-centric management and archiving solution that can set and schedule policies to enforce retentions and/or deletions, archive information, apply legal holds, reduce storage, mitigate potential risks, address regulatory requirements, and much more. Its comprehensive feature set combined with the ability for administrators to apply management granularly (at the user, department or group level) ensures that information is selectively managed, protected, and readily accessible for future inquests.

Much of the information users need to do their jobs is usually bound up in e-mail or other information stores. Therefore, message stores are a critical source of information for knowledge management, e-discovery, and data mining purposes. However, proper retention practices are extremely difficult to imple-

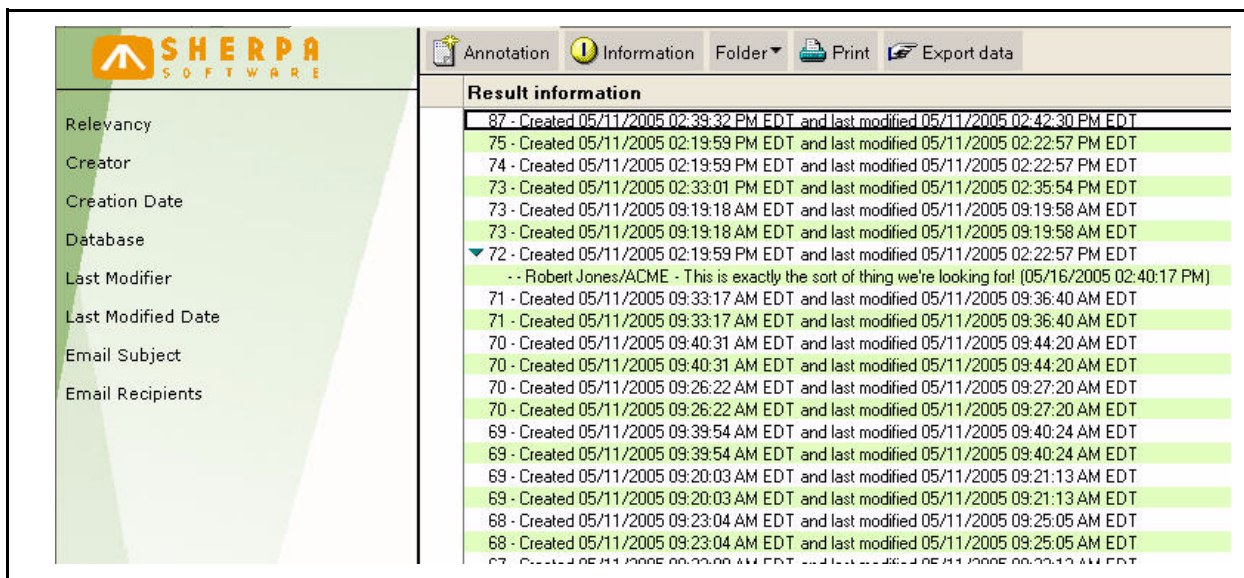


Figure 2

ment if appropriate retention tools are not employed. With Mail Attender, company retention requirements can be automatically executed through its enforcement of Mail Restrictions that define the parameters for what information will be kept, what will be deleted, where it will be stored, and how it will be maintained long term. Policies can be enforced by name, date, size, location, etc. with actions such as archive, delete, copy, and report. When put into place, these policies can drastically decrease storage and the amount of information to review in the event a discovery request is issued, while offering a secure location to store your corporate knowledge and business records.

Figure 3 shows how to easily configure the processing that is to occur within the mail databases.

If archiving actions are selected, e-mails and attachments within mail files and the Domino Journal can be moved to an archive location for safekeeping. By having a centralized storage location, such as an archive, business information can be organized in a way that will expedite future searches thus reducing the time and cost to present discovered data for lawsuits and internal compliance policies. Archiving data out of susceptible mail servers also gives administrators the ability to single-instance duplicate attachments, set retentions to purge information after its useful life, apply legal holds to potential evidence, and encrypt archived data for increased security.

In addition to proactively managing and archiving information for e-discovery searches, Mail Attender can also effectively protect document integrity and reduce liabilities by enforcing restrictions that prohibit users from editing, deleting or sending e-mails with specific content. These restrictions provide the ability to certify document authenticity, remove the onus on employees for determining what is deemed as “important” information and maintain that nothing that can increase your legal exposure leaves the corporate systems.

Figure 4 illustrates how to successfully limit legal exposure by prohibiting users from sending e-mails containing unauthorized content.

Mail Attender’s robust archiving, policy enforcement and content management feature sets allow companies to effectively address issues related to e-discovery, archiving, storage management, retention, and compliance within Lotus Notes e-mail.

Take Preparedness One Step Further with File Attender®

In most companies, retention policies are being enforced on the e-mail messages within each user’s mail database, which normally include any attachment that exists within the e-mail messages. However, other areas of concern are the files and attachments that users have saved to their hard drive or to a file server. Many administrators have a difficult time reaching these files for discovery and management purposes.

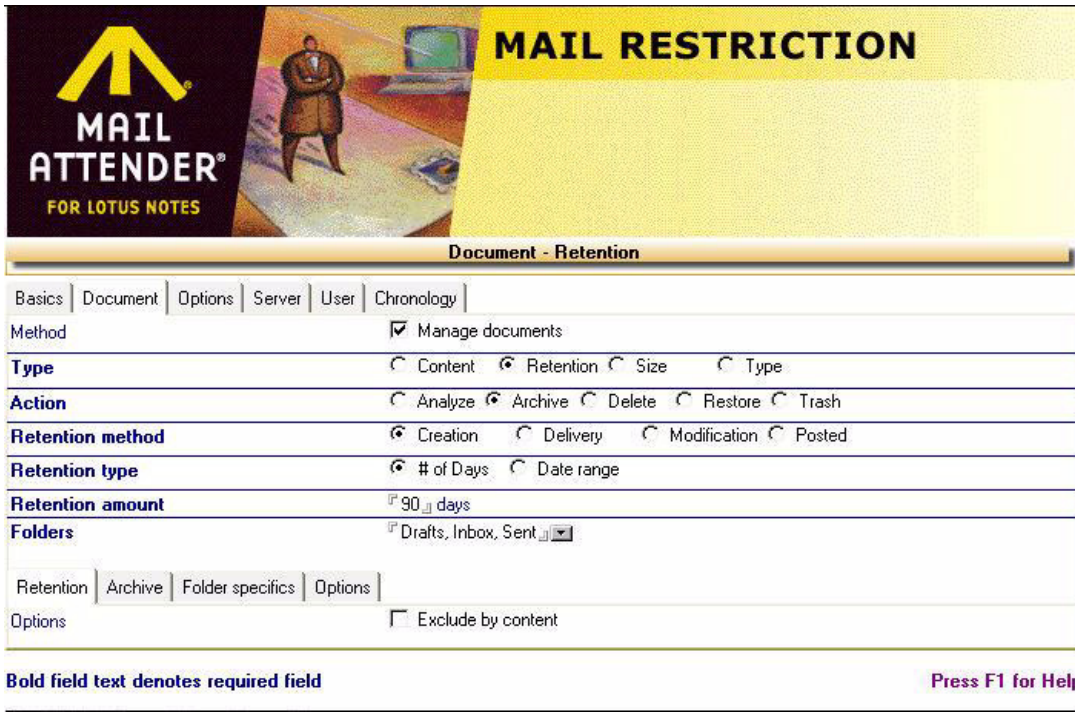


Figure 3

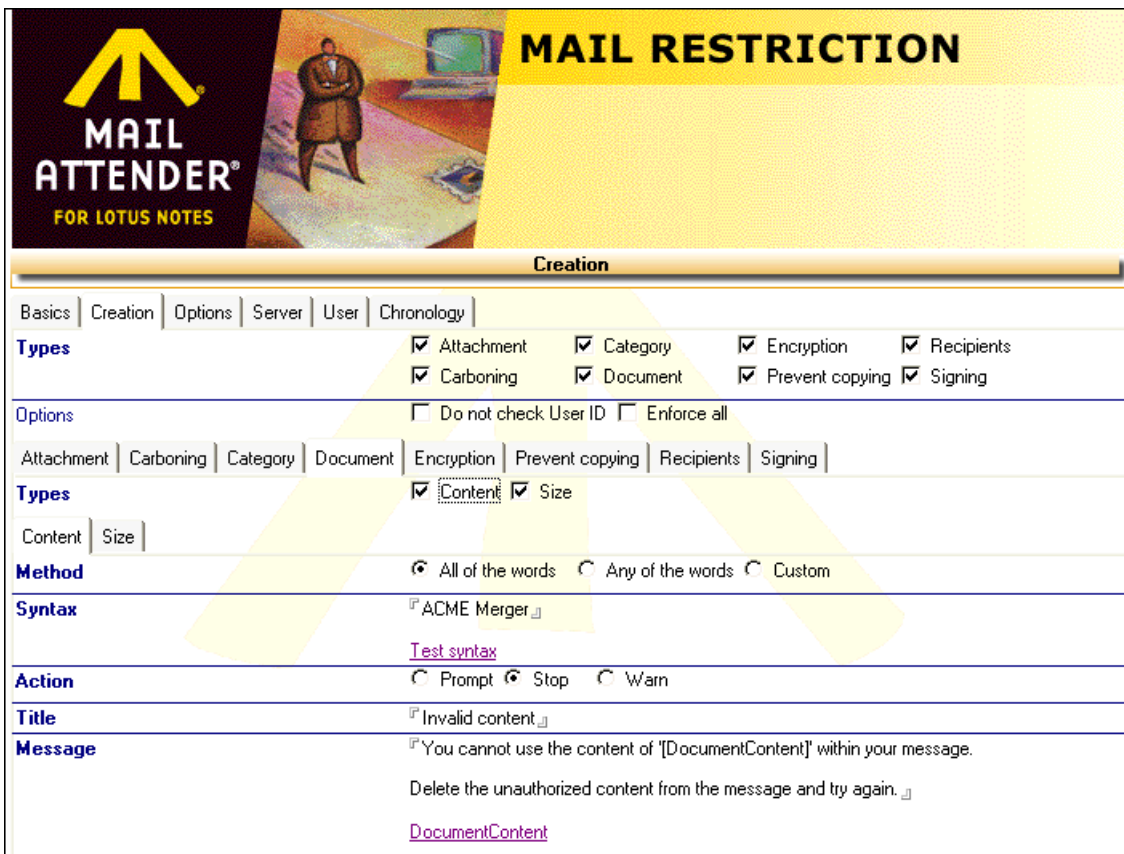


Figure 4

File Attender can manage and locate the business sensitive files on a user's hard drive that were previously out of reach. Using File Attender, you can locate files within specified locations using the file age, name and/or size. Once information is located you can collect a list of files that exist, copy files to another location, delete non-business/unnecessary information or move files to a secure archive location. Additionally, File Attender can interface with Discovery Attender to provide in-depth search capabilities that utilize keywords to locate files for management.

Figure 5 shows how you can specify files by their age, location, name, and size. This allows administrators to create very granular rules for the entire set of users or for a specific subset of users.

Successfully Navigate E-Discovery with Sherpa Software

You wouldn't try to tackle Mount Everest without the help of a Sherpa, so why try to tackle content discov-

ery, archiving, and management without Sherpa Software? Our solutions are specifically designed to address e-discovery, archiving, storage, information security, and compliance requirements as they may relate to content discovery and regulations such as the new amendments to the Federal Rules of Civil Procedure. Discovery Attender, Mail Attender, and File Attender streamline the often difficult task of addressing discovery requests while offering flexible management architectures and reasonable pricing models to any size company or law firm.

For more information on Discovery Attender, Mail Attender, and/or File Attender, visit www.sherpasoftware.com to download a free trial version or call 1-800-255-5155 to speak with a Sherpa Software Sales Representative.

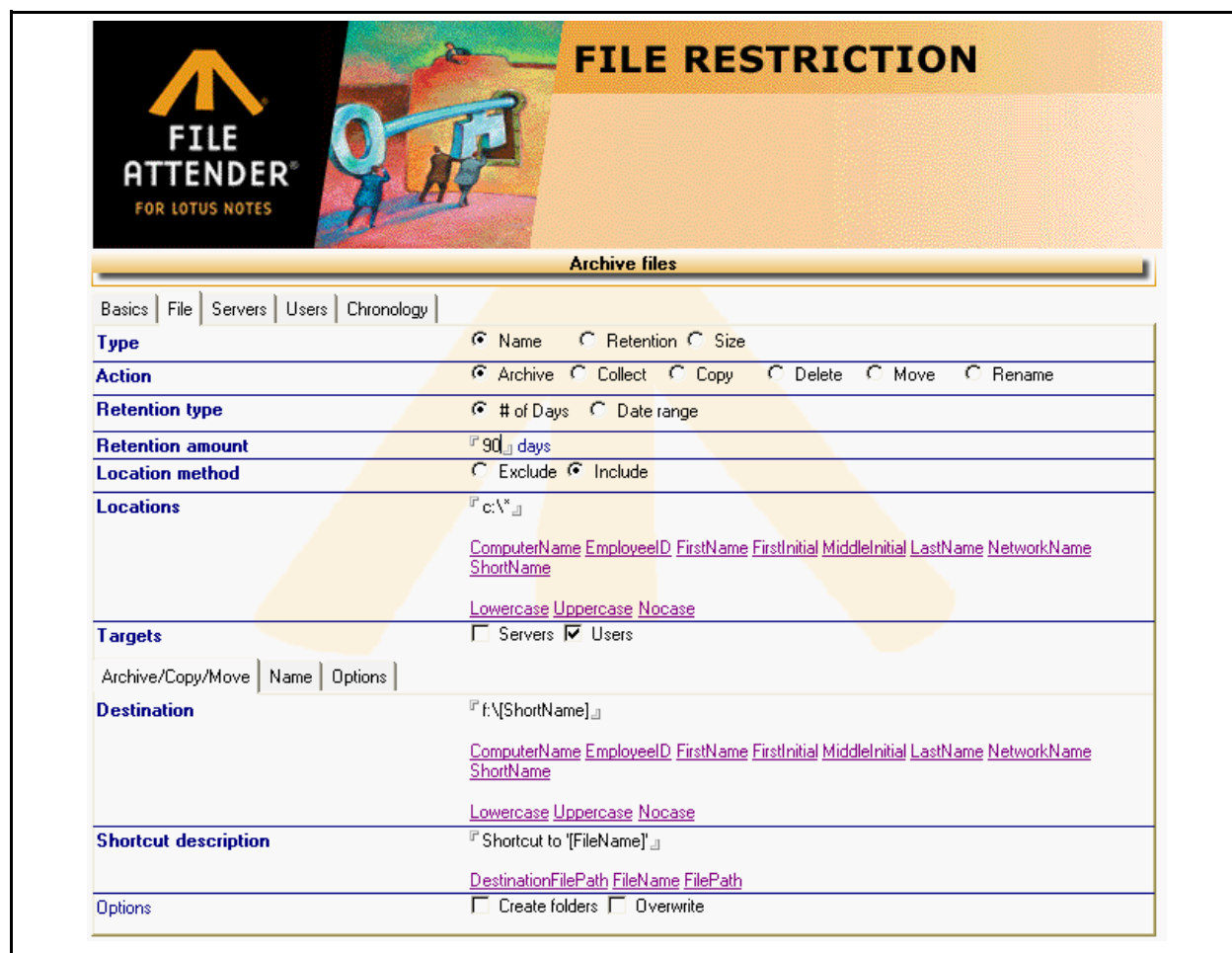


Figure 5



About TechTarget

We deliver the information IT pros need to be successful.

TechTarget publishes targeted media that address your need for information and resources. Our network of technology-specific Web sites gives enterprise IT professionals access to experts and peers, original content, and links to relevant information from across the Internet. Our events give you access to vendor-neutral, expert commentary and advice on the issues and challenges you face daily. Our magazines give you in-depth analysis and guidance on the critical IT decisions you face. Practical technical advice and expert insights are distributed via specialized e-Newsletters, video TechTalks, podcasts, blogs, and wikis. Our Webcasts allow IT pros to ask questions of technical experts.

What makes TechTarget unique?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events, the expert interaction of Webcasts, the laser-targeting of e-Newsletters, and the richness and depth of our print media to create compelling and actionable information for enterprise IT professionals.

SHERPA_03_2008_0001