

The Importance of Archiving Your Organization's Email Communications



S H E R P A
S O F T W A R E

1300 Old Pond Road
Bridgeville, PA 15017

www.sherpasoftware.com

PH: 412-206-0005

FX: 412-206-0018

Toll Free: 1-800-255-5155

Email: information@sherpasoftware.com

Table of Contents

Introduction	1.0
The Daily Abundance of Email Messages	1.1
Archiving Email Communications	2.0
The Issues That Make It A Critical Necessity	2.1
Compliance and Legal Issues	2.1.1
Storage Issues	2.1.2
Server Performance Issues	2.1.3
An Effective Means for Archiving Email Communications	2.2
Sherpa Software Mail Attender for Notes	3.0
Optimizing Email Management	3.1
Email Archiving: Assuming Control Over Your Email	3.2
Responding to Legal and Infrastructure Concerns	3.3
Sherpa Software Database Attender	3.4
Summary	4.0
Appendix A	5.0
Technical Specifications for Sherpa Software Mail Attender for Notes	5.1

1.0 Introduction

1.1 The Daily Abundance of Email Messages

Email still dominates as the most utilized form of electronic communications in the workplace, as it is the most efficient method for transferring documents and reaching people around the globe. Employees in organizations transmit and receive thousands of email messages on a daily basis — emails are incoming, outgoing and circulated across the enterprise. Consequently, the large volume of email transmissions creates several issues, each with either legal or infrastructure implications for the organization.

Since the Supreme Court ruled that an employee does not own their email and that it is the property of the employer, companies want and need to have control over their organization's email messages. Managing email is a complex task, however, and entails having adequate storage space and ensuring the unimpeded flow of incoming and outgoing messages. With the never-ending accumulation of emails, organizations often face the issue of space limitations and how to continually find storage space for messages and their attachments. Further, the steady stream of emails can be a drain on server capacity and performance.

Most importantly, the constant and increasing transmission of email messages — each likely containing internal and private information and documents — necessitates organizations ensure the protection of important corporate data, compliance with governmental regulations and adequate preparation in the event of litigation. Doing so requires thorough record-keeping and the ability to gain quick access to specific pieces of information.

Clearly, these issues resulting from the ongoing movement of email messages are all good arguments for why organizations need to archive their email communications.

While email management systems exist that will allow organizations to archive emails and attachments, IT administrators need extensive capabilities that will enable them to:

- Track emails meeting specific criteria;
- Establish archiving rules as granularly as possible;
- Specify groups of employees to be impacted by those rules; and
- Determine and place restrictions based on governmental regulations and corporate security policies.

2.0 Archiving Email Communications

2.1 The Issues That Make It A Critical Necessity

Findings by Osterman Research reveal that the average message store size has increased by more than 25% during the past 12 months for nearly half of organizations, and it has grown by more than 50% for one out of every eight organizations. Much of that data increase is the result of email information stores — increased email and attachment loads.

The infrastructure implications of these findings are becoming apparent to organizations of all sizes and necessitating the implementation of an email archiving solution that will address their rapidly changing storage circumstances.

Compliance and legal concerns have also contributed to increasing awareness of the need to archive emails. Even companies that are not impacted by the recent governmental laws regarding the privacy of financial, patient and customer data need to secure their corporate information and be prepared if presented with a lawsuit.

The following illustrates in greater detail the issues caused by an organization's email messages that establish email archiving as a critical necessity.

2.1.1 Compliance and Legal Issues

Email messages can contain information that is highly important, private, sensitive, and even damaging. A significant portion of emailed information could also fall under the jurisdiction of governmental regulations, such as the following:

Sarbanes-Oxley Act (SOX) – Requires publicly-traded companies to implement controls for protecting critical business and financial data;

Health Insurance Portability and Accountability Act (HIPAA) – Requires that health institutions limit the disclosure of an individual's personal health information as it is collected, processed and transmitted to other health organizations; and

Gramm-Leach-Bliley Act (GLB) – Mandates that financial institutions adopt strict measures to protect the privacy and security of customer data.

Because of the nature of the content they often contain in both the text of their message as well as attachments, emails place organizations at risk for legal action or lawsuits. In addition to being found non-compliant with the above regulations, an email could implicate a company in a legal matter, providing negative evidence that could be used in a court of law. Or, an employee could sue an organization as a result of inappropriate or offensive emails sent by co-workers in the workplace.

Therefore, email requires a specific and secure database for storage as well as close monitoring. Email archiving is a good-sense business practice that allows organizations to ensure compliance and provides broad control over employees' email content. By archiving, organizations can protect corporate data, locate specific content quickly, have a record of important communications, and be prepared in the event of litigation. Archiving also allows organizations to manage the lifecycle of specific data, as retention policies can be established for data that requires permanent storage and data that can be deleted once a mandatory time period has passed.

2.1.2 Storage Issues

Email users generally do not realize that the server space in their organization is limited, and that retaining all their sent and received email messages can have a negative impact on the space available. Users' access to new as well as saved messages can become obstructed when servers are near or at full capacity.

IT administrators are constantly facing an ever-expanding need to obtain more storage for their organization's email databases. Consequently, the costs of acquiring more hardware to address storage issues are significant, and determining the costs of future hardware needs is problematic.

Because organizations need to save and store all their business, financial and legal-related email communications, email databases will continue using more space every day. Archiving is a more cost-effective means of storing saved emails and ensuring the retention and security of critical email messages and attachments.

2.1.3 Server Performance Issues

Burdening servers with the increasing amount of email messages that are sent, received and must be saved drains their overall effectiveness. Server performance slows and back-up times become lengthy. Successful delivery of emails can be hindered. Dealing with an enlarged email message and attachment load on the servers can also deplete administrators' resources.

By automatically archiving email messages and attachments to a separate data store, organizations can alleviate excessive server loads as well as administrator workloads, and consistently maintain strong server performance levels.

2.2 An Effective Means for Archiving Email Communications

To effectively archive their email messages and attachments, organizations need a solution that enables administrators to capture and manage every email by selectively archiving or deleting it. Email archiving is optimally achieved by creating predetermined configurations based on a number of criteria, such as content (using keywords), age (and retention time), folder the email resides in, and size. Attachments would be archived by creating a separate set of configurations using similar criteria, such as attachment name, extension, age of the email, size of the attachment, and size of the email.

When selecting an email archiving solution, organizations should demand comprehensive functionality, including the ability to apply archiving rules to specific users and servers or groups of users and servers, as well as to the email messages. Automatic retention is necessary for ensuring mission-critical messages are captured, stored and saved for the required interval. The archived data stores should be highly secure and easily accessible.

Most importantly, a powerful email archiving solution should address all the abovementioned legal and infrastructure issues that are inherent to email databases — with a focus on reducing space usage, preventing infrastructure problems and averting legal activity.

3.0 Sherpa Software Mail Attender® for Notes

3.1 Optimizing Email Management

Developed to handle the volume of emails produced within an organization and its impact on infrastructure and business, Sherpa Software's **Mail Attender for Notes** is a Lotus Notes email administration product that allows administrators to control email content, properties and user activity within email databases. Mail Attender automatically archives emails and/or attachments to separate data stores based upon multiple criteria (such as age, date/date range, message/attachment size, keywords/phrases, and sender/receiver).

Through Mail Restrictions — rules created by Lotus Notes administrators — Mail Attender provides the ability to create and enforce automated rules for managing several email components. Mail Attender can perform many different tasks, including document (email) retention and attachment retention, which track and protect critical data and affect whether employees can use specific content and change or delete email messages.

Mail Attender contains 16 different types of Mail Restrictions, each of which affects the automatic processing of a specific area of the email system: ACL (access control lists), activity (by end-user), address books (local), attachments, creation (new messages), documents (the email text), folders, full-text indexes, Out-of-Office alerts, personal agents, preferences, properties, quotas, replication entry, design and profile.

Each Mail Restriction can be configured based on the parameters required by the organization. A Mail Restriction can apply to all servers and end-users or a sub-set of servers/end-users. The subset of servers/end-users can be based upon groups (identified in the address book), OU structures or explicit server/end-user names. Exclusion or inclusion lists can be created for identifying specific names.

Several different types of Mail Restrictions can exist for the same user or set of users concurrently — there are no limitations on the number of restrictions established for either a single user or all users. Organizations can manage their users individually or collectively, depending on what will meet their needs and objectives. Also, within each Mail Restriction, administrators can also specify the priority of that restriction. A higher priority restriction will supercede any other restriction of the same type with a lower priority.

Simply put, Mail Attender enables administrators to make a Mail Restriction as granular as the organization wants it to be.

3.2 Email Archiving: Assuming Control Over Your Email

Because email is a mission-critical application, the legal issues it creates can affect your organization’s reputation, image and credibility, as well as its bottom line. The impact of email overload to the infrastructure can be discernible and experienced across the organization. The email archiving capabilities in Sherpa Software’s Mail Attender provide you with the power to restrict employees from email actions that would be detrimental to the organization and to prevent an overload to the email infrastructure that could cause storage space losses and server crashes.

Mail Attender’s archiving capabilities can be found in three of its 16 types of Mail Restrictions — Document, Attachment and Activity — each of which addresses the email messaging components that can create legal, storage and server performance issues for organizations.

Document Restrictions and Archiving

The Document (email) Restrictions allow administrators to locate and manage documents (emails) using four different methods. Then, with each document, an administrator can take one of four actions: Analyze (Report), Archive, Delete or Trash.

The four methods for locating and managing documents (emails) are:

1. By content, specifying specific words or syntax.
2. By documents’ (emails’) age, specifying the folder(s) in which the documents reside and the maximum age. Keywords can also be specified that will exclude a document from processing if the keywords exist.
3. By document (email) size, specifying folders, age and documents with or without attachments.
4. By document (email) type, specifying field name, values, folders and age.

Attachment Restrictions and Archiving

The Attachment configurations allow administrators to locate attachments for archiving or deletion using four different methods (see below). This type of restriction is most useful for reducing legal liability and reclaiming server space.

Once an attachment has been located, one of five actions can be taken: Archive, Report, Collect, Copy, Delete, or Delete Document (email). For example, an attachment with a specific extension can be designated for archiving from the document after the employee has been notified one time.

Methods for managing attachments:

1. Attachments can be managed according to the type of attachment (attachment name or extension). This allows administrators to create multiple restrictions and take different actions after a specified number of processes for each type of attachment. Administrators can also specify the age of the document containing the attachment before the attachment is processed.
2. Attachments can be managed by the retention or age of the document. For example, an administrator can designate that attachments in a document older than 180 days are archived after three processes.
3. Attachments can be managed according to their size. For example, an administrator can specify that any attachment whose size is greater than or equal to 5 MB will be deleted after three processes.
4. Attachments can be managed by the size of the document. For example, an administrator can authorize that any document that contains at least one attachment and greater than or equal to 1 MB will be archived after three processes.

Activity Restrictions

This type of restriction allows organizations to preserve specific email messages in their original form by preventing employees from deleting or editing documents in their email files. Activity Restrictions are used to maintain the integrity of sensitive or confidential information or evidence for legal actions, and to protect documents (emails) matching specific criteria. For example, an activity restriction can be placed on documents containing particular words in the content. Organizations that have mandatory retention policies pertaining to “protected” documents can ensure that a user cannot delete any email that has existed less than the specified number of days.

Administrators can prevent users from deleting or editing emails using one of five criteria:

1. Content – specifying key words or phrases.
2. Correspondents – selecting a list of people who are either in the “From,” “Send To,” “Copy To,” or “Blind Copy To” fields.
3. Date – selecting a start and end date.
4. Retention – entering the retention period and method (older/younger).
5. Subject – identifying a complete or partial subject line.

3.3 Responding to Email-Related Legal and Infrastructure Concerns

The comprehensive set of archiving capabilities offered by Sherpa Software’s Mail Attender for Notes delivers numerous benefits for organizations that use the solution to address the issues created by the constant and increasing flow of email messages.

With respect to compliance and legal concerns, organizations can mitigate the possibility of lawsuits and fines. Because Mail Attender indexes all archived content and provides the ability to search archives quickly, it is easy to extract email content that is relevant to compliance or legal matters, such as data or documents that may be private, proprietary, or damaging to the organization and need to be secured. Mail Attender also allows administrators to grant specific users the ability to search their own archives.

Regarding the issue of impact to the email infrastructure, organizations will observe greater efficiency in the use of their storage space and experience a reduction in hardware costs. Server performance will improve, creating efficiencies overall and increasing business speed. Also, Help Desk calls will be reduced because server crashes and slow-downs will become almost non-existent.

An added benefit of Mail Attender is that it stores emails in their original format (nsf), eliminating the need for proprietary applications to access email messages in the future.

Mail Attender is native to Lotus Notes and Domino.

By providing the control and flexibility to manage and automatically archive emails to a separate data store, Mail Attender helps organizations overcome the burden of legal and server issues. Its extensive functionality proactively enforces the restrictions created by administrators. Mail Attender is managed from a central location and does not require additional hardware, therefore it does not need to be uninstalled when server changes occur. A truly unique solution, Mail Attender is the only email management system that allows organizations to monitor employee email activity, ensure emails with certain words or attachments are not sent, and enforce archiving and retention policies.

3.4 Sherpa Software’s Database Attender

In addition to Mail Attender for Notes, Sherpa Software offers Database Attender for Notes, another product with wide-ranging archiving capabilities. Database Attender is a Lotus Notes database management tool that monitors and controls database security, usage, content and deployment. From a single, centralized location, Database Attender oversees the Notes infrastructure, thereby streamlining the administration process.

Database Attender’s archiving features provide a broader spectrum of document retention policy enforcement, which is crucial for addressing the legal and server space issues previously discussed. With respect to legal issues, Database Attender allows organizations to establish consistent document retention rules to reduce the potential of harmful content appearing in their databases. By maintaining automated rules for document retention, organizations can avoid the appearance of destroying evidence to prevent discovery.

To help organizations manage space on both email and application servers and avoid spending significant sums acquiring additional servers and hard drives, Database Attender provides superior and efficient document management. Database Attender enables administrators to create rules that identify documents matching specific criteria, such as age, author, or last access date, and then either report the documents, move them to an archive database, or delete them.

With Database Attender, archiving can be based upon a document’s creation date, last modification date, or last access date by stipulating a specific number of days prior to the current date or by specifying a date range. Archiving rules can be applied to separate databases or all databases, applied to all documents within an application or limited to those that exist within certain views. Archiving rules can also be refined by whoever last updated them. Additional options allow administrators to define how to treat documents that are part of larger document “threads.” Database Attender is also capable of creating archive databases automatically when documents that match the archival criteria are discovered. The archive database(s) can exist on the server itself or any device to which the server has access.

4.0 Summary

Email’s stature as the most utilized form of electronic communications and a significant enterprise application elevates an organization’s obligation to lessen and resolve its impact. Several issues are created as a result of the steady and rising stream of email messages that move in and out of the organization every day — most importantly, issues pertaining to possible legal and infrastructure ramifications.

Because of the need to be compliant with governmental regulations and corporate policies, organizations are concerned about protecting critical financial data, proprietary business reports, and patient and customer information that could be contained in email messages. To protect themselves from potential lawsuits, they also need to watch out for internal messages that could be deemed inappropriate.

With the daily glut of email messages organizations typically experience, action is necessary to stem the possibility of servers overloading and space becoming unavailable. Organizations need an email management system that will help them with addressing these issues by providing capabilities for email content management and archiving, attachment management and archiving, and email activity management.

Sherpa Software’s Mail Attender is an email management system featuring Mail Archiving and Restrictions, which are configured by administrators to establish rules on whether or not specific emails can be edited, deleted, or archived. With Mail Attender’s Mail Restrictions, administrators can specify multiple criteria, gaining the control organizations need to ensure their legal and infrastructure concerns are addressed.

Mail Attender can help resolve almost any issue found within user email databases, as it performs many unique and necessary functions, such as reclaiming critical server and storage space, archiving documents, enforcing corporate retention policies, controlling electronic sabotage, removing non-business-related documents, and protecting authenticity. For more extensive document retention capabilities, Database Attender is a complimentary database management

tool that helps with maximizing server space usage and specifying and controlling the types of content that can and cannot reside in email and application databases.

As a result, administrators will realize immediate benefits, such as improved server performance, reduced storage use and decreased hardware costs. Users will no longer experience server downtime or email quotas. Most of all, organizations will have a powerful set of tools to prevent legal consequences and possible infrastructure failure.

5.0 Appendix A

5.1 Technical Specifications for Sherpa Software Mail Attender for Notes

Installation

- Easy, non-intrusive Lotus Notes-based installation
- Installed from a single Notes client to all servers
- Server based product – installed on Notes mail servers

Architecture

- Runs on all Domino platforms including 6.x, 6.5.x and 7.x
- No Domino architectural changes required
- Uses LotusScript-based agents
- Server-based processing
- All processing is performed from a single database

###

Copyright © 2006 Sherpa Software

Sherpa Software
1300 Old Pond Road
Bridgeville, PA 15017

www.sherpasoftware.com

PH: 412-206-0005

FX: 412-206-0018

Toll Free: 1-800-255-5155

Email: information@sherpasoftware.com