

Policing Exchange

If you need to police your Microsoft Exchange environment, Sherpa Software has an arresting application that's just right for the job

BY ANDY LEANING

What was started in Seattle in 1996 by a team of programmers, project managers and marketing folk has gone on to become one of the premier collaboration tools for organisations of every size and shape across the world. Microsoft Exchange has indeed come a long way since its inception but despite its considerable popularity and ever-swelling feature list there are still some duties administrators of this e-mail heavyweight struggle with.

A common complaint levelled at Microsoft's mail server is the inflexibility and complexity of managing user mailboxes – the files that hold the messages and other data trafficked by Exchange. As e-mail has become the primary means of communication in many organisations, the importance of data in mailboxes has become paramount. Yet managing, controlling and policing these vital and often legally admissible messages is at best onerous and time-consuming.

Stepping in to fill this gap is Mail Attender Enterprise Edition. It may not have the catchiest name, but with features to answer the above problems, it's a dream come true for hard-pressed Exchange administrators.

The software is accessed through a web browser interface to a server-bound element that monitors and controls Exchange. The various functions

accessed through this point-and-click interface all fall into one of three broad groups: managing content in mailboxes, managing the mailbox files themselves and monitoring usage.

Policy police

As regulatory and legislative requirements become more demanding in the wake of the various accounting scandals here and in the US, the need to implement and enforce e-mail policies and ensure documents are

"Mail Attender works by defining rules and actions to be carried out when the rules are broken. Rules and actions can be applied to individuals or groups"

retained will become vital for most organisations and it is in this context that the Mail Attender and its content policy management tools prove most useful.

While it has been possible to perform some of the content handling functions of Mail Attender in Exchange, it has usually required a lot of co-operation from staff and a considerable administrative overhead. Mail Attender greatly simplifies the process while also making it possible to enforce the policies defined.

Mail Attender works by defining rules and actions to be carried out when the rules are broken. The predefined list of rules includes checks for practically every conceivable message eventuality relating to message and attachment: age, content, size, type, date and name; folder size and count and even mailbox size quota checking (**Figure 1**). Once rules are defined, it's a case of creating the actions to be carried out when a breach of the rules occurs. This includes forwarding suspect messages, changing subject lines to warn users, deleting messages, moving them to other folders or executing other programs and scripts (**Figure 2**). Rules and actions can then be applied to individuals or groups of users and messages checked against them.

Administrators looking after large Exchange environments will appreciate the ability to apply rules right across their Exchange real estate. Whether on

Statistic Type	Value
Folder Count	177 total folders
Message Count	7253 total messages
Message Size	6643 messages larger than 1 KB
Message Size	3387 messages larger than 5 KB
Message Size	2474 messages larger than 10 KB
Message Size	574 messages larger than 100 KB
Message Size	159 messages larger than 1024 KB
Message Size	0 messages larger than 5120 KB
Message Type	1804 messages of type IPM
Message Type	103 messages of type IPM.Activity
Message Type	5 messages of type IPM.Appointment
Message Type	8 messages of type IPM.Contact
Message Type	5305 messages of type IPM.NOTE
Message Type	2 messages of type IPM.Note.Rules.OofTemplate.Microsoft
Message Type	26 messages of type REPORT.IPM.Note.NDR
Attachment Count	2274 total attachments
Attachment Size	1686 attachments larger than 5 KB
Attachment Size	1550 attachments larger than 10 KB
Attachment Size	610 attachments larger than 100 KB
Attachment Size	159 attachments larger than 1024 KB
Attachment Size	0 attachments larger than 5120 KB
Attachment Size	0 attachments larger than 10240 KB
Attachment Extension	2 attachments with extension *.avi
Attachment Extension	1 attachments with extension *.bat
Attachment Extension	6 attachments with extension *.bmp
Attachment Extension	3 attachments with extension *.cpp
Attachment Extension	30 attachments with extension *.dat
Attachment Extension	148 attachments with extension *.doc
Attachment Extension	6 attachments with extension *.eml
Attachment Extension	16 attachments with extension *.exe

Figure 1: Statistics and more statistics, Mail Attender can report on numerous eventualities

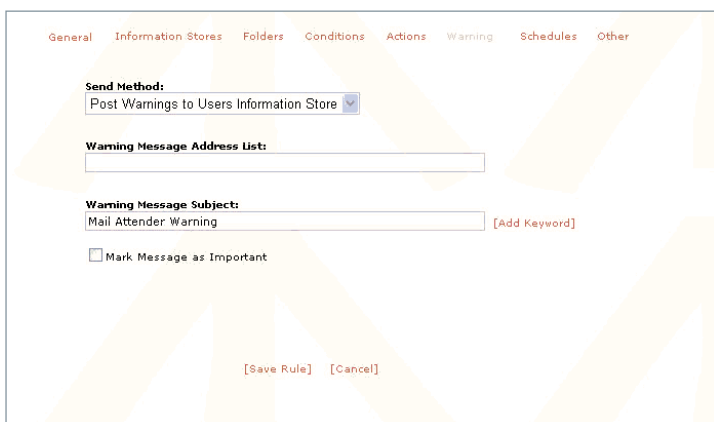


Figure 2: With rule definitions it's possible to set actions such as posting warnings

desktops or servers, mailboxes can be controlled from just one location. There's no need to hop around systems and servers applying rules in different places – you just open one web browser.

I particularly liked the powerful content checking and search capabilities, which allow the e-mail header fields (sender and subject, for example) along with the message bodies and attachments to be searched for words, phrases and combinations and to do so using Boolean logic (AND, OR and NOT clauses) and wild cards. With this, for example, it would be simple to search for messages containing 'slush fund' AND 'transfer' or all documents from a particular client. This function would have saved me many hours hunting for suspect activity and looking for particular messages needed in a hurry in the past few weeks alone.

The policy management tools don't just apply to the content inside mailboxes. It's equally possible to define policy rulings governing size and age for the mailbox files themselves and enforce them for the worst abusers.

Mailbox mayhem

Policies on mailboxes takes us neatly to the next category of Mail Attender function – managing mail stores and mailboxes. Even non-Exchange users – those just running Outlook on desktops – will appreciate a common problem with their e-mail data files: their propensity to quickly grow to ridiculous sizes. A quick scan around the desktops local to me turned up PST files frequently in excess of 500Mb and several bordering on 1Gb.

It's easy to appreciate how disk capacity, and its bedfellow tape backup capacity, can quickly become a sore point for administrators of even small Exchange environments. Via its web user interface, it's possible to really get your teeth into the files that constitute stored e-mails.

Attachments to e-mails can be exported and compressed reducing the size of the PST files that previously held them while the PST files themselves

can be compressed. Applying this procedure to a variety of sample PST files resulted in savings of 10Mb per PST file. Extrapolate such savings across large numbers of users and the savings in disk space would easily become considerable.

As with the policy management functions, these features can be automated by creating rules and corresponding actions that are carried out automatically as matching messages are found, effectively automating many Exchange management duties.

The last element of Mail Attender is the reporting function and this is perhaps its weakest element, although it's still a weighty improvement over the reporting capability built in to Exchange. You can run reports to show a wealth of statistics, including message, mailbox and attachment size and attachment extension types. Despite the value of these reports, more could have been done here, such as the ability to sort report outputs by different criteria and cross-reference data between reports – the attachments type by the heaviest users for example – to identify hard to spot trends. More visually appealing reports with pie charts, say, would also be a benefit.

Law enforcement

Mail Attender is guilty as charged: it does exactly what it claims to do and does it with aplomb. It's straightforward and easy to use and as a tool to ease and extend the management of Exchange and PST files, it will quickly become indispensable to many administrators. As a means to implement and enforce corporate policy, it's a must-have. <

Andy Leaning is a systems engineer specialising in networking and security. You can reach him at editorial@esmag.co.uk

2Gb or not 2Gb

One of the biggest gotchas of Microsoft's mail environment is the size limitation on PST files. When these files, holding all your messages, reach 2Gb in size, messages start disappearing or can't be retrieved and there's no recovery other than hoping you've got the mail on a backup that can be restored. Worse still, there's no warning as to when this will happen, short of checking each mailbox.

Hence, one of the most valuable elements of Mail Attender is the ability to identify and warn when a PST file is approaching this fatal limit. Defined as a rule, you can configure it to fire off a warning e-mail when a PST file reaches a definable percentage of this 2Gb limit – 80 per cent, for example.

For good measure, it's also possible to check disk usage and so ensure the PST file won't fill up an entire disk or partition – with similar disastrous results.

System requirements

Operating system: Windows 2000, XP with MSDE 2000 or later and IIS 5. Desktop systems need Outlook 98 in Corporate Workgroup mode. Compatible with Exchange 5.5 and above.

UK supplier

Pillar Solutions
Tel 01732 363670
E-mail
sales@pillar-solutions.com
Web
www.pillar-solutions.com

Cost

Price on application. As an example, it would be £10.50 per licence for 200 users.

Bottom line

Pros A single point of control for managing, policing and monitoring mailboxes and document retention across an enterprise.

Cons Limited online help and would benefit from improved reporting.