Global Relay - Searching for Emails - Standard and Advanced

Last Modified on 01/15/2016 4:52 pm EST

INTRODUCTION

The Message Archiver and Compliance Reviewer has dynamic search and recovery tools that enable messages to be located based on virtually any contents of the body, header and attachments.

Standard Search focuses on the Sender, Recipient, Subject, Date or contents of a message and can be performed by Standard User's with any level of experience. Basic Search is typically all a User needs when searching for their own messages in the archive.

Advanced Search supports Boolean logic, Wildcards, proximity searches and requires knowledge of these sophisticated search techniques. These powerful and versatile search techniques can locate specific messages based on subtle combinations of search criteria and are typically required when performing Audits and eDiscovery.

STANDARD SEARCH

Standard Search involves searching for a word, a string of words, a phrase or a combination. Users can select the Date Range(s), and all message types (i.e. Email, Blackberry, Bloomberg, Reuters, Instant Messages) that they would like to search. Global Mail users must select both Email and Sent Items to search all of their email messages.

Fields marked with a double asterisk (**) also support Advanced Search Techniques. See

Advanced Search Techniques for details

Start Date/End Date: Start Date and End Date narrows the search results to the days selected. Search results will include only messages sent on or between the date range selected. The default date range is the last seven (7) days.

Start Time/End Time: Within Start Date/End Date there is an option to include a Start Time and End Time. If no Start or End Time is defined by the User, the default is "all day",

meaning any message sent between midnight to midnight on the selected day. If a Start and End time are defined, the search results will include only messages sent on or between the hours/minutes selected.

Folder: Select the all applicable message types which are to be searched. If your company only archives one message type, this will be the default.

From (User)**: Searches for messages sent by an individual. Users may search on the complete first name, last name, email address, or domain name. A sub-string search is not automatically applied to words in a search, so Wildcard values need to be used when searching on only part of a sender's name or domain (see Advanced Search Techniques below). The more specific the search criteria entered, the more specific the results will be.

Message From	Will be found searching on...	Will not be found searching on...
Will.Baker@domain.com	"Will"; "Baker" or "domain.com"	"*baker"
wbaker@domain.com	"wbaker" or "domain.com"	"baker" or "*baker"
WilliamB@domain.com	"Williamb"; "William?"; "William*"; "Will*" or "domain.com"	"*b"
wbaker@uk.domain.com	"wbaker"; "wbak*" "domain.com" or "uk.domain.com"	"baker" or "*baker"

From (Group): Includes all members in the specified Group in the From search. (i.e. if there are 10 employees in a Group labeled "Sales" then all messages sent by these employees will be included in the search results.)

To/Cc/Bcc (Users)**: Searches for messages received by an individual, in either the To, Cc, or Bcc fields. Users may search on the first name, last name, email address, or domain name of the recipient. Users may also search on partial data. The more specific the search criteria entered, the more specific the search results.

To/Cc/Bcc (Groups): Includes all messages received by members in the specified Group in the To/Cc/Bcc search (i.e. if there are 10 employees in a Group labeled "Sales" then all messages sent to these employees will be included in the search results.

User Search Tips:

Addresses as phrases: The Message Archiver indexes message addresses as individual words (it does not recognize the period (.) between words in a message address (e.g. bob.smith@domain.com)). Because of this, the address of a sender or receiver is seen as a phrase of words. To find an exact sender or recipient, put the complete address "in quotation marks".

Multiple User Search: To search on a subset of Users within the company, place those Users into a Group and conduct a search on the Group. To retrieve all messages "To" and "From" a single User or a Group, you would conduct "To" and "From" searches separately. You can also

perform a Boolean search to find the multiple users with a single search (see Boolean Searches in the Advanced Search Techniques below for details).

Include All Data Types: Be aware of all possible email addresses for each User, including Bloomberg names or Instant Message User names, as you will need your search to cover all user addresses.

Searching on partial terms: a Wildcard substring search is not automatically executed for the From/To/Cc/Bcc (User) and must be explicitly specified by Users. In the Message Archiver v.5.x, entering a value such as "test" into the FROM field in the search page resulted in a sub-string search being automatically performed, so that any email address or username beginning with the word "test" was returned. In the Message Archiver 6.x, Users must explicitly enter "test*" to search for all email addresses or names that begin with the letters "test" in the FROM field in the search page.

Subject**: The Subject of a message varies depending on the message type. For email, the Subject is the Subject Line of the email, and a search against Subject will return email that has the search criteria in their Subject Line. For Chat, the Subject will return conversations from chat rooms containing the search criteria in the chat room name. The Subject line is not recommended for use with IM.

Attachments**: Filters a search by the type of attachment. Only messages with the specific attachment type will be found. Common file types are listed in the pull-down menu. If the file extension is not listed, select "Other..." and enter the extension name in the field provided. Messages with one or more attachment types can be returned by a single search by using a Boolean expression (e.g. "pdf AND gif"). Users can also search for a specific attachment name by selecting "Other..." and entering the attachment name and type (e.g. "document.txt").

Attachments Search Tips:

File Extensions: Applications such as Microsoft Word and Microsoft Excel have different file extensions for different version and document types. Users can search for more than one similar attachment type by using Wildcard characters (e.g selecting "Other..." and searching for ".doc*" will find not on ".doc" attachments, but also ".docx" attachments)

Optical Character Recognition: The Message Archiver does not perform OCR on flat files (images such as PDF, GIF, TIFF, JPG) when they are imported into the archive. Because these images are not converted to characters, it is not possible to search on the words contained in an image. Only the image metadata can be indexed and used in a search. This metadata includes the name of the image, type of image, date created and last modified

date.

Encrypted Attachments: The contents of an encrypted and/or password protected attachment cannot be indexed because the Message Archiver cannot bypass these security features. Only the attachment metadata can be indexed and used in a search. This metadata includes the name of the image, type of image, date created and last modified date.

Keywords**: The Keyword field allows the User to search for specific words or phrases in a message body (including attachment body). To look for a specific phrase, place the phrase in quotations, i.e. "confidentiality agreement". This will return messages with that exact phrase. Up to 1000 characters can be used to define the keywords in a search.

Keyword Search Tips:

Phrase Search: To search for a phrase, put the phrase to be searched in quotations (e.g. "this investment can't fail"). This ensures that the words in the phrase will be used in a search in the same order they appear in the phrase. If the phrase is not put in quotations then the resulting search will return the words in any order (e.g. a search for This is funny will return funny this is or This is not funny.

Encrypted Messages: The contents of an encrypted and/or password protected message cannot be indexed because the Message Archiver cannot bypass these security features. Only the message metadata can be indexed and used in a search. This metadata includes the sender, recipient, date sent and other metadata contained in the Header.

Priority: The Priority field enables Users to search on the current status of any message. The Priority filter can be used along with a Flag option to narrow a search.

Bloomberg: Bloomberg customers can filter a search against Bloomberg to return Bloomberg IB, Bloomberg Mail or both. This option requires the Bloomberg Folder to be selected.

Reuters: The Reuters filed allows Reuters Customers to search for conversation messages that contain one of the Reuters Messaging premium features: RM Chat, File Transfer, Forms and Screenshots.

Serial#: This field enables Users to search based on the unique sequentially serialized identifier assigned to every message conversation. Messages can be searched based on a single Serial #, entering multiple Serial #'s, each separated by a comma, or a message range by entering a serial number in the "from" Range field and entering a larger serial number in the "to" Range field.

ADVANCED SEARCH

Advanced Search provides powerful and versatile search techniques that can locate specific messages based on subtle combinations of search criteria and are typically required when performing Audits and eDiscovery.

Advanced Search Fields

Header: Users to search for metadata contained within the message X-header that cannot be otherwise leveraged for a search by another field in the Message Archiver and Compliance Reviewer interface. In the left hand field, enter the name of the Header Tag to be searched and in the right hand field enter the Header Value for which the User is searching.

In this version of the Message Archiver, the Header is indexed as a single block of text. Consequently, a search against the Header Tag searches all fields in the Header, including Header Tags that are otherwise exposed in the Message Archiver and Compliance Reviewer interface (such as Subject, From, To/Bcc/Cc, etc.).

Header Search Tips:

Sub-string Search: When performing a search on a value in the Header Tag, it is not necessary to enter the name of the full header tag. Entering a partial header tag is sufficient (e.g. it is sufficient to enter "acceptlanguage" in place of "X-GR-MA-acceptlanguage").

Boolean Search: Boolean search is not available in Header Tag (e.g. Users cannot search for a Header Tag of "Message Archiver" AND "Exchange"; however, it is available in the Header Value field.)

Wildcard Search: Wildcard * and ? are not supported in Header Tag search. So the following searches are not supported: Message* Exchang?

Flag: The Flag field enables Users to search on the current Flag status of any message. The Flag filter can be used along with a Priority Flag option to narrow down a search.

Label: Labels are created by Reviewers and Super Reviewers to assist with organizing and categorizing messages. Use the Label drop down to select a Label and search for messages to which this Label has been applied.

Event: Events are used to search the Audit Trail associated with each message. Use the

Event drop down to select an Event and search for messages to which this Event has occurred. Optionally, a user name can be added to the field below to restrict the Event search to this specific individual (i.e. all messages "Viewed" by "Bob Brown").

Advanced Search Techniques

Wildcard Searches

Wildcards in a search are characters that will match any character. They are useful in searches when only part of the search criteria is known (i.e. if searching for someone with the first name of Jacobs or Jacobson the Wildcard search would be "Jacob*"). Using a Wildcard as the first character in a search (e.g. *stone) is not supported.

The Message Archiver supports single and multiple character Wildcard searches within a single term, but not within a phrase.

Single Character Wildcard: The single character Wildcard search looks for terms that match that with the single character replaced. To perform a single character Wildcard search, use the "?" symbol. For example, to search for "text" or "test" you can use the search: te?t

Multiple Character Wildcard: Multiple character Wildcard search looks for 0 or more characters. To perform a multiple character Wildcard search, use the "*" symbol. For example, to search for test, tests or tester, use the search: test*. The multiple character Wildcard search can also be used in the middle of a term (e.g. te*t).

Notes:

1. Wildcard characters * and ? cannot be uses as the first character of a search.

2. A filename and extension separated with a period (.) are considered two words for a Wildcard search (e.g. "Testfile.txt" is considered to be two words and a search for "Testfile*txt" will not be "Testfile.txt").

3. Wildcard characters will not work within a phrase (e.g. "This is a test*" will drop the * in the search).

4. Searches that include a Wildcard character after a period in a message address will fail when applied to FROM field searches.

5. Wildcard substring search is not automatically executed for the From/To/Cc/Bcc (User) and must be explicitly specified. In the Message Archiver v.5.x, entering a value such as "test" into the FROM field in the search page resulted in a sub-string search being automatically performed, so that any email address or username beginning with the word

"test" was returned. In the Message Archiver 6.x, Users must explicitly enter "test*" to search for all email addresses or names that begin with the letters "test" in the FROM field in the search page.

Proximity Searches

The Message Archiver supports finding words are a within a specific number of words of each other. This supports searching for keywords that have a relationship to each other but which may not always be entered in exactly the same way each time. For example, the phrase "this investment can't fail" might also be in a message as "this investment in the swamplands can't possibly fail", in which case searching for the exact phrase would not find both. Proximity searching makes it possible to find both phrases by searching for occurrences of the keywords "investment" and "fail" within a defined number of words of each other.

To do proximity search use the tilde "~", symbol at the end of a phrase. For example, to search for "investment" and "fail" within 10 words of each other in a document use the search: "investment fail"~10.

Boolean Searches

Boolean searches allow you to combine words and phrases using the words AND, OR, and NOT to limit, widen, or define your search.

AND

TermA AND TermB matches documents where both terms appear anywhere in the single document. The terms can be single words or phrases. The symbol "&&" or plus "+" can be used in place of the word AND. The word AND must be capitalized.

Examples:

Investment AND Guarantee Investment && Guarantee

"Investment Banker" and "Money back guarantee" "Investment Banker" && "Money back guarantee"

The AND operator is the default conjunction. If there is no Boolean operator between two terms the AND operator is used by default. For example:

"Investment Guarantee" or Investment AND Guarantee

OR

TermA OR TermB match documents where either term appear anywhere in the single document. The terms can be single words or phrases. The double-pipe symbol "||" can be used in place of the word OR. The word OR must be capitalized.

Examples:

Foolproof OR Guarantee Foolproof || Guarantee "Can't Lose" OR Guarantee

"Can't Lose" || Guarantee

NOT

TermA NOT TermB match documents which only the first term appears anywhere in the single document and the second term does not appear anywhere in the same document. The exclamation point "!" or minus "-" can be used in place of the word NOT. The word NOT must be capitalized.

Examples:

Guarantee NOT Guaranteed Guarantee ! Guaranteed

"Personal Guarantee" NOT "Guarantee Success" "Personal Guarantee" ! "Guarantee Success"

The NOT operator cannot be used with just one term. For example, the following search will return no results: NOT "Guarantee Success".

Grouping

You can control the precedence of the Boolean operators using brackets. In the query one OR two AND three the AND takes precedence, so this is the same as one OR (two AND three). You can override the precedence using (one OR two) AND three.

To search for either "Foolproof" or "Guarantee" and "Broker" use the query: (Foolproof OR Guarantee) AND Broker

Notes:

- Searching with the Message Archiver is not case specific other than when using the Boolean operators AND, OR and NOT. These must be capitalized.