Search Criteria

https://campus.barracuda.com/doc/43222968/

The **Search Criteria** dialog allows you to define the search criteria for your policy search:

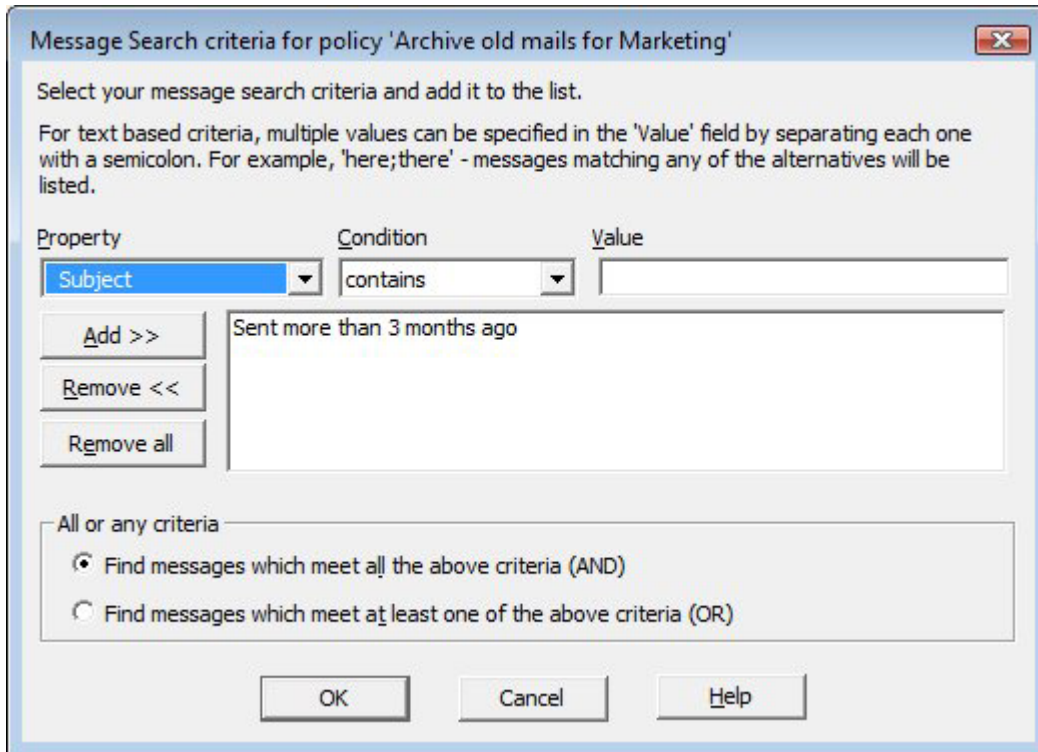Search criteria is split into four levels:

- **Store** criteria (these differ between mailbox and PST policies).
- **Folder** criteria.
- **Message** criteria, which includes the number of attachments.
- **Attachment** criteria.

When selecting attachment search criteria, you can choose whether attachments must meet ALL or ONE of the search criteria.

When defining search criteria, you can specify whether all or only one of the search criteria must be met by 'AND'ing or 'OR'ing the conditions together. Note that criteria at each level must be met before the next level is considered. That is, criteria at different levels are always 'AND'ed together.

Use the **Message Search criteria** dialog to define the search criteria for your policy search. A search criterion has three parts, indicated by the three fields along the top of the dialog:

- **Property** of the message to search on – Some of the available options are properties of the attachments, if any, to the message.
- **Condition**, such as 'contains' or 'less than' – The range of conditions available depends on the selected property type, string vs numeric.
- **Value** used to compare with the property's value. For instance, in the criterion 'Subject starts with "hello"', 'subject' is the property, 'starts with' the condition, and 'hello' the value. If you enter multiple criteria, only those messages that match all the criteria are returned.

Property

Properties are divided into groups.

- Standard message properties, such as:
  - Subject.
  - Type – appointment, task, or normal message.
  - Body (not including attachments) – When specifying a value to search for, you cannot specify an end-of-line character, and since the message usually ends with an end-of-line, then 'ends with' is not a condition you can use.
  - From, To, Cc, and Bcc. All forms of the user's address are searched, including their display

name, e-mail address and, if they are an internal user, all their proxy addresses (these are addresses as defined on other mail systems such as MSMail and SMTP) both with and without the address type prefix, e.g., **SMTP:**). Note that a semicolon in an address (such as an X400 address) is interpreted as a separator between alternative values to search for, not as a part of the address. The search criterion **recipient** includes From, To, Cc, and Bcc.

  ○ Last modified – message's creation and delivery modification times. You can enter dates (not times) for comparison, that must either be for a specific date, such as 1st March 2004, or a relative date, such as 3 days ago.
  ○ Total size, including attachments, counted in K.
  ○ Whether the message is a message link – one created by ArchiveOne when it moves a message into an archive.
- Attachment properties, such as:
  ○ Attachment file name – note that you cannot use '*' as a wildcard in attachment filenames. For instance, if you want to search for attachments of type AVI, then don't set the criterion as 'Attachment filename contains "*.AVI"' but use 'Attachment filename ends with ".AVI"'.
  ○ Attachment size, counted in K.
  ○ Text in the attachment – If the selected property is a property of an attachment, and the message does not have an attachment, then the message necessarily fails the search. If there is more than one attachment, specify whether ALL or ONE of the attachments must meet the attachment criterion.

> **Example**
> Ff the criterion is **Attachment size less than 20** (meaning 20K) and the message has no attachments, it fail to meet the criterion. If it has two attachments, one of 10K and one of 30K, then the message succeeds if the attachments setting is set to **at least one attachment meets criteria** but fails if the setting is **all attachments meet criteria**.

  ○ The policy results file highlights all attachments that meet the criteria. The text in the attachment can be searched if the **Document text** search criterion is selected. The process uses the Microsoft IFilter API to extract words from formatted documents, so any document format for which an IFilter is installed is searched including text files, office documents, and HTML. Note that Microsoft Office does not need to be installed. If the attachment is a ZIP file, all files inside the ZIP are searched. Note that file types such as **.log** files are not searched as they are not registered file types.

  > To search other file types, contact the application vendor that generates the file and determine if they have an IFilter DLL available.

  ○ If PSTs are searched using **AOnePolPSTProc** then searching into documents uses IFilter if it is available (if the PC running **AOnePolPSTProc** is Windows 2000 or later), otherwise it uses a binary search into attachments, i.e., it assume all attachments are text files.

- Folder properties, such as:
  ○ Folder name.
  ○ Folder's default message type. For instance, the **Calendar** folder has a default message

type of **appointments**. When you create a new folder, you can specify the default message type contained by the folder.

- Folder path, including parent folders. Typically this is used for folders in mailboxes in order to identify a folder and its subfolders. Mailbox folder paths start with a backslash (\) character, and public folder paths start with a backslash (\) but do not include **All Public Folders**. For instance, the criterion **Folder path starts with '\Inbox'** finds the **Inbox** folder and all subfolders, and **Folder path starts with '\Inbox\'** finds subfolders of the Inbox but not the Inbox itself.
- Whether the folder is replicated.
- Mailbox properties, such as:
  - Size or number of messages in the mailbox.
  - Mailbox size compared to its quota – for instance, is the mailbox more than 90% of its quota size. There are three quotas that can be defined for a mailbox using **Active Directory Users and Computers**, called **Issue warning at**, **Prohibit send at**, and **Prohibit send and receive at**, which are the three limits that ArchiveOne can compare against.
- Properties specific to appointments and tasks.
  - Be aware that checking for recurring appointments may be predictable. For instance, trying to delete all appointments before a given date may delete all instances of a recurring appointment or none of them, depending on when the recurring appointment was created. For more reliable results, you can combine such actions with the **is appointment recurring** criterion and only delete non-recurring appointments.
  - Appointment busy status (0-3) which can be 0=free, 1=tentative, 2=busy or 3=out of office.
  - Task status (0-4) which can be 0=not started, 1=in progress, 2=completed, 3=waiting on someone else or 4=deferred.
- Less commonly used message properties, such as:
  - Conversation name, which is a property common to an original message and its replies (typically subject of the original message) – this is used by Outlook to group messages and replies together.
  - Importance, as set by the message sender from Outlook – this can be 0 (low), 1 (normal) or 2 (high).
  - Priority – Property assigned by the messaging system of what priority to give processing the message, and can be -1 (non-urgent), 0 (normal) or 1 (urgent)
  - Sensitivity, as set by the message sender from Outlook – this can be 0 (normal), 1 (personal), 2 (private) or 3 (company confidential).
  - Message class – this can be used to distinguish forms from normal messages.
  - The read/unread status of the messages. This is only meaningful for messages in mailboxes and corresponds to whether the message appears in bold in the list of messages in Outlook. If a read message is changed to unread status using the Outlook menu option, then it appears as unread to ArchiveOne.

Enter the criterion details and click **Add** to add it to the list.

If you have defined any custom properties to search for, these are listed in the **Property** drop-down

menu in the **Custom properties** section. If there are multiple criteria, you can choose whether the object is selected if it meets ALL the criteria. If you only define search criteria at, for instance, the folder level, then all messages in matching folders are processed.

If the property being searched for is text, then you can specify multiple alternative values – the message is selected if any of the alternatives are found. Specify alternatives by putting semicolons between the alternatives in the value box. For instance, the criterion **Body text contains "christmas;easter"** finds all messages referring to either Christmas or Easter. The criterion **Attachment filename ends with ".EXE;.DLL;.OCX"** finds any attached EXE, DLL or OCX files.

Some of the text search criteria include **(word)**. This means they search for whole words. For instance, the criterion **Subject contains "at"** selects messages with a subject such as **bats** since the word **bats** contains the word **at** within it, but the criterion **Subject contains (word) "at"** only selects messages containing **at** as a word on its own (preceded and followed by characters which are not letters).

All searches are case insensitive. You cannot search for a semicolon as it is interpreted as specifying alternatives, or special characters such as end-of-line or tab, and you can search for an asterisk (*****) but a warning displays in case you are trying to use it as a wildcard character. All spaces are included in the search, so if you put a space on either side of a semicolon, as in **"christmas ; easter"** then the message must have a space there as well in order to match.

During a search, the **subject**, **body** and **subject and body** criteria and the attachment criteria (**name**, **size**, and **attachment content**) are applied to embedded messages, but no other criteria (such as delivery time). That is to say, a search for **"subject contains X"** finds a message that has an embedded message with a subject that contains **X**, but a search for **"delivered more than 100 days ago"** does NOT find a message that was delivered more recently than 100 days but has an embedded message that was delivered more than 100 days ago.

Figures

1. search01.png
2. search02.png