WHITE PAPER: TECHNICAL

symantec™

Confidence in a connected world.

# Discovery Accelerator 8

## Effective Searching

*Logan Sutterfield, Principal E-Discovery Specialist*

*May 2010*

# Content

# Introduction

The purpose of this document is to provide guidance for creating and running searches in the Symantec Discovery Accelerator application.

The information in this document will describe the process and assist the reader with understanding:

- Search Basics
- Simple Searching
- Advanced Searching
- Analytical Searching

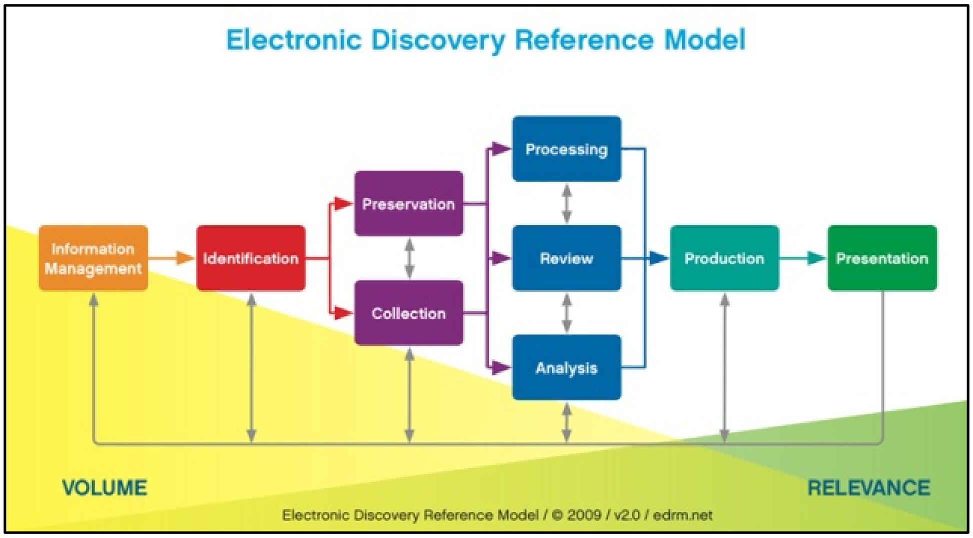
In each section, there will be examples of some of the most common configurations for search criteria to assist the reader with creation of accurate searches. Simple, Advanced, and Analytical searching will be discussed from the perspective of Discovery Accelerator version 8.0 application capabilities.

## Target Audience

This document is intended for Attorneys, Paralegals, or Litigation Support Professionals who utilize Discovery Accelerator to perform collection searches in response to eDiscovery requests.

## The Electronic Discovery Reference model – EDRM

From the perspective of the Electronic Discovery Reference Model, this document will address methods for “Collection” and “Processing”. Although not discussed in detail in this document, the “Preservation” step is also facilitated by utilizing the Discovery Accelerator Legal Hold capabilities. Symantec is actively participating in EDRM.



### Symantec Discovery Accelerator

Discovery Accelerator extends the basic search functionality of Enterprise Vault E-mail, file, SharePoint, Instant Messaging, and structured data archiving to help lower the cost of data collection and preservation and to facilitate the review and analysis of archived items in electronic discovery.

The release of Discovery Accelerator 8.0 provides significant enhancements, delivering a more powerful and efficient user interface through advanced search and analysis capabilities such as Guided Review, Conversation Threading and Bulk Marking. Relevant items are easily preserved and provided to the requesting party through a flexible export process to simplify production.

### Technical Considerations

A very important note: Please engage the Enterprise Vault and Email administrator to gain an understanding of how your environment is configured. The Enterprise Vault considerations in Appendix A of this document will help ensure the accuracy of your search results.

## Understanding Cases and the Research Folder

In this section, we will briefly discuss the uses and differences between the Case and the Research Folder. Before searching with Discovery Accelerator, you should have a clear understanding of when to use Research Folders and Cases.

### Cases

The Case is meant to be used for everything that is related to a discovery action including searching, legal hold, review, analysis, and production. Within a single Discovery Accelerator system, reviewers can work on multiple Cases simultaneously. Discovery Accelerator 8.0 provides a new “Analytics” option for Cases or Research Folders provides additional analysis of the metadata and content for items that were collected during a search.

### Research Folders

The Research Folder is meant for researching matters or performing “Early Case Assessment” when a claim has been made. The Research Folder has the capability of running searches against data in Enterprise Vault to help with initial investigation into a matter. By creating one or more Research Folders, you can work privately on the items that interest you without generating additional work for other reviewers.

For example, suppose that you are pursuing an alleged instance of insider trading. Rather than add a large number of search results to the review set, where they are visible to other reviewers, you can conduct the searches from a Research Folder and store the results there. Then you can review and mark the items in the normal way, or export them for offline review. Research Folders provide almost the same functionality as Cases. Like Cases, you can enable analytics on a Research Folder. However, unlike Cases, Research Folders cannot place items on legal hold.

# Archive Search Security

Some organizations have a requirement to only allow specific reviewers the ability to search executives or VIP data to maintain the highest level of privacy. Discovery Accelerator version 8.0.3 and above enables an administrator to control search and review permissions at the archive level to facilitate the required privacy.

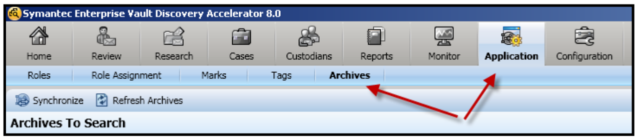
## Selecting the archives in which to search

You can customize the list of Enterprise Vault archives in which Discovery Accelerator searches for items. For example, there may be archives that you want to exclude from any searches because they contain irrelevant material. As well as setting the default, global list of archives, which are available to the searches that you conduct in any case, you can customize the searchable archives for individual cases.

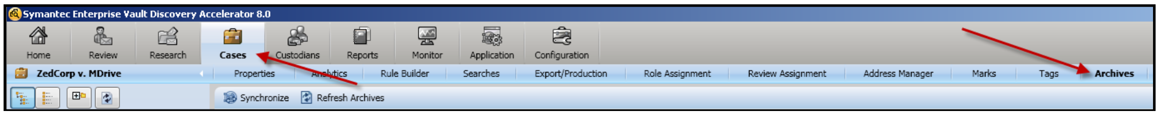
You must have the application permission Manage Archives to set the global list of archives, and the case permission Manage Archives to set a case-level archive list.

**To select the archives in which to search**

1. Perform one of the following:
   - To set the default list of archives that are available to all cases, click the Application tab in the Discovery Accelerator client, and then click the Archives tab.



   - To set the list of archives in which to search for one case only, click the Cases tab and then click the required case in the left pane. Then click the Archives tab.

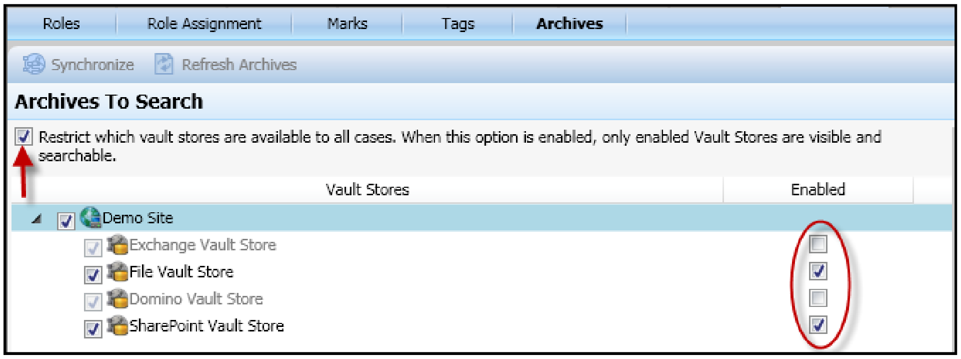


If Discovery Accelerator lists a lot of cases, you can filter the list with the fields at the top of the pane. As well as filtering the cases by name, you can choose whether to list any research folders that are associated with them.

2. Choose the archives in which to conduct searches.

Use the following techniques to include or exclude archives:

- If you are setting the application-wide list of archives that are available to all cases, and you want to hide certain vault stores from case administrators, check Restrict which vault stores are available to all cases.



Archives To Search

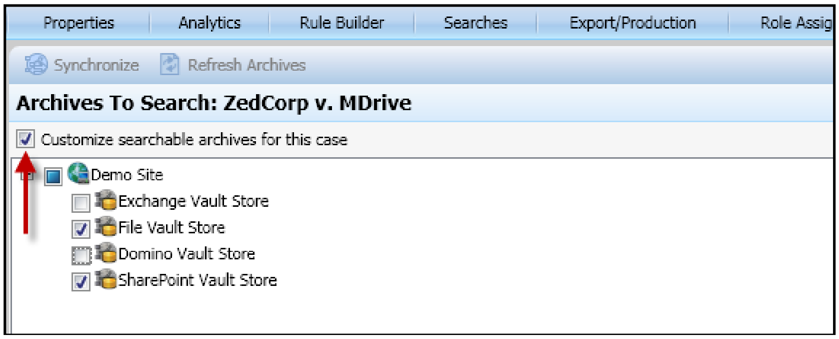
☑ Restrict which vault stores are available to all cases. When this option is enabled, only enabled Vault Stores are visible and searchable.

| Vault Stores | Enabled |
|---|---|
| ☑ Demo Site | |
| ☑ Exchange Vault Store | ☐ |
| ☑ File Vault Store | ☑ |
| ☑ Domino Vault Store | ☐ |
| ☑ SharePoint Vault Store | ☑ |

Then, in the Enabled column of the vault store list, check the vault stores that you want to make visible and searchable. When a case administrator sets the list of searchable archives for a case, only those archives that are in enabled vault stores are available for selection.

If you restrict a vault store and then later remove the restriction, the vault store automatically becomes available to existing cases, where it is included in new searches.

- If you want to set the list of archives in which to search for one case only, check Customize searchable archives for this case.



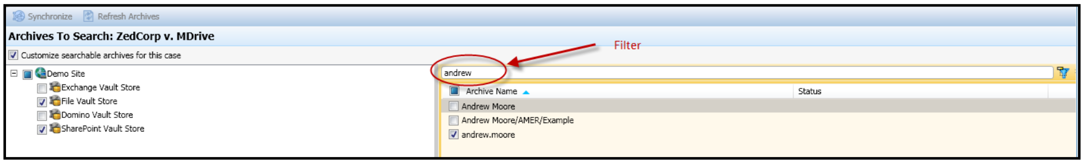
Archives To Search: ZedCorp v. MDrive

☑ Customize searchable archives for this case

■ Demo Site
☐ Exchange Vault Store
☑ File Vault Store
☐ Domino Vault Store
☑ SharePoint Vault Store

- Check or uncheck a vault store at the left to include its archives in searches or exclude them from searches.

- Click a vault store at the left to list the associated archives at the right. Then check or uncheck the archives to include or exclude them.



**Archives To Search: ZedCorp v. MDrive**

☑ Customize searchable archives for this case

- Demo Site
  - □ Exchange Vault Store
  - ☑ File Vault Store
  - □ Domino Vault Store
  - ☑ SharePoint Vault Store

andrew

| | Archive Name | Status |
|---|---|---|
| □ | Andrew Moore | |
| □ | Andrew Moore/AMER/Example | |
| ☑ | andrew.moore | |

If Discovery Accelerator lists a large number of archives, you can filter the list with the fields at the top of the right pane.

- Check or uncheck the Archive Name box at the top of the right pane to include or exclude all the available archives.

3. Click Save.

## Search Basics

Once a Case or Research Folder has been created, collection searches may be created and run within each. The following are typical activities:

- Running one or more searches on the relevant vault stores for suitable information. Discovery Accelerator offers a wide range of search criteria from which to choose: words and phrases to look for, date ranges, message size, author and recipient addresses, and more.

- Browsing the search results to assess their suitability, and then either accepting or rejecting the results.

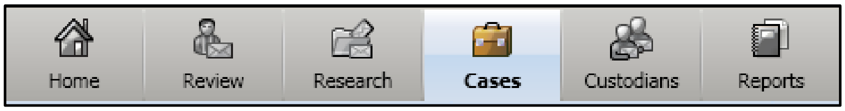
- Searching again, until you have amassed all of the data required.

When a meaningful result set has been collected and accepted, the review interface may be utilized for culling down to what is relevant.

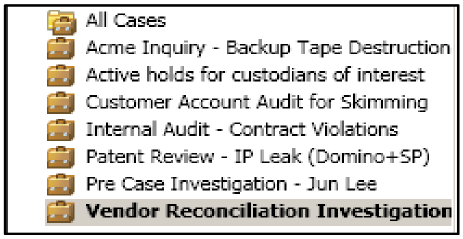
Search schedules may be created to run searches at set times or set up recurrent searches that run automatically. The Enterprise Vault archive list may also be customized to control where Discovery Accelerator searches for items.

## Accessing the Search Module

To access the search module, log into the Discovery Accelerator and select “Cases” from the application toolbar.



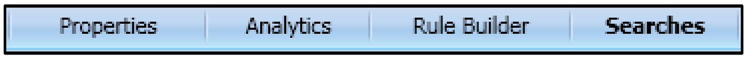
Proceed to the “Search Dashboard” by selecting the Case from the case list in the left portion of the cases interface.



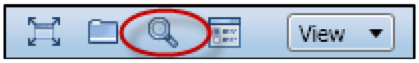
All Cases
Acme Inquiry - Backup Tape Destruction
Active holds for custodians of interest
Customer Account Audit for Skimming
Internal Audit - Contract Violations
Patent Review - IP Leak (Domino+SP)
Pre Case Investigation - Jun Lee
**Vendor Reconciliation Investigation**

Discovery Accelerator will list all Cases and Research Folders in which you have permissions to access. If there are many, you can search the list in the field located just above the left pane.

Then select the “Searches” from the Case menu.

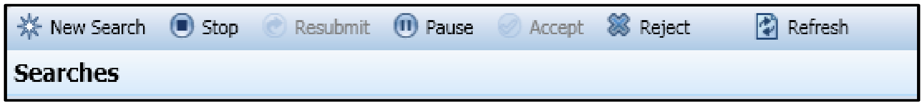


Optionally the search interface may be accessed from the review interface by clicking the magnifying glass icon from the review toolbar.

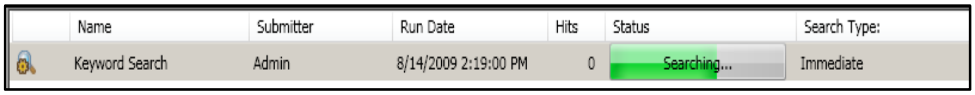


## The Search Dashboard

The Search Dashboard enables you to view the status of all searches for the Case. If a search is running, pending, or has been accepted into review, it will appear here. Let’s discuss each area of the dashboard.

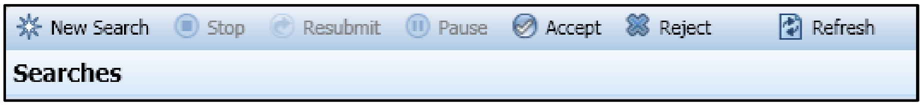


The top portion of the dashboard will be referred to as the “Search Action” menu. Here you will have options to create a new search, pause or stop an active search, or refresh the search status area.

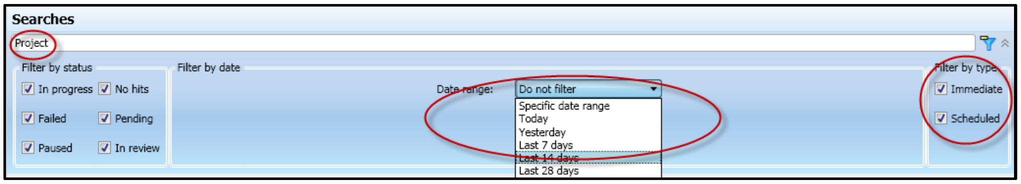


| | Name | Submitter | Run Date | Hits | Status | Search Type: |
|---|---|---|---|---|---|---|
| | Keyword Search | Admin | 8/14/2009 2:19:00 PM | 0 | Searching... | Immediate |

While the search is active, the dashboard will display the status of "Searching." The status will continue to refresh every minute (configurable) until the search completes, and will then change to the status of "Pending Acceptance".



Once the active search has completed, the "Accept" option is made available. You will now have the option to accept or reject the search based on the results. If the search was configured for "Automatically Accept", then the results will be immediately accepted into the Case and you will not have the opportunity to browse the results before committing the search to the Case. If "Accept" has not been pre-selected, you may preview the results before accepting them into a Case.



Searches

Project

Filter by status

☑ In progress ☑ No hits

☑ Failed ☑ Pending

☑ Paused ☑ In review

Filter by date

Date range: Do not filter

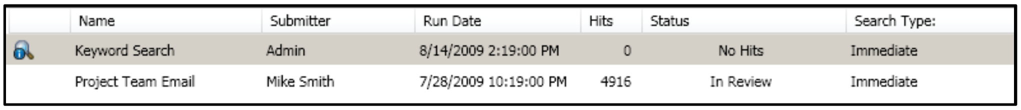
Specific date range
Today
Yesterday
Last 7 days
Last 14 days
Last 28 days

Filter by type

☑ Immediate

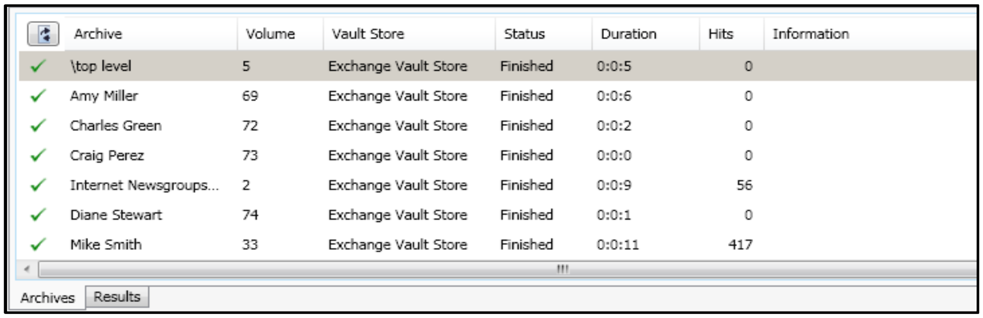
☑ Scheduled

Just below the search action menu, you have the ability to filter which of the searches are visible on the dashboard. The options for filtering include name, status, date range in which it was run, and type (Immediate or Scheduled).



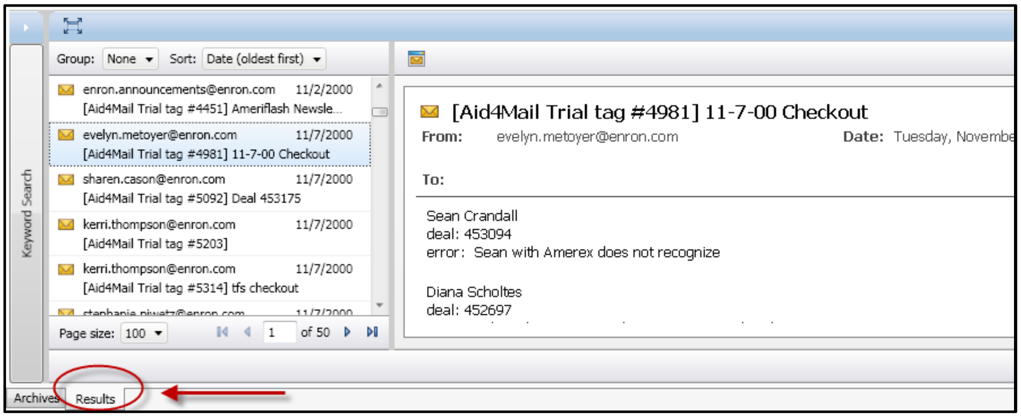
| | Name | Submitter | Run Date | Hits | Status | Search Type: |
|---|---|---|---|---|---|---|
| | Keyword Search | Admin | 8/14/2009 2:19:00 PM | 0 | No Hits | Immediate |
| | Project Team Email | Mike Smith | 7/28/2009 10:19:00 PM | 4916 | In Review | Immediate |

In the search status area, you may view all searches based on the filter selections. The status area will also display the user who submitted the search, the data and time it was run, the number of hits, and the search type.



| | Archive | Volume | Vault Store | Status | Duration | Hits | Information |
|---|---|---|---|---|---|---|---|
| ✓ | \top level | 5 | Exchange Vault Store | Finished | 0:0:5 | 0 | |
| ✓ | Amy Miller | 69 | Exchange Vault Store | Finished | 0:0:6 | 0 | |
| ✓ | Charles Green | 72 | Exchange Vault Store | Finished | 0:0:2 | 0 | |
| ✓ | Craig Perez | 73 | Exchange Vault Store | Finished | 0:0:0 | 0 | |
| ✓ | Internet Newsgroups... | 2 | Exchange Vault Store | Finished | 0:0:9 | 56 | |
| ✓ | Diane Stewart | 74 | Exchange Vault Store | Finished | 0:0:1 | 0 | |
| ✓ | Mike Smith | 33 | Exchange Vault Store | Finished | 0:0:11 | 417 | |

In the results area, at the lower portion of the dashboard, you are able to view the number of hits by archive. The results area will also display the volume the archive resides in, the vault store, the individual archive status, and the duration of the search per archive.



enron.announcements@enron.com 11/2/2000
[Aid4Mail Trial tag #4451] Ameriflash Newsle...

evelyn.metoyer@enron.com 11/7/2000
[Aid4Mail Trial tag #4981] 11-7-00 Checkout

sharen.cason@enron.com 11/7/2000
[Aid4Mail Trial tag #5092] Deal 453175

kerri.thompson@enron.com 11/7/2000
[Aid4Mail Trial tag #5203]

kerri.thompson@enron.com 11/7/2000
[Aid4Mail Trial tag #5314] tfs checkout

[Aid4Mail Trial tag #4981] 11-7-00 Checkout

From: evelyn.metoyer@enron.com

Date: Tuesday, Novembe

To:

Sean Crandall
deal: 453094
error: Sean with Amerex does not recognize

Diana Scholtes
deal: 452697

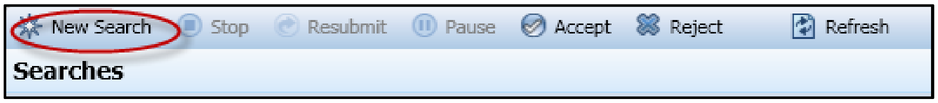
Upon completion of a search, you will be able to browse the results to check for accuracy. In the lower portion of the results area, there is an "Archive" tab which displays the individual archive information and a "Results" tab that will display a list of all results and preview the result. There are only options for sorting and viewing in this area. To take action on a result set such as marking or applying legal hold, the search must be accepted into the Case.

## Search Page Layout

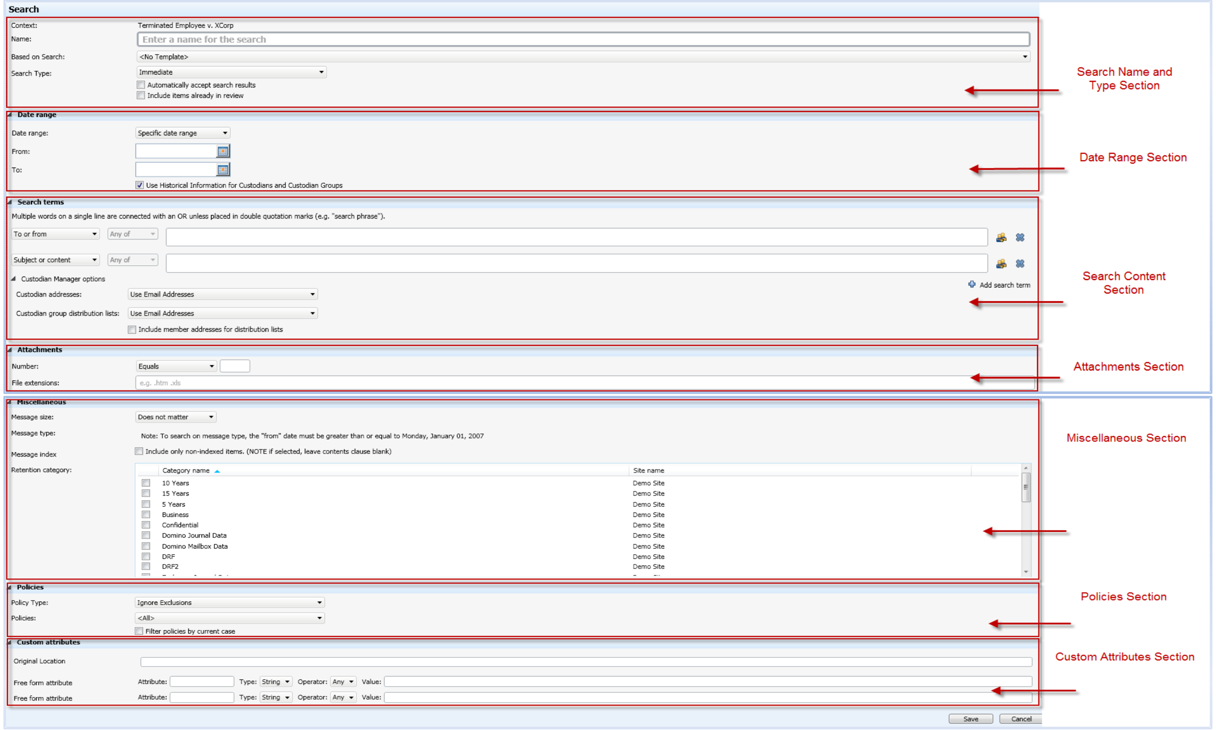
Is this section we will discuss the layout of the search page, the different options for constructing a search, and special considerations when running a search.

The search page enables immediate or scheduled searches to be created and run against all data stored in Enterprise Vault. Where there are many options to construct the search please pay special attention to how each search option interacts with other options on the page. The behavior of search options when compared to the others will be a Boolean AND. For example, a search term in the subject field and the content field along with a specified attachment or retention period will return only the results that meet all of the search criteria.

You can access the search page by selecting "New Search" from the search action menu in the search dashboard.



Selecting “New Search” will open up a blank search page that will return results for that specific Case.



**Search**

Context: Terminated Employee v. XCorp
Name: Enter a name for the search
Based on Search: <No Template>
Search Type: Immediate
□ Automatically accept search results
□ Include items already in review

**Date range**

Date range: Specific date range
From:
To:
☑ Use Historical Information for Custodians and Custodian Groups

**Search terms**

Multiple words on a single line are connected with an OR unless placed in double quotation marks (e.g. "search phrase").

To or from | Any of
Subject or content | Any of

Custodian Manager options
Custodian addresses: Use Email Addresses
Custodian group distribution lists: Use Email Addresses
□ Include member addresses for distribution lists

**Attachments**

Number: Equals
File extensions: e.g. .htm .xls

**Miscellaneous**

Message size: Does not matter
Message type: Note: To search on message type, the "from" date must be greater than or equal to Monday, January 01, 2007
Message index □ Include only non-indexed items. (NOTE if selected, leave contents clause blank)
Retention category:

| | Category name | Site name |
|---|---|---|
| □ | 10 Years | Demo Site |
| □ | 15 Years | Demo Site |
| □ | 5 Years | Demo Site |
| □ | Business | Demo Site |
| □ | Confidential | Demo Site |
| □ | Domino Journal Data | Demo Site |
| □ | Domino Mailbox Data | Demo Site |
| □ | DRF | Demo Site |
| □ | DRF2 | Demo Site |

**Policies**

Policy Type: Ignore Exclusions
Policies: <All>
□ Filter policies by current case

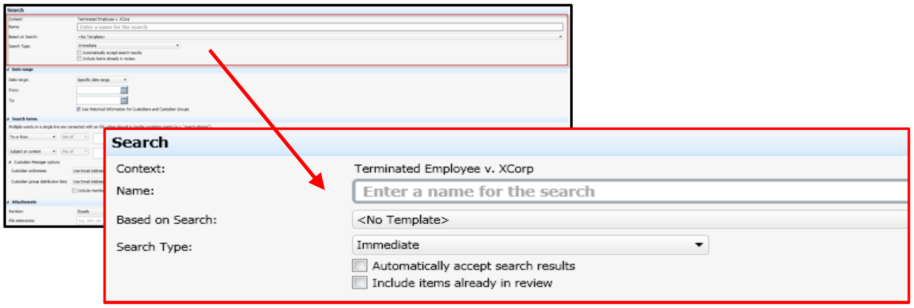
**Custom attributes**

Original Location
Free form attribute Attribute: Type: String Operator: Any Value:
Free form attribute Attribute: Type: String Operator: Any Value:

Discovery Accelerator groups the search criteria options into multiple sections which are described below. Below is an image of the blank search page, if you do not see all fields in your Discovery interface, you may click the arrow icons at the right to expand the sections.

## Search Name and Type Section

This section will describe the options when configuring the name and type search you will be running. Use the image below to reference the different areas of this section.



**Search**

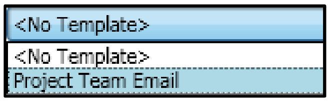
Context: Terminated Employee v. XCorp
Name: Enter a name for the search
Based on Search: <No Template>
Search Type: Immediate
□ Automatically accept search results
□ Include items already in review

## Context

Identifies the Case or Research Folder in which the search will run. When the Research Folder is not linked to any Case, "My Research "appears.

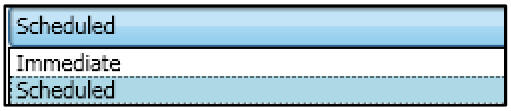
### Name

Specifies a name for the search, such as “Key Word Search John Doe”.



### Based on Search

Allows you to select an existing search as the basis on which to set the criteria for the new search.

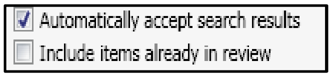


### Search Type

This option specifies whether the search should run immediately or run at a scheduled time. If you select Scheduled, you can specify a period during which the search is to run. See “Search Scheduling”.

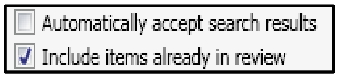
### Automatically accept search results

Specifies whether to add the search results to the review set automatically. This option may be useful for any proven searches that you intend to run on a regular basis. If you check "Automatically accept search results", you cannot reject the results and change the search criteria.  In other words, there is no way to “un-accept” a previously accepted search.  We recommend that you uncheck "Automatically accept search results" until you have tested that the search returns the expected results.



☑ Automatically accept search results
□ Include items already in review

A search that returns an error from any archive is not automatically accepted, regardless of this setting.



□ Automatically accept search results
☑ Include items already in review

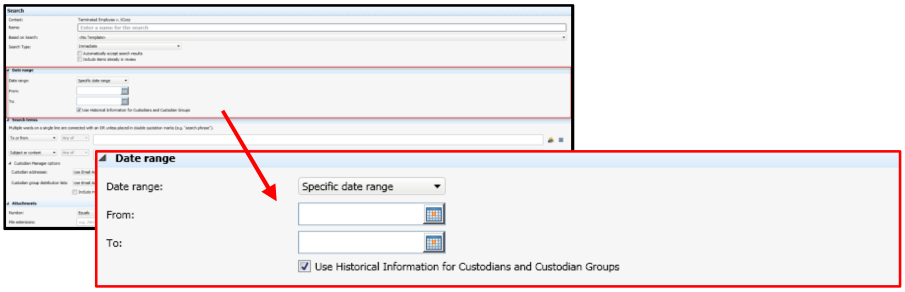
### Include items already in review

Specifies whether the search results can include the items that you have previously captured and added to the review set.  This option gives you control over whether to combine the results of subsequent searches or keep a unique reference to the result on a “per search” basis.  When a search is “Accepted”, the results returned are being compared to every other search result within the Case to ensure that no duplicate results will be added to the Case.

Please refer to Appendix B of this document for use cases of the option “Include items already in review”

## Date Range Section

This section will discuss the options when configuring the date range for the search you will be running.  Use the image below to reference the different areas of this section.



Date range

Date range: Specific date range

From:

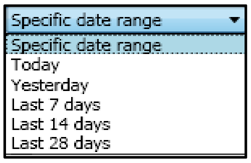
To:

☑ Use Historical Information for Custodians and Custodian Groups

### Date Range

Limits the search to items that were sent or received during the selected period.  The date ranges are relative to when the search runs, which is today in the case of an immediate search.

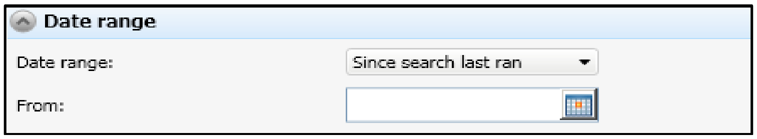
You may find these options useful when creating a scheduled, recurrent search that runs once every day, week, two weeks or four weeks. For example, if the search runs once a week, select "Last 7 days" to limit the range to the days since the search last ran.



### Since Last Search Ran

For a scheduled search only, this option allows the searching of new items that have arrived since the last time you ran the search. This option is similar to options such as Today and Yesterday. However, it lets you set an explicit start date for the first run of the search.

By default, this option searches from the date of the last run (or the start date for the first search) to the current day minus 1 (that is, up to yesterday).

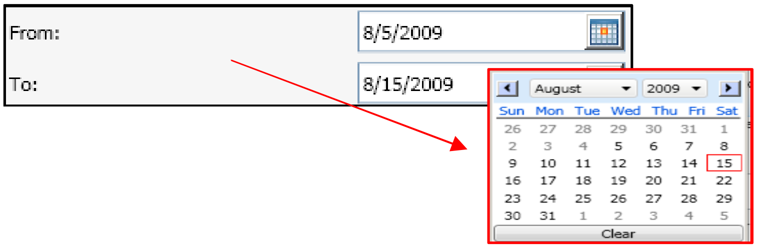


Date range: Since search last ran

From:

### Specific date range

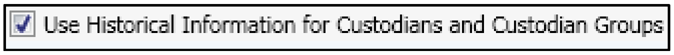
Enables searching for items that were sent or received during a longer or more specific period than the other date range options permit. To enter a date, click the buttons at the right of the From and To boxes, then select the required date.  Unlike the other date range boxes, a specific date range remains static and not relative to when the search runs.



From: 8/5/2009

To: 8/15/2009

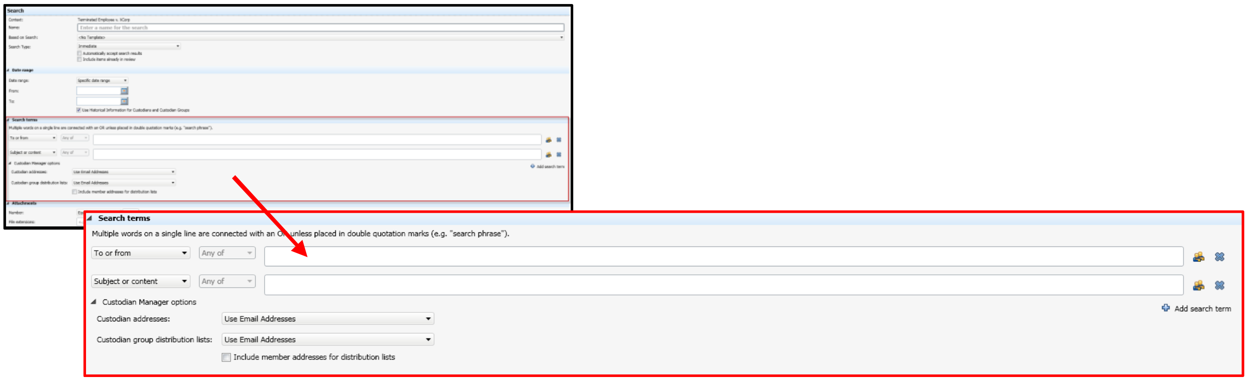
Check "Use Historical Information for Custodians and Custodian Groups" to use both the current and historical information for Custodians and Custodian Groups in the search. If you uncheck this option, Discovery Accelerator uses only the current set of Custodians, groups, and E-mail addresses. Any users that had name or email changes, or were deactivated due to termination are excluded from the search.



☑ Use Historical Information for Custodians and Custodian Groups

## Search Terms Section

This section will describe the options when configuring the author, recipient, subject, and content of your search. Use the image below to reference the different areas of this section.



Multiple words on a single line are connected with an OR unless placed in double quotation marks (e.g. "search phrase").

To or from | Any of

Subject or content | Any of

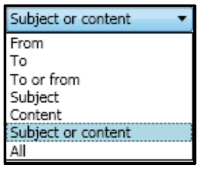
Custodian addresses: Use Email Addresses

Custodian group distribution lists: Use Email Addresses

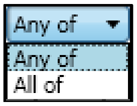
□ Include member addresses for distribution lists

The Search terms section specifies the words or phrases for which Discovery Accelerator should search in items. Click Add search term to add each word or phrase for which you want to search.

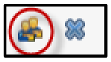
- Modify the value of the search term field utilizing the drop-down menu to search for a phrase, enclose the words in quotation marks.



- If you type multiple words on the same line, Discovery Accelerator finds all items that contain any of the words or phrases on the line.
- Press the “Enter” key in a search box to add another line to it. If you type multiple lines in a search box, choose “Any of” or “All of” in the left box to determine whether the lines are connected by OR/AND conditions.



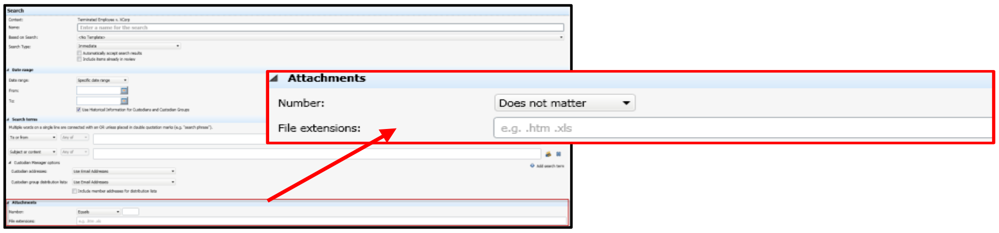
- To add the name of a Target or Custodian to the “From” box or “To” box, click the “Custodian” icon to the right of the search field and select the required Target or Custodian.



If you specify as a Target or Custodian a Domino user whose details you synchronize with a Domino directory, you must ensure that this user has an SMTP address defined in the Domino directory. Otherwise, the search will fail to find the matching items. Alternatively, you can search for such users by their display names.

### Attachments Section

This section will describe the options when searching for a specific the number of attachments or file extension. Use the image below to reference the different areas of this section.



**Attachments**

Number: Does not matter

File extensions: e.g. .htm .xls

### Number

Specifies the required number of attachments. The default option, "Does not matter", means that the item can have zero or more attachments. All the other options require you to type one or two values that specify the required number of attachments.

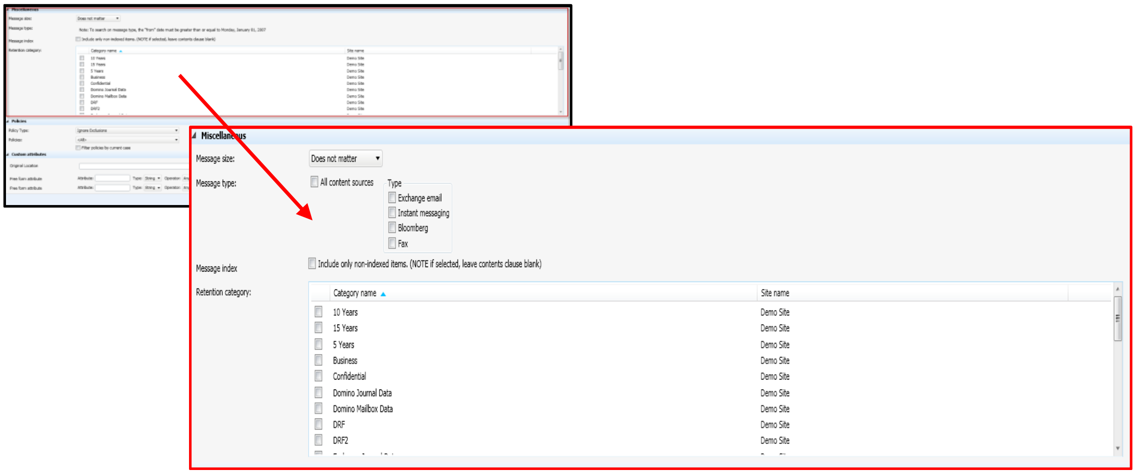
### File Extensions

Specifies the file name extensions of particular types of attachments for which to search. Separate the extensions with space characters.  If you specify one or more attachment types, only the attachments are searched, and not the items that contain them. For example, you cannot search for those items that have a specific word in their subject line or content and that contain a specific type of attachment.

Attachment file formats such as Fax or Voice do not contain text, so they are not indexed and not searchable.

## Miscellaneous Section

This section will describe the options when searching message size, message type, non-indexed items, or a specific retention category.  Use the image below to reference the different areas of this section.



**Miscellaneous**

Message size: Does not matter

Message type: □ All content sources

Type
- □ Exchange email
- □ Instant messaging
- □ Bloomberg
- □ Fax

Message index: □ Include only non-indexed items. (NOTE if selected, leave contents clause blank)

Retention category:

| | Category name ▲ | Site name |
|---|---|---|
| □ | 10 Years | Demo Site |
| □ | 15 Years | Demo Site |
| □ | 5 Years | Demo Site |
| □ | Business | Demo Site |
| □ | Confidential | Demo Site |
| □ | Domino Journal Data | Demo Site |
| □ | Domino Mailbox Data | Demo Site |
| □ | DRF | Demo Site |
| □ | DRF2 | Demo Site |

### Message Size

Specifies the size in kilobytes of each item for which to search, as reported by the message store (Microsoft Exchange, Lotus Domino etc.). The item size includes the size of any attachments.

### Message Type

Enables searching for items of the selected types. This option is only available if:

- Your Enterprise Vault server is running Enterprise Vault 5.0 or later.
- You have specified a date range that does not include a date before you installed Enterprise Vault 5.0 or later.

### Include only non-indexed

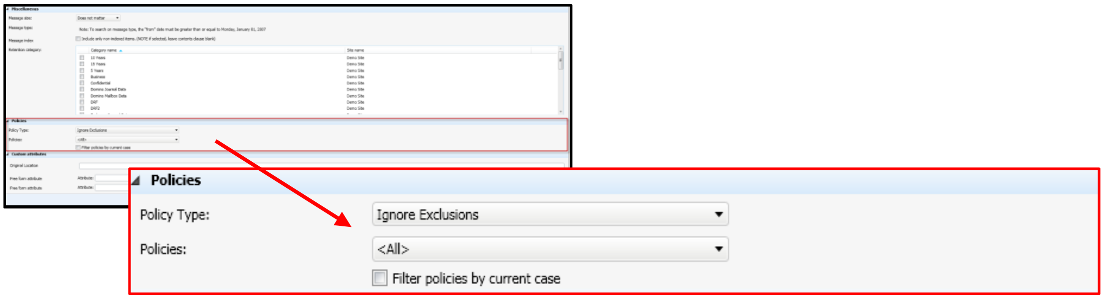
Allows searching for non-indexed items that would not appear in the content search results, such as encrypted/corrupted mail items and password protected .zip files.

### Retention Category

Searches for items to which Enterprise Vault has assigned the selected retention categories.

## Policy Section

This section will describe the options when searching message size, message type, non-indexed items, or a specific retention category.  Use the image below to reference the different areas of this section.



Policies

Policy Type: Ignore Exclusions

Policies: <All>

□ Filter policies by current case

### Policies

Allows searching for those items that the Automatic Classification Engine has tagged with particular types of policies.

The Automatic Classification Engine is a policy server that is a separate module from Discovery Accelerator that allows the organization to process rules against data during archival to add search attributes or assign retention based on the message content

There are three policy types:

- **Inclusion**. This type of policy addresses the most serious issues, such as profanity, harassment, and insider trading.  You would normally want to ensure that the items exhibiting any of these features were included in your review set.
- **Exclusion**. This type of policy either precludes capture or advocates the non-capture of items. For example, spam items or newsletters may fall into this category.
- **Category**. This type of policy does not affect the capture of items in any way; it provides a means to categorize items. For example, you can use category policies to flag those items that are marked as Personal.

These policy types are not mutually exclusive; you can apply multiple policies of different policy types to the same item.

### Policies

Enables searching for items processed by the Automatic Classification Engine with a specific policy applied.

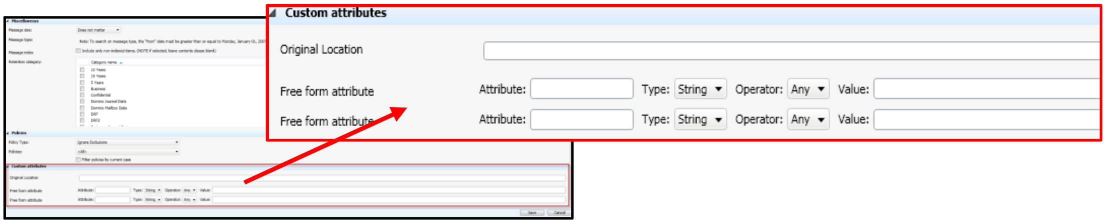
- Discovery Accelerator automatically adds to the policy list any new policies that it encounters when running a search.

### Filter policies by current Case

Allows omission from the list, those policies that are not in use in the current Case.

## Custom Attribute Section

This section will describe the options when searching against custom attributes.  Use the image below to reference the different areas of this section.



Miscellaneous

Message size: Does not matter

Message type: Note: To search on message type, the "from" date must be greater than or equal to Monday, January 01, 2007

Message index: □ Include only non-indexed items. (NOTE if selected, leave contents clause blank)

Retention category: Category name

□ 10 Years
□ 15 Years
□ 5 Years
□ Business
□ Confidential
□ Domino Journal Data
□ Domino Mailbox Data
□ DRF
□ DRF2

Policies

Policy Type: Ignore Exclusions

Policies: <All>

□ Filter policies by current case

Custom attributes

Original Location

Free form attribute  Attribute:  Type: String  Operator: Any  Value:

Free form attribute  Attribute:  Type: String  Operator: Any  Value:

### Custom Attributes

Custom search attributes enable you to assign criteria that are not available from the search interface by default. This, for example, allows searches for items to which a third-party application has added custom attributes.  The following attributes are available for configuration into the search page as checkbox, radio button, list box, or drop-down list.

| Attribute | Description |
|---|---|
| Archived Date | Searches for messages according to the date upon which Enterprise Vault archived them. |
| Categories And Keywords | Searches for messages according to the category that the author has assigned to them. |
| Conversation Tracking GUID | Searches for messages that have been indexed with the specified conversation tracking identifier. |
| Expiry Date | Searches for messages according to the date on which their retention period expires. |
| Languages | Searches for messages in the specified language. |
| Last Modified Date | Searches for messages according to the date on which they were last modified. |
| Message Class | Searches for messages that fall into a specific message class, such as IPM.Appointment or IPM.Contact. |
| Message Importance | Searches for messages that are marked with a particular importance level. |
| Message Security | Searches for messages according to whether the author has digitally signed or encrypted them. |
| Message Sensitivity | Searches for messages that are marked with a particular sensitivity level. |
| Number Of Days To Expiry | Searches for messages that are scheduled for deletion in the specified number of days. |
| Number Of Recipients | Searches for messages that have the specified number of recipients. |
| Original Identifier | Searches for messages by their original identifier. |
| Original Location | Searches for messages according to their original folder location, such as the Inbox or Drafts folder. |
| Saveset Identifier | Searches for messages according to the identifier that is assigned to the saveset (.DVS) file. |
| Vault Permission | Searches for messages that are in all the folders to which a particular user has access. |

ℹ For information and configuration assistance, contact your Discovery Accelerator Administrator

### Punctuation

When Enterprise Vault archives and indexes and item, any punctuation is treated as a “Space”.  When using Discovery Accelerator to search against a phrase or name with punctuation such as a middle initial followed by a period, the “Period” will be ignored.

## Search Scheduler

When searching with Discovery Accelerator, you have the ability to run the search immediately or to schedule it for an “Off Peak” time.  One of the most common uses of the scheduler is to run a search nightly to collect the data delta for an ongoing matter.

### Schedule Type

The scheduler may be configured to run a search when the SQL agent starts, when CPU’s are idle, “Once,” or “Recurring.”

### Recurring Schedule

- Daily may be configured to run every day, every two days, every three days, etc.
- Weekly may be configured to run every week, every two weeks, etc.  The day may be specified, e.g. Saturday.
- Monthly may be configured to run every month, every two months, etc.  The date may be specified, e.g. 1st, 15th etc.  Also, it may be configured to run on a named day, e.g. 1st Sunday of each month.

### Daily Frequency

The scheduler may be configured for a specific hour of the day, e.g. 6:30 AM or every 30 minutes from 8:00 AM to 5:00 PM.

### Duration

The scheduler may be configured to start and end on specific dates or start on a specific date and have no end date.

ℹ Please contact your Discovery Accelerator Administrator for configuration of the scheduler.

## Targets

### Targets

Among the criteria that you can define when you set up a search in Discovery Accelerator are the email addresses for which to look in items. If an employee has multiple email addresses then, to save you from having to enter them all whenever setting up a search, they can be added to a target entry in Address Manager. Then you can specify the target name in your search criteria as a shorthand way of listing all the associated addresses.

Discovery Accelerator has the capability to enable organizations to pre-configure individuals and groups of individuals for selection when creating a search. If your organization is highly litigious or employs individuals that are frequently involved in legal matters, then these configurations could reduce the amount of effort when creating a search.

Creation of a Target enables the organization to select a configured individual directly from the search page when populating the “To” or “From” search field. The Target will contain every E-mail and display name variation used by the individual during the duration of their employment. This functionality is useful when changes in the E-mail environment or legal name have occurred, and there is a potential for missing relevant data.

### Target Groups

Target groups provide a way to collect a number of people under a group name. You can then use this name as a shorthand way of referring to the list of people. For example, you could create a target group called "Directors" and then add the names of all the company directors to the group. When you create a search, you can search for items that are sent to the target group Directors, instead of listing all their names individually. You can add a target to multiple target groups.

## Custodians

### Custodian Manager

Custodian Manager allows you to submit the details of custodians and custodian groups for which to search against in Discovery Accelerator. A custodian is an individual employee, whereas a custodian group is any collection of employees, such as an NT group, distribution list, Active Directory container, Domino LDAP query, or Domino group.

Once you have submitted a few details of a custodian or group with Custodian Manager, they can be synchronized with an external source like Active Directory or a Domino LDAP directory. This will keep the data in Custodian Manager up-to-date and allows you retrieve additional information about the custodian or group from the external source.

Custodian Manager also allows assignment of additional, custom attributes to custodians and custodian groups. These attributes may be used to filter the list of custodians and groups for which to search in Discovery Accelerator. For example, a custom attribute called "Cost Center 1"may be created and assigned to the custodians who belong to the cost center, then selected when defining search targets with Discovery Accelerator.

**Custodians**

Creation of a Custodian enables the organization to select an individual from the company directory by way of a module of Discovery Accelerator known as the Custodian Manager. In the Custodian Manager, an individual can be configured to synchronize with an employee that is listed in directory (Active Directory or Lightweight Directory Access Protocol – "LDAP)" so that the "To" or "From" search field may be easily populated with the most current information in the E-mail server.

**Custodian Groups**

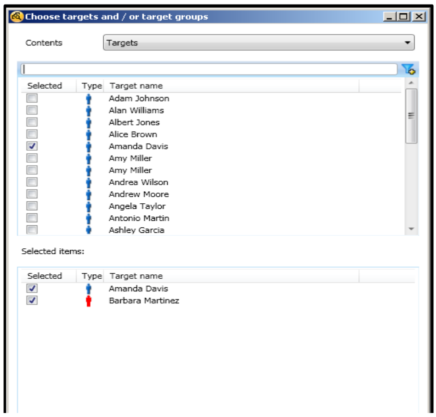
Creation of a Custodian Group enables the organization to synchronize groups of individuals based on the following:

- Domino Distribution List
- Domino Group
- Domino LDAP Search
- Windows Group
- Windows Distribution List
- Active Directory Container
- Active Directory Search

**Accessing Targets and Custodians**

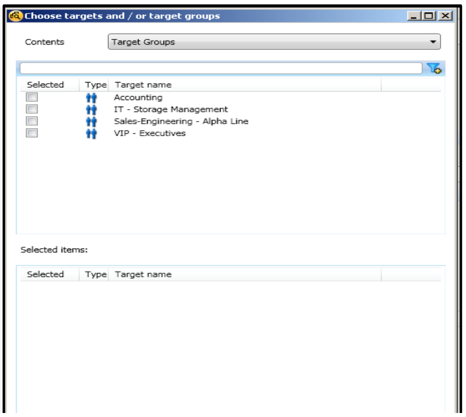
Targets, Target Groups, Custodians and Custodian Groups will all be accessed in the same manner. From the search page, you select the "Custodians" from the far right portion of the search term section.

A new window will open displaying the "Targets" or "Target Groups" depending on which is selected in the "Contents" drop down menu.



| Selected | Type | Target name |
|---|---|---|
| ☐ | ● | Adam Johnson |
| ☐ | ● | Alan Williams |
| ☐ | ● | Albert Jones |
| ☐ | ● | Alice Brown |
| ☑ | ● | Amanda Davis |
| ☐ | ● | Amy Miller |
| ☐ | ● | Amy Miller |
| ☐ | ● | Andrea Wilson |
| ☐ | ● | Andrew Moore |
| ☐ | ● | Angela Taylor |
| ☐ | ● | Antonio Martin |
| ☐ | ● | Ashley Garcia |

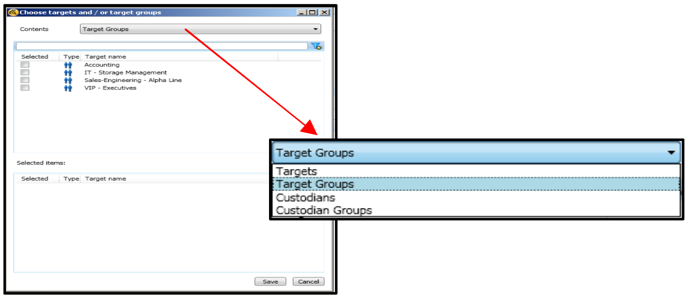
| Selected | Type | Target name |
|---|---|---|
| ☑ | ● | Amanda Davis |
| ☑ | ● | Barbara Martinez |



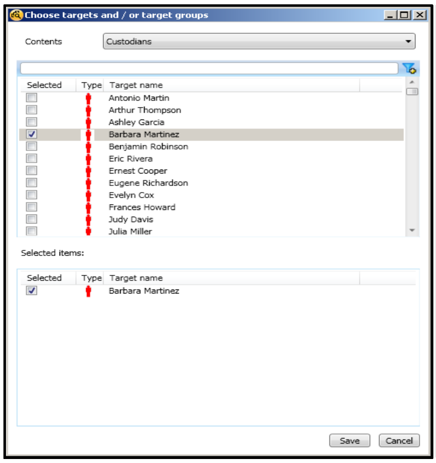
| Selected | Type | Target name |
|---|---|---|
| ☐ | ●● | Accounting |
| ☐ | ●● | IT - Storage Management |
| ☐ | ●● | Sales-Engineering - Alpha Line |
| ☐ | ●● | VIP - Executives |

| Selected | Type | Target name |
|---|---|---|

To access Custodians or Custodian Groups, use the “Contents” drop-down menu and select.

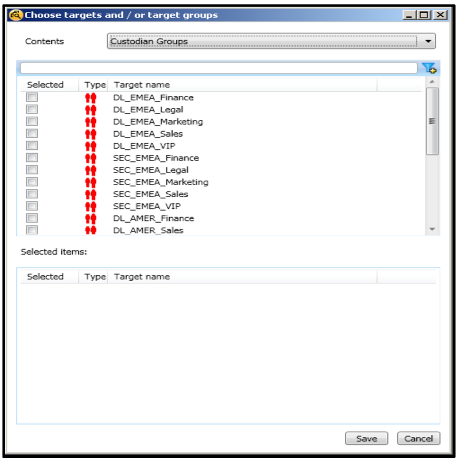


The window will now display the “Custodians” or “Custodian Groups” depending on which is selected in the “Contents” drop down menu.



| Selected | Type | Target name |
|---|---|---|
| ☐ | ● | Antonio Martin |
| ☐ | ● | Arthur Thompson |
| ☐ | ● | Ashley Garcia |
| ☑ | ● | Barbara Martinez |
| ☐ | ● | Benjamin Robinson |
| ☐ | ● | Eric Rivera |
| ☐ | ● | Ernest Cooper |
| ☐ | ● | Eugene Richardson |
| ☐ | ● | Evelyn Cox |
| ☐ | ● | Frances Howard |
| ☐ | ● | Judy Davis |
| ☐ | ● | Julia Miller |

| Selected | Type | Target name |
|---|---|---|
| ☑ | ● | Barbara Martinez |



| Selected | Type | Target name |
|---|---|---|
| ☐ | ●● | DL_EMEA_Finance |
| ☐ | ●● | DL_EMEA_Legal |
| ☐ | ●● | DL_EMEA_Marketing |
| ☐ | ●● | DL_EMEA_Sales |
| ☐ | ●● | DL_EMEA_VIP |
| ☐ | ●● | SEC_EMEA_Finance |
| ☐ | ●● | SEC_EMEA_Legal |
| ☐ | ●● | SEC_EMEA_Marketing |
| ☐ | ●● | SEC_EMEA_Sales |
| ☐ | ●● | SEC_EMEA_VIP |
| ☐ | ●● | DL_AMER_Finance |
| ☐ | ●● | DL_AMER_Sales |

| Selected | Type | Target name |
|---|---|---|

For assistance with configuring Targets and Custodians, please contact your Discovery Accelerator Administrator.

# Simple Searching

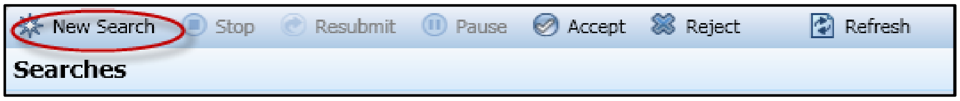
In this section, we will discuss the steps for searching an individual's E-mail, for specific key words or key phrases during a specified period of time.

## Simple Search Examples

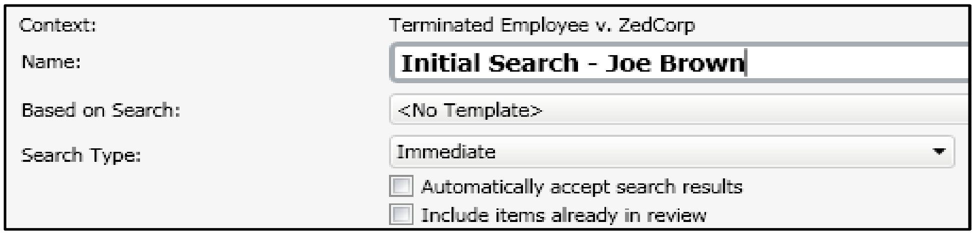
### Example 1: Author/Recipient Date Specific Searching

In this example, we will create a search where the desired results will be any data sent to or from "Joe Brown" for the duration of his employment, July 1, 2007 to May 31, 2009.

First select "Cases" from the application toolbar, then "Searches" from the cases menu. The search dashboard should now be displayed. Select "New Search" from the search action area.



Once the search page is displayed, we will first populate the context section with a search name, a previous search template, the search type (Immediate or Scheduled), and select options for automatic acceptance and inclusion of previously accepted search results. In this example, the default settings have been selected.



Context: Terminated Employee v. ZedCorp

Name: Initial Search - Joe Brown

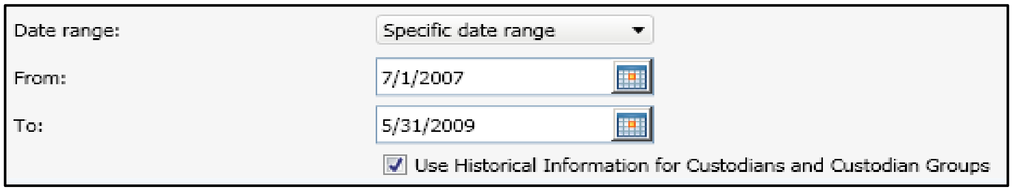
Based on Search: <No Template>

Search Type: Immediate

□ Automatically accept search results

□ Include items already in review

In the date range section, we will leave the default of "Specific date range" and click the calendar icon to populate the start and end dates. The option for historical Custodian information is checked by default in the event a preconfigured Custodian is selected as search criteria. The option has no effect when entering individuals by free form text. In this example, free form text will be used.



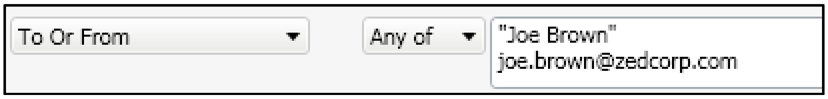
Date range: Specific date range

From: 7/1/2007

To: 5/31/2009

☑ Use Historical Information for Custodians and Custodian Groups

In the search term section, change the value of the search field from “All” to “To or From”, and enter all variations of the individual in the search field.  In this example we entered the display name in quotes on the first line and the E-mail address without quotes on the second line.  When entering more than one word on a single line, they must be enclosed in quotes to be associated together.  An email address does not need to be enclosed in quotes as Enterprise Vault recognizes it as an address and indexes the four words together as if they were a phrase then ignores the punctuation when searching.

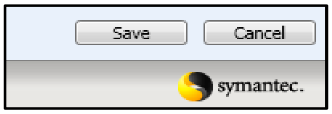


To Or From | Any of

"Joe Brown"
joe.brown@zedcorp.com

Please pay special attention when searching display names ensuring that the full name is always enclosed in quotes.  In the event that the search was targeting “Joe L. Brown” and not “Joe Brown”, the Discovery Accelerator would ignore the period, and search for the name as a phrase of three words “Joe” AND “L” AND “Brown”.

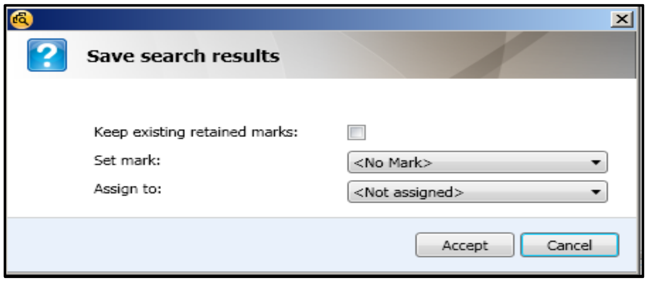
Now that the required criteria has been entered in the search page, click the “Save” button located in the lower right area of the search page to start the search.



While the search is running, the search dashboard will be displayed.  Viewing the dashboard is not required during the active search, allowing you to create more searches, navigate to the review interface, or just grab a cup of coffee.

Search completion time is difficult to estimate as environmental factors must be considered.  From a user perspective, it is best to understand that if more specific search criteria is used, fewer results will be returned.  With fewer results to process, the search time should decrease.

Once the search has completed, you will have the option to “Accept” or “Reject” the search from the search action area of the dashboard.  Upon accepting, a dialog box will be displayed allowing you to assign the results to a specific reviewer and bulk mark.  In this example, we will accept the default and make assignments at a later date.


Save search results

Keep existing retained marks: □

Set mark: <No Mark>

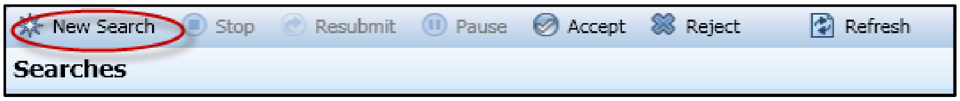
Assign to: <Not assigned>

The options to assign a default mark and reviewer to the search results apply only to newly discovered items. If the search results include items that you have previously captured and added to the review set, these items retain their assigned marks and reviewers. The option to keep existing marks applies only to those items to which reviewers have already assigned marks in another search within the Case. A user may reject a search if too many or unexpected results are returned. If you reject the results of a search, the results will be removed from the Case; however, the rejected search will still be auditable.

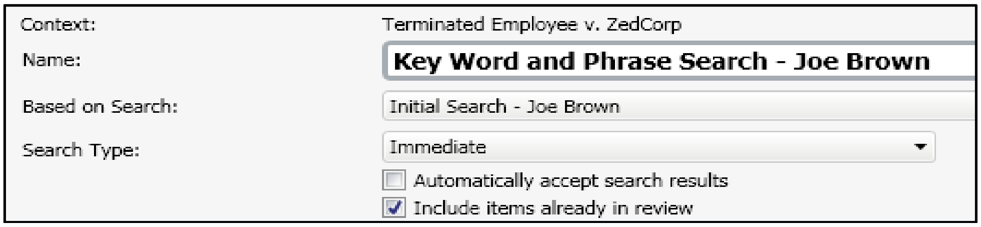
### Example 2: Author/Recipient Date Specific Searching with Key Word and Phrases

In this example, we will create a search where the desired results will be any data sent to or from "Joe Brown" with the word "Evaluation" or the phrase "Performance Plan" for the duration of his employment, July 1, 2007 to May 31, 2009.

First select "Cases" from the application toolbar, then "Searches" from the cases menu. The search dashboard should now be displayed, select "New Search" from the search action area.



Once the search page is displayed, populate the context section with a search name, a previous search template, the search type (Immediate or Scheduled), and select options for automatic acceptance and inclusion of previously accepted search results. In this example, we will use the search template from example 1, and we will select the option to include items already in review. Since we are building on a previous search, this will allow us to search the results already found as well as use the previous criteria automatically entered.



Context: Terminated Employee v. ZedCorp

Name: Key Word and Phrase Search - Joe Brown

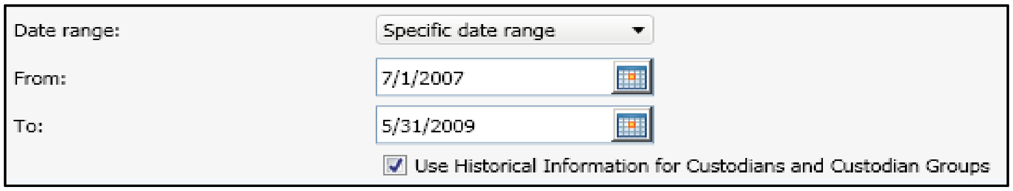
Based on Search: Initial Search - Joe Brown

Search Type: Immediate

□ Automatically accept search results

☑ Include items already in review

The date range section should already be populated by use of the template.



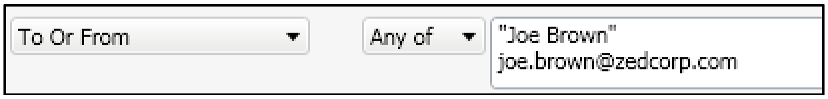
Date range: Specific date range

From: 7/1/2007

To: 5/31/2009

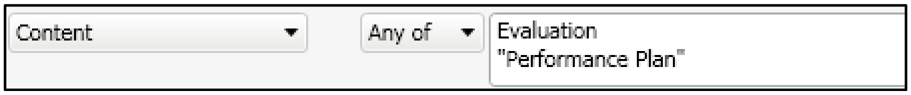
☑ Use Historical Information for Custodians and Custodian Groups

In the search term section, the search field for “To or From” should already be populated by use of the template.



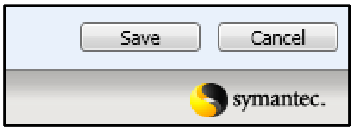
To Or From | Any of | "Joe Brown"
joe.brown@zedcorp.com

Add another search term field, and change the value from “All” to “Content”, input the word “Evaluation” on the first line, press enter on your keyboard and input the phrase “Performance Plan” on the second line. In this example, we entered the key word without quotes on the first line and the key phrase with quotes on the second line. When entering more than one word on a single line, they must be enclosed in quotes to be associated together.



Content | Any of | Evaluation
"Performance Plan"

Now that the required criteria has been entered in the search page, we will click the “Save” button located in the lower right area of the search page to start the search.



# Advanced Searching

How you combine words or phrases has a direct bearing on what you retrieve. To the computer, your combination of words is nothing more than a collection of characters. It tries to match your exact terms in the exact order you typed them. Most failed searches are the result of poorly constructed search queries.

The Enterprise Vault Indexing Engine allows the use of Boolean Operators and Wildcards providing the ability to retrieve more meaningful, relevant results when searching.

## Boolean Operators

Boolean operators are words used to make a logical search query and will enable you to broaden or narrow your search. With a good understanding of Boolean operators, a user can also analyze the reasons for failed searches and make appropriate adjustments.

Listed below are the Boolean operators supported by the Enterprise Vault Indexing Engine:

- AND
- OR
- NOT

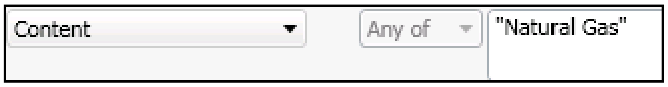
## AND Operators

The Boolean AND narrows a search by returning only results containing all of the words you search for. When using the AND operator, Discovery Accelerator is instructed to treat the word or phrase following as required criteria for every other word or phrase on that line in the search field. This operator is represented by the plus (+) symbol.

### AND Operator Examples

**Example 3: Simple Phrase Search**

If you were searching for the phrase “Natural Gas”, you would use the syntax below in the content field.

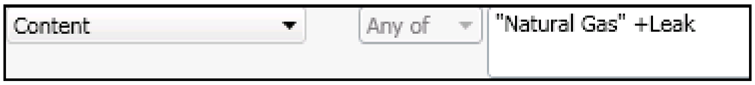


"Natural Gas"

This would return results for every E-mail, document, or attachment that contained the phrase “Natural Gas”.

**Example 4: Phrase search with required word**

If you were searching for the phrase “Natural Gas”, but only if the word “Leak” was also in the text body, then you would follow the syntax below.



Content

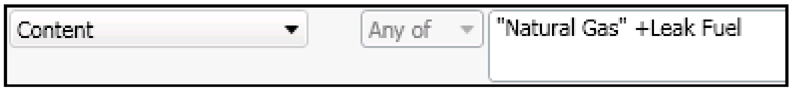
Any of

"Natural Gas" +Leak

This would return results for every E-mail, document, or attachment that contained the phrase “Natural Gas” and the word “Leak” somewhere in the text body (Natural Gas **AND** Leak).

**Example 5: Phrase search or word search with required word**

If you were searching for the phrase “Natural Gas” or “Fuel” where both needed to be associated with the word “Leak”, then you would follow the syntax below.



Content

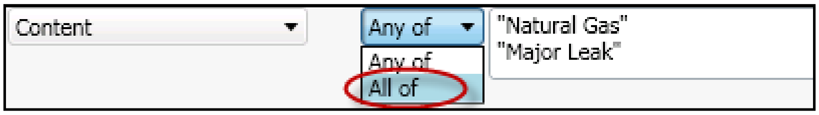
Any of

"Natural Gas" +Leak Fuel

The word “Leak” was compared to every other word or phrase on the line regardless of the order. This would return results for every E-mail, document, or attachment that contained the phrase “Natural Gas” and the word “Leak” or the word “Fuel” and the word “Leak” somewhere in the text body (Natural Gas **AND** Leak) **OR** (Fuel **AND** Leak).

**Example 6: Phrase search with required phrase**

If you were searching for the phrase “Natural Gas”, but only if the phrase “Major Leak” was also in the text body, then you would follow the syntax below.



Content

Any of

"Natural Gas"
"Major Leak"

This would return results for every E-mail, document, or attachment that contained the phrases “Natural Gas” and “Major Leak” somewhere in the text body (Natural Gas **AND** Major Leak).

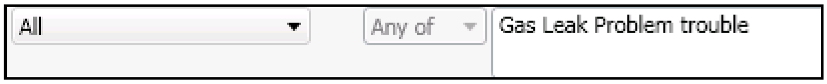
When searching multiple phrases, the **AND** operator is enabled via the Drop Down” menu adjacent to the search field. Selecting “**All Of**” instructs Discovery Accelerator to place a Boolean **AND** between each line (Carriage Return).

## OR Operators

The Boolean OR expands your search by returning E-mail or documents in which either or both words appear. By default, if multiple words or phrases are entered on the first line, Discovery Accelerator is instructed to place an **OR** between each.

### OR Operator Examples

**Example 7: Multiple words on the same line**
If you were searching for any of the words “Gas”, “Leak”, “Problem”, or “Trouble” in any of the available fields, you would follow the syntax below.


All

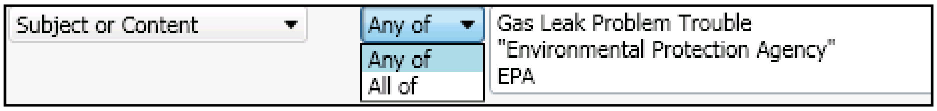
Any of

Gas Leak Problem trouble

This would return the results for every E-mail, document, or attachment that contained any of the words “Gas”, “Leak”, “Problem”, or “Trouble” in the subject line, document title, attachment title, or somewhere in the text body (Gas **OR** Leak **OR** Problem **OR** Trouble).

The behavior within the search field can be toggled between the **OR** (Any Of) and the **AND** (All Of) operators by using the drop-down menu adjacent to the search field. The drop-down menu becomes active once a second line of data has been added to the field.

**Example 8: Multiple words or phrases on multiple lines**
If you were searching for any of the words “Gas”, “Leak”, “Problem”, “Trouble” or “Environmental Protection Agency” or “EPA” in the subject or content fields, you would follow the syntax below.


Subject or Content

Any of

Gas Leak Problem Trouble
"Environmental Protection Agency"
EPA

This would return the results for every E-mail, document, or attachment that contained any of the words “Gas”, “Leak”, “Problem”, “Trouble”, “EPA” or “Environmental Protection Agency” in the subject line, document title, attachment title, or somewhere in the text body (Gas **OR** Leak **OR** Problem **OR** Trouble **OR** EPA **OR** Environmental Protection Agency).

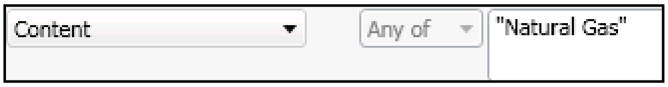
## NOT Operator

The Boolean NOT limits your search by returning only results containing the first word but not if the second word is also contained. When using the NOT operator, Discovery Accelerator is instructed to exclude the result if the word or phrase following is found in the same result returned by any other word or phrase on that line in the search field. This operator is represented by the minus (-) symbol.

## NOT Operator Examples

**Example 9: Simple Phrase Search**

If you were searching for the phrase “Natural Gas”, you would use the syntax below in the content field.

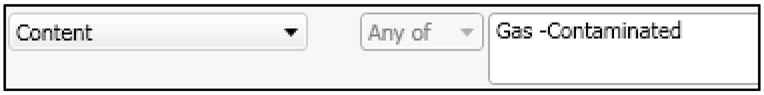


Content ▾ Any of ▾ "Natural Gas"

This would return results for every E-mail, document, or attachment that contained the phrase “Natural Gas”.

**Example 10: Single Word Search with word excluded**

If you were searching for the word “Gas”, but not if the result also contained the word “Contaminated”, you would use the syntax below in the content field.

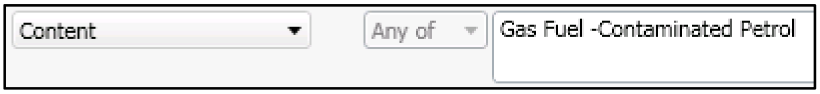


Content ▾ Any of ▾ Gas -Contaminated

This would return results for every E-mail, document, or attachment that contained the word “Gas”, but not if the word “Contaminated” was anywhere in the body text (Gas **NOT** Contaminated).

**Example 11: Multiple Word Search on same line with word excluded**

If you were searching for the words “Gas”, or “Fuel”, or “Petrol” but not if the result also contained the word “Contaminated”, you would use the syntax below in the content field.



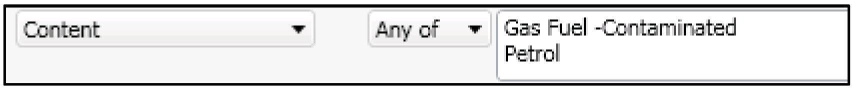
Content ▾ Any of ▾ Gas Fuel -Contaminated Petrol

This would return results for every E-mail, document, or attachment that contained any of the word “Gas”, “Fuel”, or “Petrol”, but not if the word “Contaminated” was anywhere in the body text (Gas **OR** Fuel **OR** Petrol **NOT** Contaminated).

Regardless of where the excluded word is positioned on the line, it applies to all other words on the line.

**Example 12: Multiple Word Search on different line with a word excluded**

If you were searching for the words “Gas”, or “Fuel”, but not if the result also contained the word “Contaminated”, or “Petrol”, you would use the syntax below in the content field.



Content ▾ Any of ▾

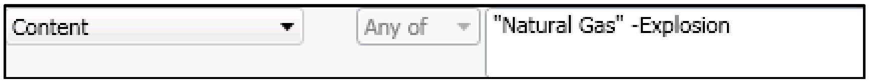
Gas Fuel -Contaminated
Petrol

This would return results for every E-mail, document, or attachment that contained any of the word “Petrol”, “Gas” or “Fuel”, and any E-mail, document or attachment that contained “Gas” or “Fuel”, but not if the word “Contaminated” was anywhere in the body text (Petrol **AND** Gas **OR** Fuel **NOT** Contaminated).

This search criteria is a little more complex in that you are looking for results that could have the words “Petrol” and “Contaminated” but not if either of the words “Gas” or “Fuel” also appeared in the result. The excluded word does not apply to words positioned on other lines.

**Example 13: Phrase Search with word excluded**

If you were searching for the phrase “Natural Gas” but not if the result also contained the word “Explosion”, you would use the syntax below in the content field.



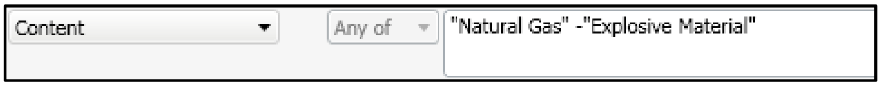
Content ▾ Any of ▾

"Natural Gas" -Explosion

This would return results for every E-mail, document, or attachment that contained the phrase “Natural Gas”, but not if the word “Explosion” was anywhere in the body text (Natural Gas **NOT** Explosion).

**Example 14: Phrase search with phrase excluded**

If you were searching for the phrase “Natural Gas” but not if the result also contained the Phrase “Explosive Material”, you would use the syntax below in the content field.



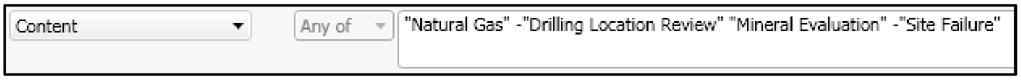
Content ▾ Any of ▾

"Natural Gas" -"Explosive Material"

This would return results for every E-mail, document, or attachment that contained the phrase “Natural Gas”, but not if the phrase “Explosive Material” was anywhere in the body text (Natural Gas **NOT** Explosive Material).

**Example 15: Multiple Phrase Search with multiple phrases excluded**

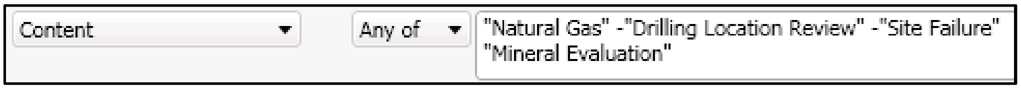
If you were searching for the phrases “Natural Gas” or “Mineral Evaluation” but not if the result also contained the phrases “Drilling Location Review” or “Site Failure”, you would use the syntax below in the content field.



Content ▾ Any of ▾

"Natural Gas" -"Drilling Location Review" "Mineral Evaluation" -"Site Failure"

This would return results for every E-mail, document, or attachment that contained the phrase “Natural Gas” or “Mineral Evaluation”, but not if the phrases “Drilling Location Review” or “Site Failure” were anywhere in the body text (Natural Gas **NOT** Drilling Location Review **OR NOT** Site Failure) or (Mineral Evaluation **NOT** Drilling Location Review **OR NOT** Site Failure).



Content | Any of | "Natural Gas" -"Drilling Location Review" -"Site Failure" "Mineral Evaluation"

Keep in mind that you cannot search using the “NOT” operator without first using a positive search attribute. In other words, you cannot search for all items that do not contain a specific word or phrase alone.

## Truncation Searching

Truncation searching allows you to retrieve E-mail and documents containing variations on a search term. Discovery Accelerator makes use of wildcards to make a logical search query and enable you to broaden or narrow your search. A wildcard is a character that may be used in a search term to represent one or more other characters.

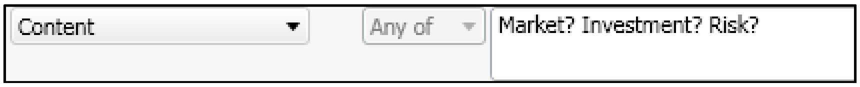
The two wildcards used in Discovery Accelerator are the Question Mark (?) and the Asterisk (*).

### Single Character

The question mark (?) may be used to represent a single alphanumeric character in a search expression. When searching, *there is a requirement to have at least three leading characters of the keyword.*

One use for the single character wildcard would be to replace one character at the end of a word such as “Trader?” would return results for “Trader” and “Traders”.

**Example 16: Multiple Word Search with Single Character Wildcard**
If you were searching for the words “Market” or “Investment” or “Risk” and wanted to ensure that the plural form of each word was also returned in the results, you would use the syntax below in the content field.



Content | Any of | Market? Investment? Risk?

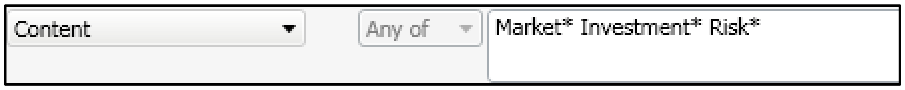
This would return results for every E-mail, document, or attachment that contained any of the words “Market” or “Markets” or “Investment” or Investments” or “Risk” or “Risks” in the body text (Market **OR** Markets **OR** Investment **OR** Investments **OR** Risk **OR** Risks).

### Multiple Characters

An asterisk (*) may be used to specify zero or more alphanumeric characters.  As with the single character wildcard, there is a requirement for three leading characters before using the asterisk.  A search term consisting of a lone asterisk could retrieve every record from the Enterprise Vault.

**Example 17: Multiple Word Search with Multiple Character Wildcard**

If you were searching for the words "Market" or "Investment" or "Risk" and wanted to ensure that any variation of the word was also returned in the results, you would use the syntax below in the content field.



Content ▾   Any of ▾   Market* Investment* Risk*

This would return results for every E-mail, document, or attachment that contained any of the words "Market" or "Markets" or "Marketing" or "Investment" or Investments" or "Investing" or "Risk" or "Risks" or "Risky" etc.…in the body text (Market **OR** Markets **OR** Marketing **OR** Investment **OR** Investments **OR** Investing **OR** Risk **OR** Risks **OR** Risky).

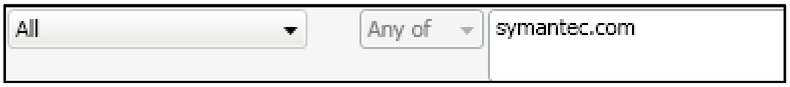
## Diacritics

The Enterprise Vault index is in Unicode; therefore, searching may be language specific.  For example, a search for "éléphant" would only yield the French variant of the word (more specifically the accented "e" in the word, regardless of the language in which it was written).  If you know that you have non-English or international E-mail which may contain special characters or accented letters, we recommend that you analyze your search criteria and either generate multiple specific variations or use the single character wildcard (?) to ensure that you return meaningful results.

**Unicode** is defined as a series of character encoding standards intended to support the characters used by a large number of the world's languages.

## Searching Email Domains

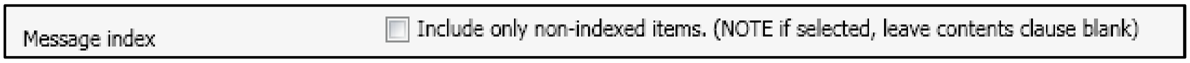
To search for all E-mail to or from a specific domain, you do not need to use the "@" symbol or any wildcards.  When in the to/from search field, enter just the domain name, e.g. symantec.com



All ▾   Any of ▾   symantec.com

## Searching Non-Indexed Items

In some organizations, there are occasions where an encrypted or protected document or a very large document is archived and not indexed. When Enterprise Vault archives an item without indexing, a "Not Indexed" search attribute is added to allow searching.



Message index ☐ Include only non-indexed items. (NOTE if selected, leave contents clause blank)

When using this option, the search can be configured for employees, date ranges, subject lines, and other available attributes, but the "Content" field must be left blank. A recommended best practice is that periodic searches are run against the entire archive(s) to identify non-indexed content (if any) that may need to be to be reviewed manually to determine relevance for current active Cases.

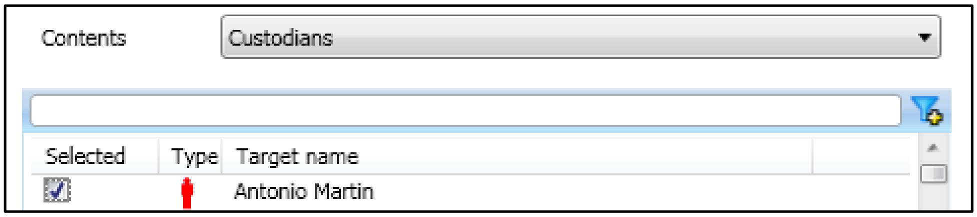
## More Advanced Search Examples

In this section we provide examples of how to create searches utilizing the options built into the search interface.

### Example 18: Search Custodians and Custodian Groups

With the availability of the Custodian Manager, individuals or groups of individuals may be configured and selected for searching. In this example, we will demonstrate selecting Custodians and Custodian groups.

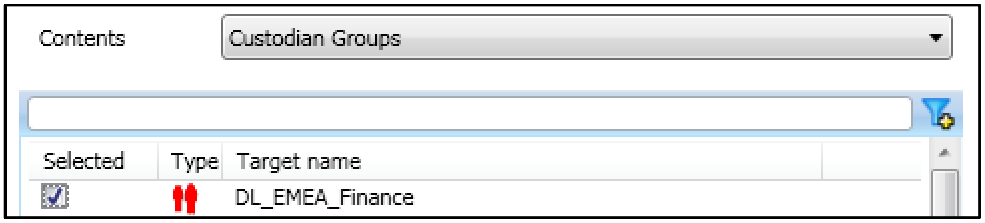
If you were searching for any E-mail sent to or from the Custodian "Antonio Martin" or the Custodian Group "DL_EMEA_Finance" you would click the "Targets" button adjacent to the search field. Once the Target selection dialogue is displayed, select "Custodians" from the content drop-down menu, then choose "Antonio Martin" to add him to the selected items area.



Contents: Custodians

| Selected | Type | Target name |
|---|---|---|
| ☑ | | Antonio Martin |

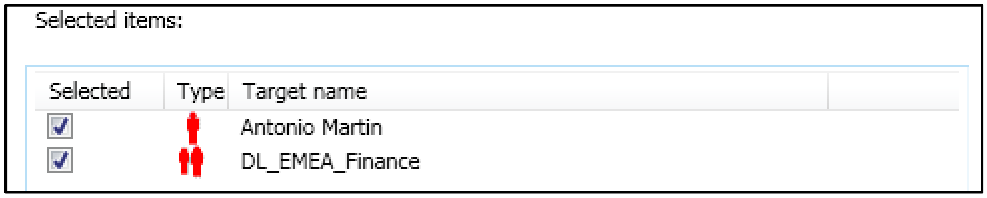
Next you select "Custodian Groups" from the content drop-down menu, then choose "DL_EMEA_Finance" to add the group to the selected items area. Click save.



Contents: Custodian Groups

| Selected | Type | Target name |
|---|---|---|
| ☑ | | DL_EMEA_Finance |

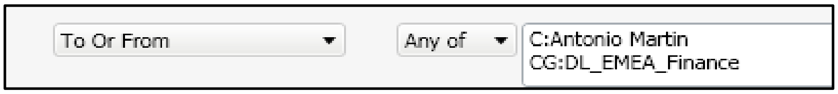
Notice that both “Antonio Martin” and the “DL_EMEA_Finance” appear in the area for selected items.



Selected items:

| Selected | Type | Target name |
|---|---|---|
| ☑ | | Antonio Martin |
| ☑ | | DL_EMEA_Finance |

Now the Custodian and Custodian Group should be displayed in the “To or From” search field as seen below.



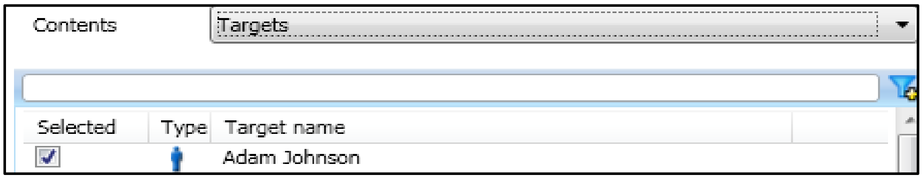
To Or From | Any of | C:Antonio Martin
CG:DL_EMEA_Finance

This would return results for every E-mail sent to or from “Antonio Martin” or any individual configured as member of the distribution list “DL_EMEA_Finance”.

**Example 19: Search Targets and Target Groups**

When creating a search that involves individuals who are frequently involved in matters, it may be more convenient to configure the individual or individuals as Targets and place them into Target Groups.

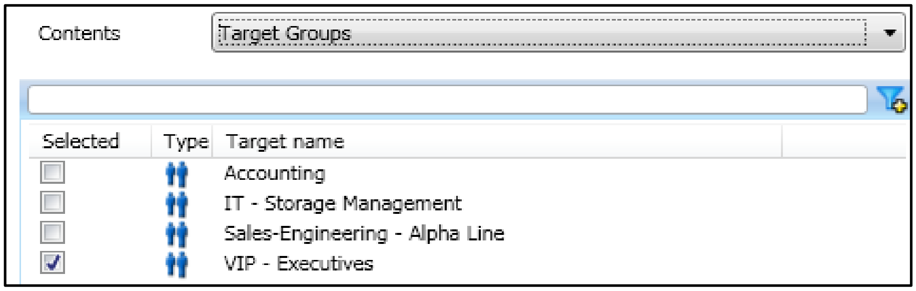
If you were searching for any E-mail sent to or from the Target “Adam Johnson” or the Target Group “VIP – Executives” you would click the “Targets” button adjacent to the search field. Once the Target selection dialogue is displayed, select “Targets” from the content drop-down menu, then choose “Adam Johnson” to add him to the selected items area.



Contents: Targets

| Selected | Type | Target name |
|---|---|---|
| ☑ | | Adam Johnson |

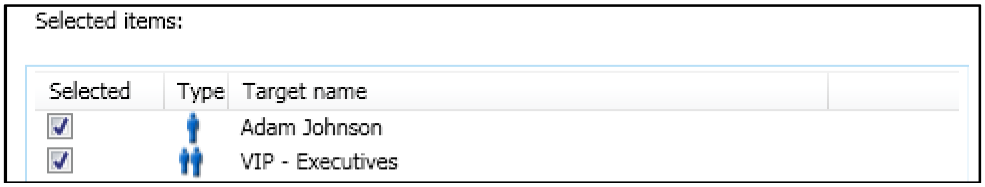
Next you select “Target Groups” from the content drop-down menu, then choose “VIP – Executives” to add the group to the selected items area. Click save.



Contents: Target Groups

| Selected | Type | Target name |
|---|---|---|
| □ | 👥 | Accounting |
| □ | 👥 | IT - Storage Management |
| □ | 👥 | Sales-Engineering - Alpha Line |
| ☑ | 👥 | VIP - Executives |

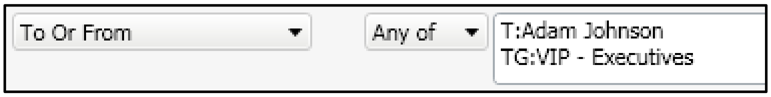
Notice that both “Adam Johnson” and the “VIP-Executives” appear in the area for selected items.



Selected items:

| Selected | Type | Target name |
|---|---|---|
| ☑ | 👤 | Adam Johnson |
| ☑ | 👥 | VIP - Executives |

Now the Target and Target Group should be displayed in the “To or From” search field as seen below.



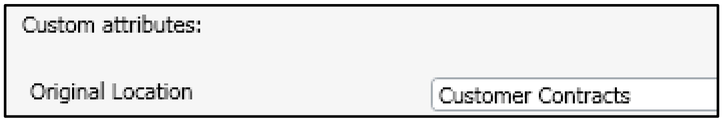
To Or From | Any of | T:Adam Johnson<br>TG:VIP - Executives

This would return results for every E-mail sent to or from “Adam Johnson” or any individual configured as member of the Target Group “VIP – Executives”.

**Example 20: Search Folder Location**

Enterprise Vault stores index metadata for the folder location of each individual E-mail. In some instances, you may have a requirement to search for E-mail that was located in a specific subfolder in the individual’s mailbox which can be accomplished by a custom attribute available through configuration. Once enabled, this will allow the item to appear in the “miscellaneous” section of the search page.

If your organization were configuring employee mailboxes with specific folders, the folder name could be specified in the custom attribute search field. In this example, we will search the subfolder “Customer Contracts”.



Custom attributes:

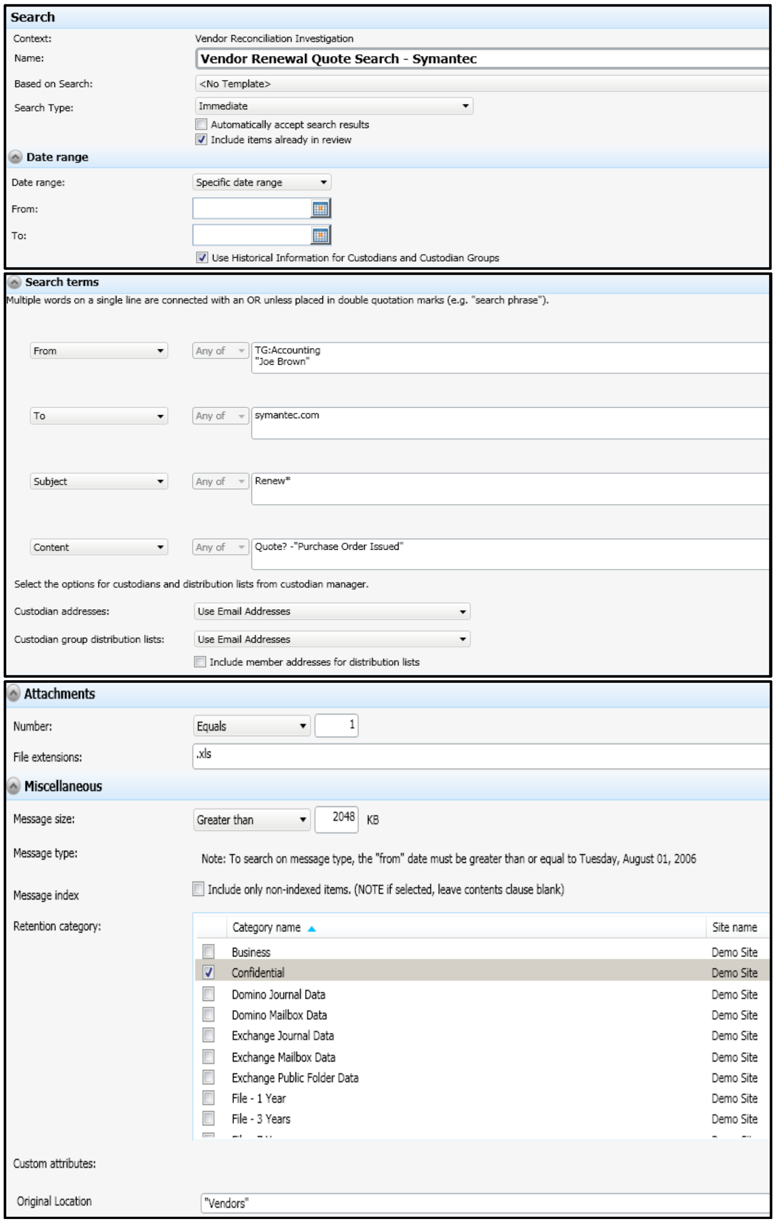
Original Location: Customer Contracts

Adding this attribute in conjunction with other criteria in the search fields will only return results that reside in the customer contracts “CC” folder.

### Example 21: A Complex Search

We have discussed populating individual fields with key words, free form text, Target selections, wildcards, and using a custom attribute. Now we will create a search using a combination of many options.

With the requirements listed below, the search page and syntax should appear as follows:



**Search**

| | |
|---|---|
| Context: | Vendor Reconciliation Investigation |
| Name: | Vendor Renewal Quote Search - Symantec |
| Based on Search: | <No Template> |
| Search Type: | Immediate |

□ Automatically accept search results
☑ Include items already in review

**Date range**

| | |
|---|---|
| Date range: | Specific date range |
| From: | |
| To: | |

☑ Use Historical Information for Custodians and Custodian Groups

**Search terms**

Multiple words on a single line are connected with an OR unless placed in double quotation marks (e.g. "search phrase").

| | | |
|---|---|---|
| From | Any of | TG:Accounting<br>"Joe Brown" |
| To | Any of | symantec.com |
| Subject | Any of | Renew* |
| Content | Any of | Quote? -"Purchase Order Issued" |

Select the options for custodians and distribution lists from custodian manager.

| | |
|---|---|
| Custodian addresses: | Use Email Addresses |
| Custodian group distribution lists: | Use Email Addresses |

□ Include member addresses for distribution lists

**Attachments**

| | | |
|---|---|---|
| Number: | Equals | 1 |
| File extensions: | .xls | |

**Miscellaneous**

| | | | |
|---|---|---|---|
| Message size: | Greater than | 2048 | KB |

Message type: Note: To search on message type, the "from" date must be greater than or equal to Tuesday, August 01, 2006

Message index □ Include only non-indexed items. (NOTE if selected, leave contents clause blank)

Retention category:

| | Category name | Site name |
|---|---|---|
| □ | Business | Demo Site |
| ☑ | Confidential | Demo Site |
| □ | Domino Journal Data | Demo Site |
| □ | Domino Mailbox Data | Demo Site |
| □ | Exchange Journal Data | Demo Site |
| □ | Exchange Mailbox Data | Demo Site |
| □ | Exchange Public Folder Data | Demo Site |
| □ | File - 1 Year | Demo Site |
| □ | File - 3 Years | Demo Site |

Custom attributes:

Original Location "Vendors"

In this example, the requirement is to search for E-mail from “Joe Brown” or the “Accounting” Target Group, to anyone with an E-mail address at Symantec, with the word “Renew” or “Renewing” or “Renewal” or “Renewals” in the subject line, and the word “Quote” or “Quotes” in the body of the E-mail, but not the phrase “Purchase Order Issued”. The date range must include all archived E-mail, and it should include any results already found within the Case.

The results must include one spreadsheet, and the message size must be greater than 2 MB. The results must reside in the “Vendors” folder and must be assigned the retention category of “Confidential”.

## Analytical Searching

Discovery Accelerator 8.0 introduced the capability to enable analytical functionality on Cases. When enabled for analytics, the Discovery Accelerator will leverage built in functionality of SQL Server 2005 for indexing of the existing search result sets. Essentially, a Case can be "promoted" and ingested by the Analytics module which provides advanced capabilities beyond that offered in the core DA module. This functionality provides you the ability to search within a result set to further cull down using advanced search syntax.

Previous search examples covered in the simple and advanced searching sections guide you through creation of “Collection Searches”. With “Analytical Searching”, you will have advanced capabilities intended to cull down the results of those Collection Searches to a data set that is more relevant to the matter. These searches act only on the data that has been previously collected in a Case, or Research Folder.

### Searching within a Review Set

When a Case has been enabled for Analytics, you will have the ability, using advanced options, to further cull down the existing search result set. In the filter area at the left of the Review pane we provide additional options with which a user may conduct searches of the items in the review set. Two types of searches are available: quick search and advanced search.

#### Quick Searching

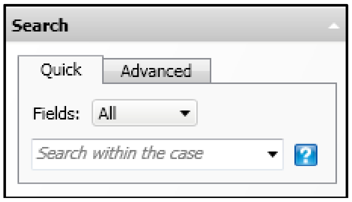
Use the quick search feature to specify one or more fields in which you want to search, such as “From” or “Subject” and the required values. The following table lists quick search features and gives examples of how they can be used in your searches:

| Feature | Examples |
|---|---|
| Boolean Operators | adam AND diana<br>adam OR john<br>adam AND NOT “adam walker” |
| Parenthesis | (adam OR diana) AND (adam OR john) |
| NEAR Operator | fuel NEAR leak |
| Search Scope | from: adam AND (subject: fuel OR subject: “fuel leak”) |
| Wildcards | gas* OR leak* |

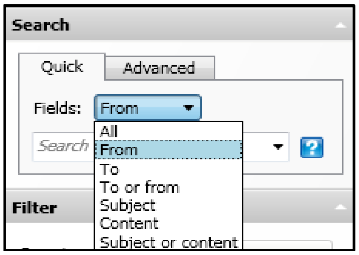
**Example 22: Conduct a Quick Search with OR Operator**

In this example, we will be searching an existing result set of the Case and using the OR operator to find all instances of where “Adam Johnson” or “John Bernard” are the author.

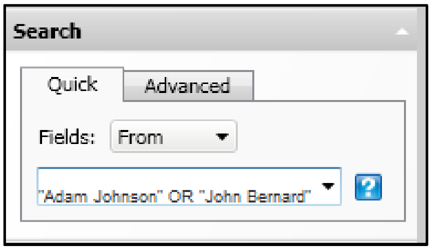
First access the quick search interface located in the left pane of the review interface.



Then select “From” from the “Fields” drop-down menu.



Next you populate the “Search within the Case” field with the name “Adam Johnson”, the OR operator, and the name “John Bernard”. Then click ‘Apply”



Fields: From

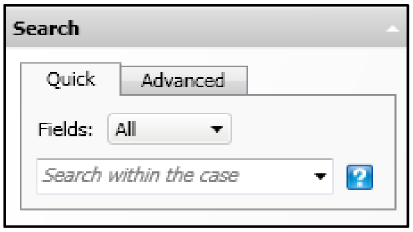
"Adam Johnson" OR "John Bernard"

This would return results for every E-mail or document within the Case that was authored by “Adam Johnson” or “John Bernard”.

**Example 23: Conduct a Quick Search with NEAR Operator**

In this example, we will be searching the existing result set of the Case and using the NEAR operator to find all instances of the word “Fuel” near the word “Leak”.,

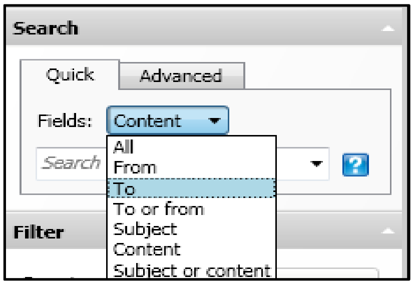
First access the quick search interface located in the left pane of the review interface.



Fields: All

Search within the case

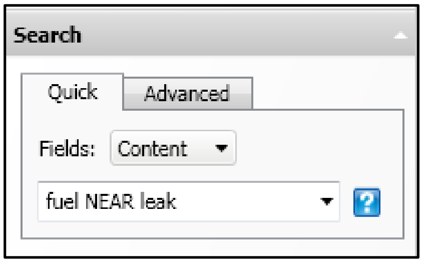
Then select “Content” from the “Fields” drop-down menu.



Fields: Content

Next you populate the “Search within the Case” field with the word “Fuel”, the NEAR operator, and the word “Leak”.

Click “Apply”.



Fields: Content

fuel NEAR leak

This would return results for every E-mail, document, or attachment within the Case that contains the words “Fuel” and “Leak” within 50 words of one another.

## Advanced Searching

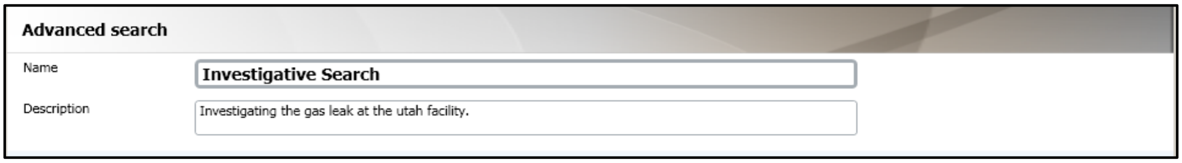
The advanced search feature lets you build complex searches that comprise multiple conditions. Unlike quick searches, you can save advanced searches for reuse.  The Analytic Advanced search page can be opened by selecting the “Advanced” tab from the quick search interface located in the left pane of the review interface.

### Advanced Search Page Layout

In this section, we will discuss the layout of the search page and the options for configuring searches.

#### Name

Provide a name and description of the search.  The description is useful when reusing the search at a later date.



Name: Investigative Search

Description: Investigating the gas leak at the utah facility.

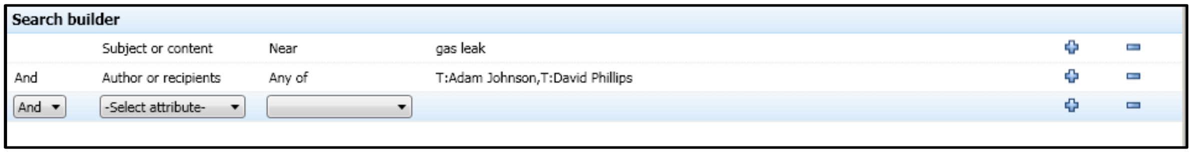
#### Search Builder

This area is used to define one or more conditions that an item must meet.  To define a condition, begin with the “Select Attribute” drop-down menu.  Choose an attribute of the items for which to search.

In the Search builder area, define one or more conditions that an item must meet. To define the conditions, proceed as follows:

- In the Select attribute dropdown list, choose an attribute of the items for which to search. For example, choose Subject if you want to search the subject lines of items.

- In the next dropdown- list, choose an operator to apply to the selected attribute. For example, if you have set the attribute to Subject, you can choose the Contains operator to search for items whose subject lines contain certain words.
- Set the required value for the attribute. For example, when the attribute is Subject and the operator is Contains, you can type "Symantec" to search for items whose subject lines contain this word. Note the following:
  - The search string cannot contain any punctuation characters other than the underscore character.
  - You can append an asterisk (*) as a wildcard character to the end of the search string.
  - SQL Server does not index commonly occurring words such as "the" and "and", so Discovery Accelerator ignores these words when it encounters them in a search string. You can override this behavior by editing the SQL Server noise word file.
- If you set the attribute to Subject, Content, or Subject or Content, make a decision whether to turn search stemming on or off. Stemming lets you match words that derive from the word that you specify.  For example, the word "run" matches "running" and "ran". You cannot use wildcard characters in conditions that use stemming.
- Click the plus (+) button to save the condition and add another one, if required. For example, you may need to search for items whose Author field contains a nominated author and whose Subject field contains a specified string.
- You define the relationship between two conditions with the And/Or buttons. AND denotes that an item must match both conditions, whereas OR denotes that the item can match one condition but not the other.
- If you want to remove a condition, click the minus (-) button at the right of its row.

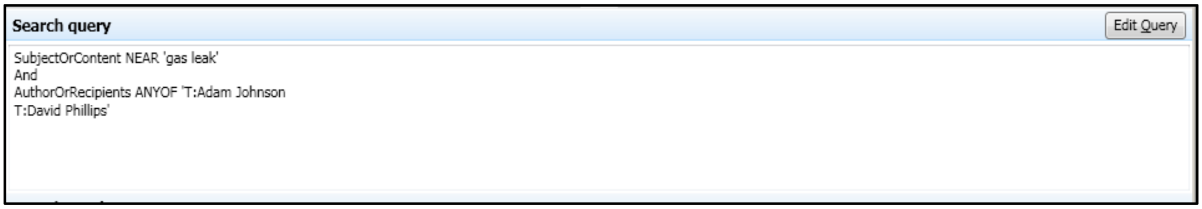


**Search builder**

| | | | | | |
|---|---|---|---|---|---|
| | Subject or content | Near | gas leak | + | − |
| And | Author or recipients | Any of | T:Adam Johnson,T:David Phillips | + | − |
| And ▾ | -Select attribute- ▾ | ▾ | | + | − |

### Search Query

As you add conditions, they appear in the Search query area. The rules that you build in the "Search Builder" display in the analytics rule definition language (RDL) in the "Search query" area.   When you become familiar with the query language, you can construct more complex queries by editing the syntax manually.

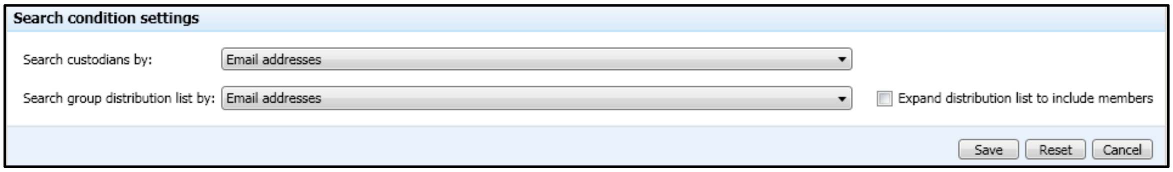


**Search query**

```
SubjectOrContent NEAR 'gas leak'
And
AuthorOrRecipients ANYOF 'T:Adam Johnson
T:David Phillips'
```

### Search Condition Settings

If you have defined one or more Custodians or Custodian Groups with Custodian Manager, use the fields in the Search condition settings area to specify how to search for them. In each Case, you can choose to search E-mail addresses, display names, or both. For Custodian Groups, you can choose to expand the distribution lists of the groups to include their members in your searches, rather than just the list names and E-mail addresses.



Search condition settings

Search custodians by: Email addresses

Search group distribution list by: Email addresses

□ Expand distribution list to include members

The conditions that you enter in the Search conditions settings area use the Custodian information that is available at the time that you build the search. This information is not updated unless you edit the search again. For example, when you create a search and select the option Expand distribution list to include members, the list members at that time are saved with the search. If the membership of the list changes later, these changes are not applied to the search until it is edited and saved again.

Discovery Accelerator does not expand the distribution lists when you use the operators NEAR and NOT NEAR with the attributes Subject, Content, Subject or Content, Author, To, CC, BCC, and Author or Recipients.

### Search Attributes

The following table lists all available attributes, accepted operators, and a description of the attribute.

| Attribute | Type | Accepted Operators | Description |
|---|---|---|---|
| AttachmentsCount | Numeric | =<br>><br>>=<br><<br><= | Use AttachmentCounts to add a condition that is based on the number of E-mail attachments. |
| Author | String | CONTAINS<br>ANYOF<br>NOT CONTAINS<br>NOT ANYOF | Use Author to add a condition that is based on the E-mail's sender.<br>Values that correspond to Targets (T:), Target Groups (TG:), Custodians (C:), and Custodian Groups (CG:) must be on a separate line. Prefixes such as T: and TG: must be in upper case. |

| Attribute | Type | Accepted Operators | Description |
|---|---|---|---|
| AuthorORRecipients | String | CONTAINS<br>ANYOF<br>NOT CONTAINS<br>NOT ANYOF | AuthorORRecipients is a composite attribute that allows you to add a condition that is based on senders and recipients in any of the following attributes:<br>• From<br>• To<br>• CC<br>• BCC<br>Values that correspond to Targets (T:), Target Groups (TG:), Custodians (C:), and Custodian Groups (CG:) must be on a separate line. Prefixes such as T: and TG: must be in upper case. |
| BCC | String | CONTAINS<br>ANYOF<br>ALLOF<br>NOT CONTAINS<br>NOTALLOF<br>NOT ANYOF | Use BCC to add a condition that is based on the E-mail's BCC recipients<br>Values that correspond to Targets (T:), Target Groups (TG:), Custodians (C:), and Custodian Groups (CG:) must be on a separate line. Prefixes such as T: and TG: must be in upper case. |
| CC | String | CONTAINS<br>ANYOF<br>ALLOF<br>NOT CONTAINS<br>NOTALLOF<br>NOT ANYOF | Use CC to add a condition that is based on the E-mail's CC recipients.<br>Values that correspond to Targets (T:), Target Groups (TG:), Custodians (C:), and Custodian Groups (CG:) must be on a separate line. Prefixes such as T: and TG: must be in upper case. |
| Content | String | CONTAINS<br>ANYOF<br>ALLOF<br>NEAR<br>NOT CONTAINS<br>NOTALLOF<br>NOT ANYOF<br>NOT NEAR | Use Content to add a condition that is based on a string in the body of the E-mail, or in the content of a file.<br>Values that correspond to Targets (T:), Target Groups (TG:), Custodians (C:), and Custodian Groups (CG:) must be on a separate line. Prefixes such as T: and TG: must be in upper case. |
| Custom | String | =<br>NOT =<br>CONTAINS<br>ANYOF<br>ALLOF<br>NOT CONTAINS<br>NOTALLOF<br>NOT ANYOF | Use Custom to add a condition that is based on any custom attributes created during archiving. Enter the name of the custom attribute before you select an operator and enter the search string.<br>For example:<br>Custom.Symantec.MyAttribute CONTAINS "Symantec"<br>Values that correspond to Targets (T:), Target Groups (TG:), Custodians (C:), and Custodian Groups (CG:) must be on a separate line. Prefixes such as T: and TG: must be in upper case. |
| Direction | List | =<br>ANYOF<br>NOT =<br>NOT ANYOF | Use Direction to add a condition that is based on the direction of the E-mail. Acceptable values are:<br>• Internal<br>• External Inbound<br>• External Outbound<br>• Not Specified |

| Attribute | Type | Accepted Operators | Description |
|---|---|---|---|
| FileExtension | String | ANYOF<br>CONTAINS<br>NOT ANYOF<br>NOT CONTAINS | Use FileExtension to add a condition that is based on E-mail extension type and files types. Enter multiple file types as a list. For example:<br><br>DOC PDF MSG |
| Importance | List | =<br>ANYOF<br>NOT =<br>NOT ANYOF | Use Importance to add a condition that is based on the E-mail's importance setting. Acceptable values are:<br><br>• Low<br>• Normal<br>• High |
| MailDate | Date | =<br>><br>>=<br><<br><=<br>BETWEEN<br>NOT BETWEEN | Use MailDate to add a condition that is based on the date the E-mail was sent, and on the modified date of the E-mail's attachments.<br><br>When you use the BETWEEN and the NOT BETWEEN operators, you must specify a start and end date. |
| MessageClass | String | ANYOF<br>CONTAINS<br>NOT ANYOF<br>NOT Contains | Use MessageClass to add a condition that is based on the E-mail's MAPI message class setting. For example:<br><br>IPM.Note |
| MessageType | List | =<br>ANYOF<br>NOT =<br>NOT ANYOF | Use MessageType to add a condition that is based on the E-mail's type. Acceptable values are:<br><br>• Exchange Mail<br>• Domino Mail<br>• SMPT Mail<br>• File<br>• Instant Messaging<br>• Bloomberg<br>• Fax |
| ModifiedDate | Date | =<br>><br>>=<br><<br><=<br>BETWEEN<br>NOT BETWEEN | Use the ModifiedDate to add a condition that is based on the date the E-mail or file was last modified.<br><br>When you use the BETWEEN and the NOT BETWEEN operators, you must specify a start and end date. |
| OriginalLocation | String | ANYOF<br>CONTAINS<br>NOT ANYOF<br>NOT CONTAINS | Use the OriginalLocation to add a condition that is based on the original location of the E-mail or file. For example:<br><br>• Inbox<br>• Sent Items<br>• \\server\share\sales |
| Recipients | String | CONTAINS<br>ANYOF<br>NOT CONTAINS<br>NOT ANYOF | Recipients is a composite attribute that allows you to add a condition that is based on recipients in any of the following attributes:<br><br>• To<br>• CC<br>• BCC<br><br>Values that correspond to Targets (T:), Target Groups (TG:), Custodians (C:), and Custodian Groups (CG:) must be on a separate line. Prefixes such as T: and TG: must be in upper case. |

| Attribute | Type | Accepted Operators | Description |
|---|---|---|---|
| RetentionCategory DisplayName | String | CONTAINS<br>NOT CONTAINS | Use RetentionCategoryDisplayName to add a condition that is based on the retention category under which the item was archived. For example:<br>General retention category |
| RetentionExpiryDate | Date | =<br>><br>>=<br><<br><=<br>BETWEEN<br>NOT BETWEEN | Use the RetentionExpiryDate to add a condition that is based on the date the E-mail or file is due to expire. The retention category under which the item was archived determines the expiry date.<br>When you use the BETWEEN and the NOT BETWEEN operators, you must specify a start and end date. |
| Sensitivity | List | =<br>ANYOF<br>NOT = | Use Sensitivity to add a condition that is based on the sensitivity of the E-mail. Acceptable values are:<br>• Normal<br>• Personal<br>• Private<br>• Confidential |
| Size | Numeric | =<br>><br>>=<br><<br><= | Use Size to add a condition that is based on the size of the E-mail or file. |
| Subject | String | CONTAINS<br>ANYOF<br>ALLOF<br>NEAR<br>NOT CONTAINS<br>NOTALLOF<br>NOT ANYOF<br>NOT NEAR | Use Subject to add a condition that is based on strings in the E-mail's subject on in file names.<br>Values that correspond to Targets (T:), Target Groups (TG:), Custodians (C:), and Custodian Groups (CG:) must be on a separate line. Prefixes such as T: and TG: must be in upper case. |
| SubjectOrContent | String | CONTAINS<br>ANYOF<br>ALLOF<br>NEAR<br>NOT CONTAINS<br>NOTALLOF<br>NOT ANYOF<br>NOT NEAR | SubjectOrContent is a composite attribute that allows you to add a condition that is based on strings in any of the following attributes:<br>• Email Subject<br>• Email Body<br>• File Name<br>• File Content<br>Values that correspond to Targets (T:), Target Groups (TG:), Custodians (C:), and Custodian Groups (CG:) must be on a separate line. Prefixes such as T: and TG: must be in upper case. |
| To | String | CONTAINS<br>ANYOF<br>ALLOF<br>NOT CONTAINS<br>NOT ANYOF<br>NOT ALLOF | Use “To” to add a condition that is based on the E-mail's recipients.<br>Values that correspond to Targets (T:), Target Groups (TG:), Custodians (C:), and Custodian Groups (CG:) must be on a separate line. Prefixes such as T: and TG: must be in upper case. |

## Operators

The operators fall into the following categories:

- Single-value operators, which accept one search value only.
- Multiple-value operators, which accept several search values.

### Single Value Operators

The following table lists the single value operators available with description.

| Operator | Description |
|---|---|
| =, NOT = | Use for numbers, dates, and lists. For example: AttachmentsCount=2. |
| <, <=, >, >= | Use for numbers and dates. |
| Contains, NOT CONTAINS | Uses for strings. Wildcards are allowed in the search values. |

### Multiple Value Operators

The following table lists the multiple value operators available with description.

| Operator | Description |
|---|---|
| ALLOF, NOT ALLOF | Use for strings.<br>Searches match items that contain (or do not contain) all the values you supply. For example:<br>CC ALLOF bill@example.com ted@example.com<br>The search matches only items that contain both addresses in the CC field.<br>Wildcards are supported. |
| ANYOF, NOT ANYOF | Use for strings.<br>Searches match the items that contain (or do not contain) any of the values you supply. For example:<br>CC ANYOF bill@example.com ted@example.com<br>This search matches items that contain one of the addresses or both addresses in the CC field.<br>Wildcards are supported. |
| BETWEEN, NOT BETWEEN | Use for dates. For example:<br>MailDate: BETWEEN date1, date2<br>The earlier date must be placed first. |
| NEAR, NOT NEAR | Use for strings.<br>Searches match items where the words that you specify are (or are not) within 50 words of each other.<br>Important Note: Symantec has discovered an issue with |

| Operator | Description |
|---|---|
| | NEAR operator searches in Discovery Accelerator 8.0. This issue is expected to be fixed in SP4 and will function as described. In versions of Discovery Accelerator 8.0 prior to SP4, NEAR operator searches will function as AND operator searches and will return results where all search terms appear in the field or document being searched. |

The syntax for searches that contain multiple value operators is, for example:

attribute operator ‘value1  
“John Doe”  
value3  
T:Jane Smith’

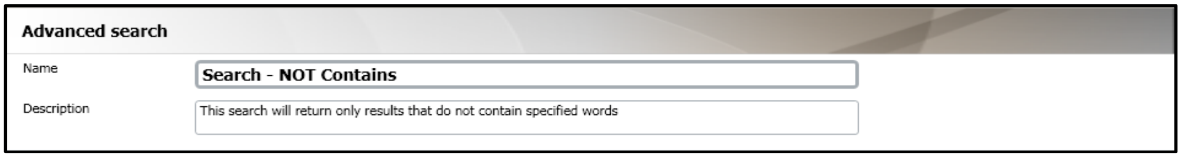
Each Custodian or Target value must be on a separate line.

## Analytic Advanced Search Examples

In this section, examples will be provided for using the advanced analytic search to narrow down the existing results in a Case.

### Example 24: Advanced Analytic Search – NOT Contains

In this example, we will Target the existing results, but search for only those which do not contain the word “Paradise” or the word “Run” and any derivatives such as “Running”, “Ran”, etc.  First name the search and provide a description so that if the search is reused at a later date, you will understand the criteria.

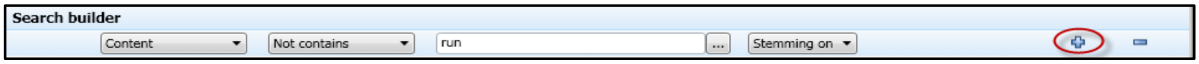


Advanced search

Name: Search - NOT Contains

Description: This search will return only results that do not contain specified words

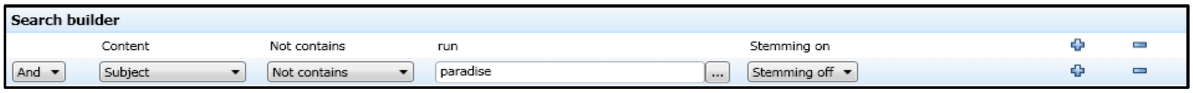
Next, select the attribute “Content”, the operator “NOT Contains”, enter the word “Run”, turn stemming “ON” from the drop-down menu, then click the plus (+) button to add the condition.



Search builder

Content | Not contains | run | Stemming on

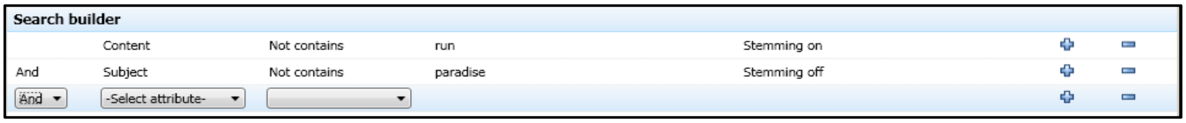
Then repeat the steps for the word “Paradise” but leave stemming in “OFF” position.



**Search builder**

| | | | | |
|---|---|---|---|---|
| | Content | Not contains | run | Stemming on |
| And | Subject | Not contains | paradise | Stemming off |

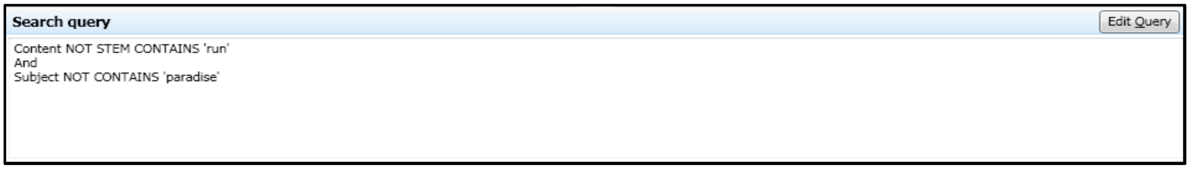
The conditions should be displayed as follows.



**Search builder**

| | | | | |
|---|---|---|---|---|
| | Content | Not contains | run | Stemming on |
| And | Subject | Not contains | paradise | Stemming off |
| And | -Select attribute- | | | |

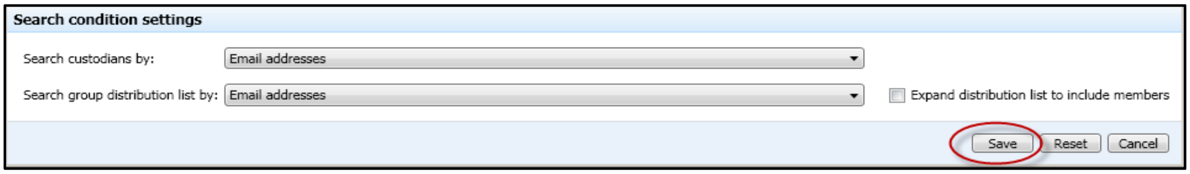
The search query window will now display the raw syntax of the conditions.



**Search query**

```
Content NOT STEM CONTAINS 'run'
And
Subject NOT CONTAINS 'paradise'
```

This search does not include Targets or Custodians therefore the condition settings can remain at the default. Click "Save".



**Search condition settings**

Search custodians by: Email addresses

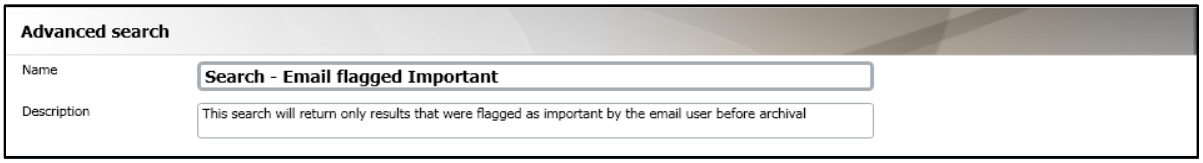
Search group distribution list by: Email addresses

☐ Expand distribution list to include members

The results displayed in the review interface should be only those that do not contain the word "Paradise" or the word "Run" and the derivatives.

**Example 25: Advanced Analytic Search – Importance Flag**

In this example, we will Target the existing results, but search for only those which were flagged by the client as "High Importance". First name the search and provide a description so that if the search is reused at a later date, you will understand the criteria.

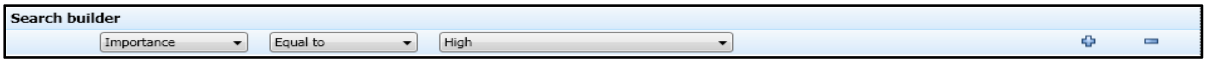


**Advanced search**

Name: Search - Email flagged Important

Description: This search will return only results that were flagged as important by the email user before archival

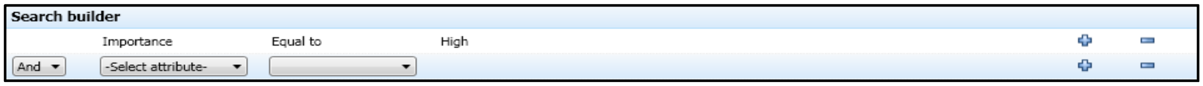
Next, select the attribute "Importance", the operator "Equal To", and the value to "High" from the drop-down menu, then click the plus (+) button to add the condition.



**Search builder**

| | | |
|---|---|---|
| Importance | Equal to | High |

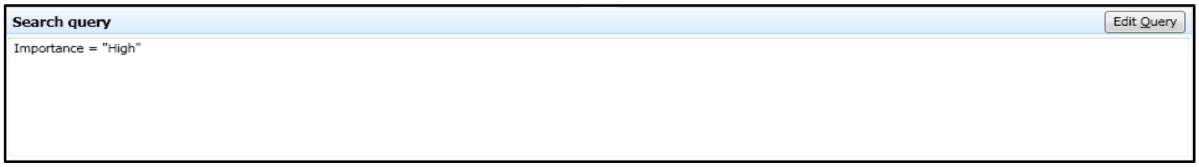
The condition should be displayed as follows.



Importance Equal to High

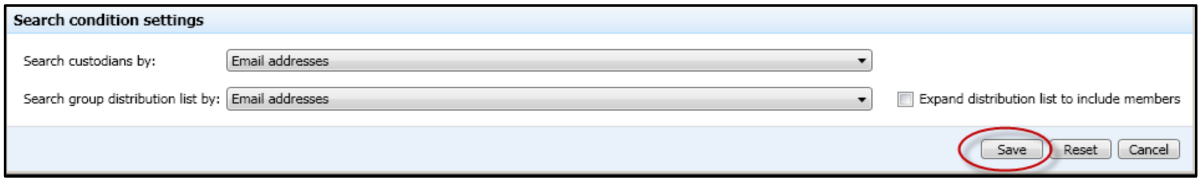
And -Select attribute-

The search query window will now display the raw syntax of the conditions.



Importance = "High"

This search does not include Targets or Custodians therefore the condition settings can remain at the default.  Click "Save".



Search custodians by: Email addresses

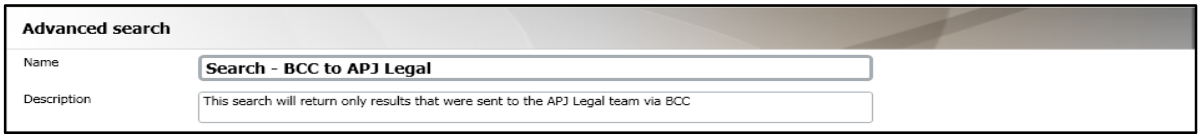
Search group distribution list by: Email addresses

□ Expand distribution list to include members

The results displayed in the review interface should be only those that were flagged by the client as "High Importance".

**Example 26: Advanced Analytic Search – Undisclosed Recipients (BCC)**

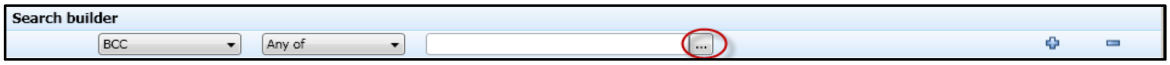
In this example, we will Target the existing results, but search for only those which were sent to the "APJ Legal" distribution list via BCC.  First name the search and provide a description so that if the search is reused at a later date, you will understand the criteria.



Name: Search - BCC to APJ Legal

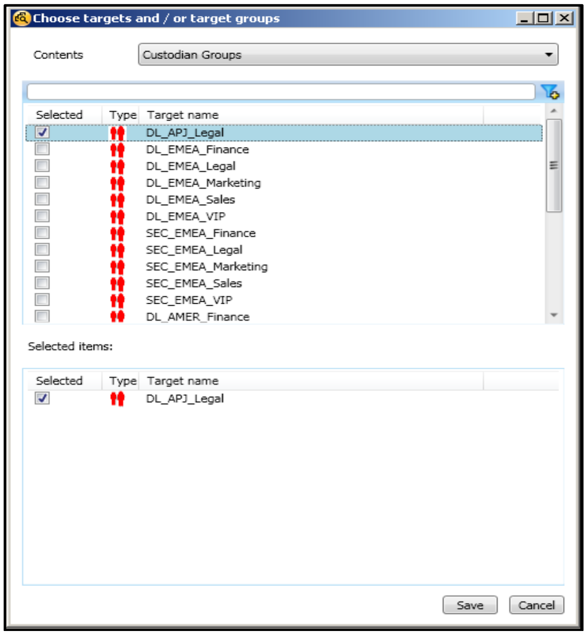
Description: This search will return only results that were sent to the APJ Legal team via BCC

Next, select the attribute "BCC", the operator "Any Of", then click the selection button adjacent to the value field.



BCC Any of

Once the Target and Custodian selection dialogue appears, select "Custodian Groups" from the contents drop-down menu.  Next scroll down and select the "DL_APJ_Legal" Custodian Group and click "Save".



Choose targets and / or target groups

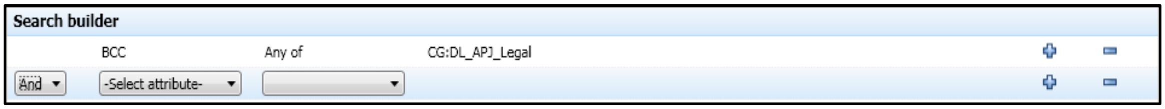
Contents: Custodian Groups

| Selected | Type | Target name |
|---|---|---|
| ☑ | 👥 | DL_APJ_Legal |
| □ | 👥 | DL_EMEA_Finance |
| □ | 👥 | DL_EMEA_Legal |
| □ | 👥 | DL_EMEA_Marketing |
| □ | 👥 | DL_EMEA_Sales |
| □ | 👥 | DL_EMEA_VIP |
| □ | 👥 | SEC_EMEA_Finance |
| □ | 👥 | SEC_EMEA_Legal |
| □ | 👥 | SEC_EMEA_Marketing |
| □ | 👥 | SEC_EMEA_Sales |
| □ | 👥 | SEC_EMEA_VIP |
| □ | 👥 | DL_AMER_Finance |

Selected items:

| Selected | Type | Target name |
|---|---|---|
| ☑ | 👥 | DL_APJ_Legal |

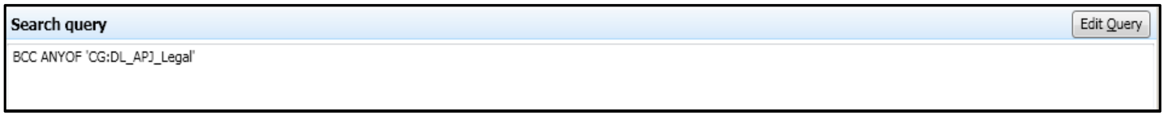
The condition should be displayed as follows.



Search builder

| | | | |
|---|---|---|---|
| | BCC | Any of | CG:DL_APJ_Legal |
| And | -Select attribute- | | |

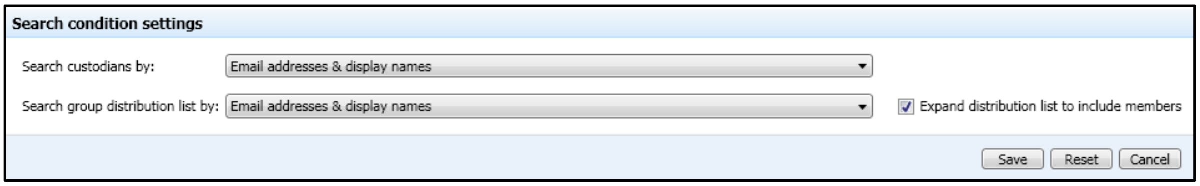
The search query window will now display the raw syntax of the conditions.



Search query

```
BCC ANYOF 'CG:DL_APJ_Legal'
```

This example does include the use of Custodian Groups, so we will modify the condition settings.  From the “Search Custodian by” drop-down menu, select “E-mail addresses and Display names” and from the “Search Group Distribution list by” drop-down menu, select “E-mail addresses and Display names”.  Then select the option to “Expand distribution lists to include members”.



Search condition settings

Search custodians by: Email addresses & display names

Search group distribution list by: Email addresses & display names

☑ Expand distribution list to include members

The results displayed in the review interface should be only those that were sent to the APJ Legal distribution list via BCC.

## Finding all items in the same conversation

In Cases that are enabled for analytics, Discovery Accelerator analyzes the items in the Case as it retrieves the data. Once this analysis is complete, you can easily find all the items that have the same subject line as the current one.

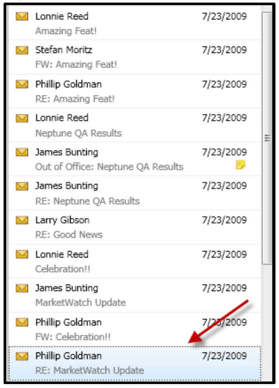
Conversation analysis is based primarily on the subject of the mail items, but also includes other mail attributes that define a conversation. For the purpose of conversation analysis, mail subjects are normalized to remove prefixes that are added by email clients. For example, RE:, Re:, Fwd:, and Antwort: are removed. After normalization, messages must have identical subjects to be considered part of the same conversation.

For any messages generated by Outlook 2003 or later, conversation analysis can also construct a conversation hierarchy. Items from Outlook clients earlier than Outlook 2003 are simply grouped in a flat list. Conversation analysis may find many conversations with a frequently used email subject such as "Hello". In this Case, the Conversation window shows all the results, from multiple conversations, each with its own top level item in the hierarchy. The conversation can display up to 1,000 top level items in the hierarchy.

### Example 27: Find all items for a selected conversation

In this example, we will find all items within the result set which are associated with the conversation titled “MarketWatch Update”.

From the review interface, select any message with the subject line “MarketWatch Update”



Lonnie Reed 7/23/2009
Amazing Feat!

Stefan Moritz 7/23/2009
FW: Amazing Feat!

Phillip Goldman 7/23/2009
RE: Amazing Feat!

Lonnie Reed 7/23/2009
Neptune QA Results

James Bunting 7/23/2009
Out of Office: Neptune QA Results

James Bunting 7/23/2009
RE: Neptune QA Results

Larry Gibson 7/23/2009
RE: Good News

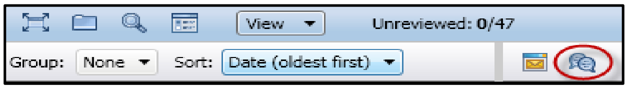
Lonnie Reed 7/23/2009
Celebration!!

James Bunting 7/23/2009
MarketWatch Update

Phillip Goldman 7/23/2009
FW: Celebration!!

Phillip Goldman 7/23/2009
RE: MarketWatch Update

Then click the “Conversation” icon from the toolbar just above the message preview

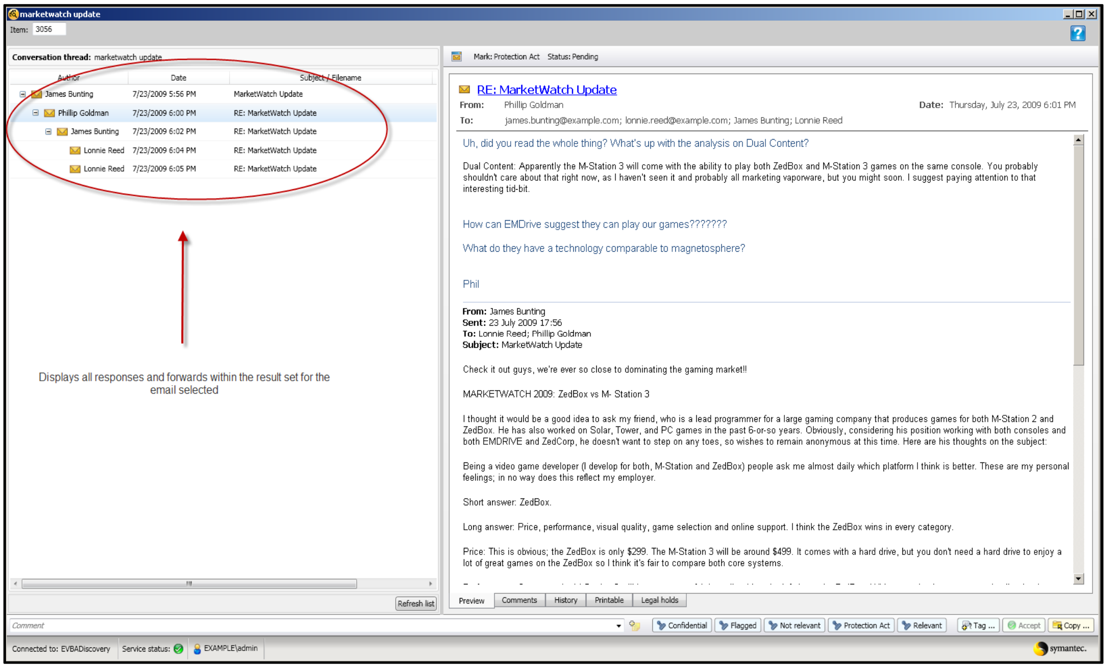


Unreviewed: 0/47

Group: None

Sort: Date (oldest first)

A new window will open and display all items from the same conversation that is contained within the Case.



Item: 3056

**Conversation thread:** marketwatch update

| Author | Date | Subject / Filename |
|---|---|---|
| James Bunting | 7/23/2009 5:56 PM | MarketWatch Update |
| Phillip Goldman | 7/23/2009 6:00 PM | RE: MarketWatch Update |
| James Bunting | 7/23/2009 6:02 PM | RE: MarketWatch Update |
| Lonnie Reed | 7/23/2009 6:04 PM | RE: MarketWatch Update |
| Lonnie Reed | 7/23/2009 6:05 PM | RE: MarketWatch Update |

Displays all responses and forwards within the result set for the email selected

Mark: Protection Act Status: Pending

RE: MarketWatch Update

**From:** Phillip Goldman **Date:** Thursday, July 23, 2009 6:01 PM
**To:** james.bunting@example.com; lonnie.reed@example.com; James Bunting; Lonnie Reed

Uh, did you read the whole thing? What's up with the analysis on Dual Content?

Dual Content: Apparently the M-Station 3 will come with the ability to play both ZedBox and M-Station 3 games on the same console. You probably shouldn't care about that right now, as I haven't seen it and probably all marketing vaporware, but you might soon. I suggest paying attention to that interesting tid-bit.

How can EMDrive suggest they can play our games???????

What do they have a technology comparable to magnetosphere?

Phil

**From:** James Bunting
**Sent:** 23 July 2009 17:56
**To:** Lonnie Reed; Phillip Goldman
**Subject:** MarketWatch Update

Check it out guys, we're ever so close to dominating the gaming market!!

MARKETWATCH 2009: ZedBox vs M- Station 3

I thought it would be a good idea to ask my friend, who is a lead programmer for a large gaming company that produces games for both M-Station 2 and ZedBox. He has also worked on Solar, Tower, and PC games in the past 6-or-so years. Obviously, considering his position working with both consoles and both EMDRIVE and ZedCorp, he doesn't want to step on any toes, so wishes to remain anonymous at this time. Here are his thoughts on the subject:

Being a video game developer (I develop for both, M-Station and ZedBox) people ask me almost daily which platform I think is better. These are my personal feelings; in no way does this reflect my employer.

Short answer: ZedBox.

Long answer: Price, performance, visual quality, game selection and online support. I think the ZedBox wins in every category.

Price: This is obvious; the ZedBox is only $299. The M-Station 3 will be around $499. It comes with a hard drive, but you don't need a hard drive to enjoy a lot of great games on the ZedBox so I think it's fair to compare both core systems.

The Conversation window may not show all the items in a conversation until the retrieval of analytics data is complete for the Case or Research Folder. Even when the retrieval of analytics data is complete, Discovery Accelerator does not include in the results of conversation analysis any items for which it failed to retrieve such data.

## Summary

In conclusion, this White Paper has focused on how to create effective collection searches using Discovery Accelerator. Whether responding to a new research investigation or responding to an adversary, we have provided nearly 30 examples of various search methods using either core search functionality or the new features offered by the Analytics module. While this document is not a replacement for formal training, it will enable you and your team to get started today and will serve as a reference when creating new searches in the future.

# Appendix A

## Enterprise Vault Environment Considerations

Before using the Discovery Accelerator interface, you should have an understanding of what configuration options were selected during the implementation of Enterprise Vault and Discovery Accelerator.

**Important Questions to ask the Enterprise Vault Administrator**

1. If your organization is using Lotus Domino, will journaling be enabled?

   What Is Domino Server Journaling?
   Domino Server journaling lets you record copies of email communications in your organization and store, or journal, them in a Mail Journaling database. The process of journaling is different from archiving. Journaling is simply a means of retaining copies of your users' messages

2. If your environment is using Microsoft Exchange, will Envelope Journaling be enabled, or is there another mechanism in place for capturing undisclosed recipients (BCC information) from journalized E-mails?

   What Is Exchange Journaling?

   Exchange Journaling is the ability to record all communications in an organization. E-mail communications are one of many different communication mechanisms that you may be required to journal. Therefore, journaling in Exchange has been developed to enable the messaging administrator to feed messaging data into a larger journaling solution, while using minimum overhead

   Envelope journaling provides a much more useful service because it records data about all recipients that a message is delivered to. One way to understand how envelope journaling works is in the context of distribution groups. Most distribution lists change, and query-based distribution lists are specifically created based on the fact that lists change. This is important to understand prior as this will affect whether or not the information in the BCC field is available for searching via the "To" searching option. Depending on how Exchange is configured, Enterprise Vault may not process the undisclosed recipients resulting in incomplete or inaccurate search results.

3. Was the Discovery Accelerator environment implemented using Microsoft SQL 2005 or above?
   In order to use the Analytics capabilities, Discovery Accelerator requires a minimum of SQL 2005 on the backend.

4. Is your organization running multiple Enterprise Vault sites due to acquisition or multiple geography implementations? You must ensure that all Enterprise Vault servers are running the same version and service pack. If not, there will be issues with preview of the results, applying legal hold, and production of data from Enterprise Vault servers that are on older versions than that of the Discovery Accelerator server.
5. Is your organization archiving data other than E-mail such as: File Servers, SharePoint Servers, Structured Databases, or Instant Messages?

   If the Enterprise Vault environment includes archives with non-E-mail content and you plan to search based on content-type, then you will need to have an understanding of what information is available in your vault. If you have legacy data that was archived in version 4.1 or earlier, then this option will not be available as it was not added until version 5.

6. What level of indexing has the Enterprise Vault system been configured to use?
   The level of indexing configured will determine what search capability will be available in Discovery Accelerator.

| **Index Level** | **Description** |
|---|---|
| Brief | Allows searching of the metadata associated with the Author, Recipients, Subject, Date Range |
| Medium | Allows searching of the metadata associated with the Author, Recipients, Subject, Date Range, as well as key word searching of the content contained in the message body and the attachments |
| Full | Allows searching of the metadata associated with the Author, Recipients, Subject, Date Range as well as key word and phrase searching of the content contained in the message body and the attachments. |

If the index level must be changed to meet search requirements, the administrator must rebuild any existing indexes to allow the increased capability.

7. Are there multiple Vault Sites in the Enterprise Vault environment?

   Discovery Accelerator has the capability to run federated searches across all sites; however, please note that Retention Categories are Vault Site specific. If you need to base your searches on specific retention categories, a separate search must be run against each site individually unless they share the same Directory. All other search types can span multiple Vault Sites.

### SQL Server noise words

To prevent a full-text index from becoming bloated, SQL Server has a mechanism that discards commonly occurring words such as "the" and "and". These discarded words are called “noise words” in SQL Server 2005 and “stop words” in SQL Server 2008. During index creation, the SQL full-text engine omits noise words from the full-text index, and consequently you cannot search for them by using Discovery Accelerator. For example, a search for the phrase "the lazy dog" returns results where the phrase "one lazy dog" matches.

You can override this behavior by editing the SQL Server noise word file. If you use SQL Server 2005, the following article in the Microsoft Knowledge Base describes how to edit the file:
http://support.microsoft.com/?kbid=905617

If you use SQL Server 2008, the following article provides information on “stop words” and “stop lists”:
http://msdn.microsoft.com/en-us/library/ms142551.aspx

Note that the noise words and stop words are common to all full-text catalogs in the SQL instance.

## Appendix B

Refer to the following use cases to get a better understanding of the expected behavior when using the “include items already in review” option on the search page

**Use Case 1: Narrowing the Search**

An organization created a Case in response to a claim, and ran an initial collection search against involved individuals for a non specific time frame to apply legal hold to all data.

Next, the legal team received the search criteria from opposing counsel.

- Date range
- Key words and phrases

Then, a keyword search was run to narrow down the result set based upon the search criteria. The option “Include items already in review” is selected to include searching against all data previously captured by the initial collection search.
When accessing the results from the review interface, the reviewer could choose to only display results from the key word search. This enables the organization to keep all data on legal hold, but filter on the meaningful result set.

### Use Case 2: Ongoing Matter

An organization created a Case in response to a matter, ran the initial search and ran the secondary search to narrow down the results based upon added search criteria. The matter is ongoing, so the new data created daily must be added to the result set for processing and legal hold until the matter is resolved.

The legal team will create a scheduled search based on the template from the keyword search and configure it to run the nightly schedule to search the date range “Since search last ran”, with no end date. The option “Include items already in review” is de-selected so that only the “Difference” or the “Delta” will be added to the Case on a nightly basis. The option to “Automatically accept search results” could be used in this configuration or optionally the searcher could verify the results daily before manually accepting them into the Case.

When accessing the results from the review interface, the reviewer could choose to display results for all searches for the Case to include results from the nightly search. This enables the organization apply legal hold to newly created, relevant data.

### About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934