Email Archiving Service
Legal Discovery and Supervision Guide

This guide is for Legal and Supervision reviewers – a special set of end-users that do searches throughout the archive and work with other people’s mail for the purpose of investigations or systematic review.

Service Version: ArchivingP_3.5
2009-07-31
Copyrights
This documentation and related technology are governed by a user agreement and shall remain the sole and exclusive property of MessageLabs. No part of this documentation or related technology may be used, reproduced, translated, displayed, distributed, disclosed, stored in a retrieval system or transmitted in any form or by any means without the written permission of MessageLabs, unless otherwise stated in the user agreement. The information contained in this documentation is confidential and proprietary to MessageLabs.

Disclaimer
MessageLabs does not warrant, guarantee or make any representations or otherwise concerning the contents of this documentation or the applicability thereof. MessageLabs reserves the right to change the contents of this document at any time without prior notification of such updates.

Trademarks
All brands or product names are trademarks or registered trademarks of their respective companies or organizations.
Table of Contents

1 Preface 3
   1.1 About this Guide 3
   1.2 Prerequisite Knowledge 3
   1.3 Other Sources of Information 3
   1.4 Contacting Support 3

2 Introduction 4
   2.1 MessageLabs Email Archiving Service Overview 4
   2.2 Accessing MessageLabs Email Archiving Service 5
   2.3 About the MessageLabs Email Archiving Service User Interface 5
   2.4 Setting Preferences 6

3 About Legal Discovery 7
   3.1 Information Management 7
   3.2 Identification, Collection and Preservation Phases of Electronic Discovery 7
   3.3 Analysis, Review and Processing Phases of Electronic Discovery 7
   3.4 Production and Presentation Phases of Electronic Discovery 7

4 About Searching 8
   4.1 How Searching Works 8
   4.2 Search Steps 9
   4.3 Types of Search Criteria 10
   4.4 Saving Search Criteria (Optional) 13

5 Performing Searches 14
   5.1 Content-Based Searching 14
   5.2 Location-Based Searching 15
   5.3 Attachment-Based Searching 17
   5.4 People-Based Searching 18
   5.5 Date-Based Searching 19
   5.6 Communication Flow-Based Searching 20
   5.7 InfoTag-Based Searching 20

6 Working with Search Results 21
   6.1 How Search Results are Presented 21
   6.2 Working with Messages Found by a Search 22
   6.3 Message Properties 23
   6.4 Saving Results in Folders 23

7 Creating and Modifying Legal Holds 26
   7.1 About Legal Holds 26
   7.2 Types of Legal Holds 26
   7.3 Assigning Permissions for Legal Hold Access 27
   7.4 Choosing a Legal Hold Type 27
   7.5 Working with Ad-Hoc Legal Holds 28
1 Preface

1.1 About this Guide

This guide introduces MessageLabs Email Archiving Service and provides step-by-step instructions for using the system to perform advanced searches of your own or other peoples’ mail stored in the archive.

This guide also explains specific functions related to legal holds and message review. These functions are available only to users who have the appropriate user access.

1.2 Prerequisite Knowledge

This document is intended for a business user with technology experience. You should be familiar with functions common to user interfaces, such as selecting multiple items using the Shift key and checking or clearing options.

You should understand your company’s electronic messaging policy. While MessageLabs Email Archiving Service is a critical element of any message compliance system, you play an important role in ensuring that information is used appropriately. Access to the archive of messages comes with a responsibility to understand and apply the standards outlined in your company’s electronic messaging policy.

To take full advantage of advanced search functionality, some basic understanding of Boolean logic is helpful. While the MessageLabs Email Archiving Service user interface attempts to shield you from these complexities, understanding the difference between “A and B or C” and “A and (B or C)” helps to ensure that you achieve expected results when searching the archive.

1.3 Other Sources of Information

This guide covers a number of topics addressing procedural information for day-to-day use. For other information, see:

Online Help: Every screen in MessageLabs Email Archiving Service user interface includes a help button. Click on this button to display information about the steps required to perform tasks on that screen.

Finding Your Own Messages: Explains basic search processes from Microsoft Outlook or OWA. Intended for users who will search the archive for their own messages.

Reports: Explains available reports and how to generate them.

1.4 Contacting Support

Please refer to the information at the end of this guide.
2 Introduction

Chapter Overview

This chapter introduces MessageLabs Email Archiving Service and its main interface elements. The chapter includes the following topics:

- MessageLabs Email Archiving Service Overview
- Accessing MessageLabs Email Archiving Service
- About the MessageLabs Email Archiving Service User Interface
- Setting Preferences

2.1 MessageLabs Email Archiving Service Overview

MessageLabs Email Archiving Service provides a complete message archiving solution that can protect your organization from legal liabilities and regulatory risks while improving email storage management and end-user productivity. Its easy-to-implement, easy-to-use web interface offers fully secure email archiving with robust search and discovery, supervision and enforcement features.

MessageLabs Email Archiving Service securely stores your electronic messages for the retention period you specify, while keeping them fully searchable and retrievable in real-time (or with a batch process). At any time, archived messages can be easily viewed, retrieved to a user’s email inbox or exported to an Outlook data file.

MessageLabs Email Archiving Service includes features used to:

- design, edit and maintain an electronic messaging policy, including retention, enforcement and supervision rules
- perform advanced and comprehensive searches of a message’s header, body, or attachments, easily meeting even the most stringent discovery requirements
- generate reports that help properly assess email patterns and behavior, and help evaluate the effectiveness and enforcement of your policies
- manage mailbox sizes, removing storage-intensive attachments from Exchange while keeping those attachments accessible to Outlook users (stubbing)
- implement a systematic supervision process for selecting and reviewing the content of electronic messages based on your organization’s policy for acceptable use of email

*Note:* Supervision and stubbing functions are optional and may not be available to all users.
2.2 Accessing MessageLabs Email Archiving Service

<table>
<thead>
<tr>
<th>Note:</th>
<th>MessageLabs Email Archiving Service works with Internet Explorer 6 and higher on the PC. You must have JavaScript enabled to access MessageLabs Email Archiving Service.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Open your web browser.</td>
</tr>
</tbody>
</table>
| 2 | Enter the URL of the Archiving Appliance in the address bar of your web browser.  
   The Login Screen appears. If it is blocked by a pop-up blocker, you need to allow pop-ups from this site before proceeding.  
   Your administrator can provide you with the URL of the Archiving Appliance. You may be able to access it using a similar URL to the one you use to access your mail server. For example, if you normally enter https://www.mycompany.com/exchange, you would enter https://mail.mycompany.com/archive. You may need to add the URL to your “trusted sites” list. |
| 3 | Enter the user name and password you use to log in to your computer and click Enter.  
   You can also log in using your primary SMTP address or UPN.  
   The MessageLabs Email Archiving Service interface opens, with the Menu on the left and the Home screen on the right.  
   User names and passwords for MessageLabs Email Archiving Service are fully integrated with your network user name and password. Whenever you change your password on the network, your password used to log in to MessageLabs Email Archiving Service is also changed. |

After a period of 60 minutes of inactivity, you will be logged out automatically. If you attempt to perform a task using your open browser window after you have been automatically logged out, you will be prompted to log in again. Once you do, the action is performed.

2.3 About the MessageLabs Email Archiving Service User Interface

The Menu (on the left) is divided into sections, each containing related functions. Clicking on a section opens it to reveal its contents. When you click a function, the workspace (right side of the screen) changes as a result.

You will be working primarily with the Search & Discovery and Supervision sections, both of which are explained in more detail in the appropriate chapters of this document.
2.4 Setting Preferences

MessageLabs Email Archiving Service user interface preferences allow you to choose:

- the opening screen you see when you log on (for example, if you most often search messages, you can have the interface open with the Search section expanded)
- defaults for standard or advanced searches (sort order, mailbox scope and date range)
- default sort order for review message lists

To set your preferences:
1. Click Preferences (in the top right corner of the interface).
   The Preferences screen appears.
2. Click the appropriate tab and set your preferences.
3. Click Save.
3 About Legal Discovery

3.1 Information Management

One of the best ways to reduce risk during legal discovery is to implement proactive information management practices. The foundation of such an approach is the establishment and enforcement of retention policies. Without clearly defined, and consistent applied, retention of information, it becomes very hard to prove that information was disposed of in the course of normal business as opposed to a malicious destruction of evidence. With MessageLabs Email Archiving’s policy component you can define, communicate and enforce retention of electronic communications.

Capturing all communications in a searchable repository in an unalterable, de-duplicated form provides going litigation readiness.

3.2 Identification, Collection and Preservation Phases of Electronic Discovery

At the point that your organization suspects that a matter may arise, you want to be able to assess the risk to your organization. Collecting data from various sources just to perform early case assessment is often cost-prohibitive, so many firms fail to appreciate their position at this point. With a searchable repository, you can easily search for items that may be relevant and make appropriate plans for addressing the matter. This investigation capability also makes it easier to identify the scope of information that should be covered under a preservation order.

With all content captured in the archive for some time period, it becomes the best place to implement a preservation hold (a “legal hold”, in MessageLabs Email Archiving). Not only can MessageLabs Email Archiving be used to hold existing content that is relevant to the matter, it can also be configured to actively evaluate and hold new messages as they are archived. This avoids the expensive, error-prone manual processes typically required for litigation holds. As information is collected on an ongoing basis, rather than at the point of a litigation hold, the process is quick and painless.

3.3 Analysis, Review and Processing Phases of Electronic Discovery

While the case progresses, you may need to perform ongoing assessment of the contents of the legal hold, for example, to prepare for meetings. The contents of all or just specific legal holds can be searched the same way as the archive can be. Advanced searching capabilities can be used to cull the dataset to focus on the relevant materials, which can then be exported to PST files for integration into a litigation review platform.

3.4 Production and Presentation Phases of Electronic Discovery

For cases that do not require sophisticated review functionality, items that should be produced can be exported to PST file for delivery directly to opposing counsel.
4 About Searching

Chapter Overview

This chapter provides an overview of the advanced searching feature in MessageLabs Email Archiving Service.

This chapter includes the following topics:

- How Searching Works
- Search Steps
- Saving Search Criteria (Optional)

4.1 How Searching Works

You can search within your own mailbox or across some or all of the mailboxes that you have been granted access to. Discovery users can search across the entire archive.

Searching falls into two types: “standard” or “advanced”.

**Standard searching** is intended for end users searching their own mailboxes. It offers the same features as those offered from within Outlook or Outlook Web Access (OWA), and is described in Finding Your Own Messages.

**Advanced searching** provides greater flexibility and control than standard searching. An advanced search contains one or more types of criteria that are combined, allowing you to constrain the search results to specific messages. While each type of search criteria (see “Types of Search Criteria” on page 10) is optional, a message must meet all of the specified criteria to be considered a match.

To repeat a search, you can simply save its criteria and perform it again.

The results of a search are displayed for you to work with: see “Working with Search Results” on page 21.
4.2 Search Steps

Step 1: Open the Search Screen

In the Search & Discovery section, click *Advanced Search*. A search bar showing possible search criteria appears.

Step 2: Enter the Appropriate Search Criteria

Specify search criteria using one of the methods described in this chapter and click *Search* or press ENTER.

*Note:* You can, if you wish, simply leave all criteria blank, but this is not usually desirable because it may retrieve a large set of messages.

Alternatively, you can repeat a recent or saved search by, in the Search & Discovery section, navigating to and selecting the desired search name.

*Note:* Executing a saved search rather than a new search simply applies the saved search criteria to the current data set. Since new messages are added to the archive all the time, search results are likely to be different each time you execute a saved search.

Step 3: View Results

Search results show both the criteria used for the search and the list of messages the search found. For example:

You can modify the search criteria and perform the search again, save the search criteria, clear the criteria and start again, or work with the messages the search retrieved. For instructions, see “Working with Search Results” on page 21.

*Note:* For users of MessageLabs Email Archiving Service batch searching, search results are stored in a folder instead of being displayed on the screen.
4.3 Types of Search Criteria

You can choose to search using one or all of the following criteria.

4.3.1 Content-Based Search Criteria

Search for keywords (optionally, using Boolean AND/OR logic) that must appear in the message content, in the fields that you specify (subject, body, attachment and/or SMTP header). See “Content-Based Search Criteria” on page 10.

4.3.2 Location-Based Search Criteria

Search for:

- only messages in a specific mailbox
- only messages that are part of a specific retention series
- only messages that are in a legal hold
- only messages that are in a specific legal hold, with the further ability to search only messages that were added to that hold manually
- only message that are in the active archive
- messages in either the active archive or any legal hold.

See “Location-Based Searching” on page 15.

4.3.3 Attachment-Based Search Criteria

Search for messages that contain an attachment at all, or only for those with an attachment of a specific type. For example, you can search only for messages with Microsoft Word documents attached. See “Attachment-Based Searching” on page 17.

This search looks only at attachment presence and/or type: if you want to search for the actual content of an attachment, use content-based search criteria.

Note: You can combine attachment-based search criteria with content-based search criteria to look for a particular type of document that features particular words or phrases. For example, you can search for messages with Microsoft Word document attachments that contain the word “Confidential.”

4.3.4 Date-Based Search Criteria

Search for messages based on the date they were:

- sent
- archived (normally the same as the send date, but may be different for imported messages)
- available for disposition.

See “Date-Based Search Criteria” on page 10.

Note: Messages available for disposition need to be removed from the archive using a process explained in the Policy Creation and Management document.
4.3.5 People-Based Search Criteria

Search based on the people who sent or received the message (the parties), and on their participation in the communication (for example, whether they sent it or received it). Messages must match both the specified parties and their type of participation. See “People-Based Searching” on page 18.

4.3.5.1 Specifying the Parties

You can identify the parties for a people-based search based on:

- membership in a user group
- Active Directory user name (the one used for addressing within Outlook), including any associated email addresses.
- display name
- personal or business email address
- Internet mail domain.

When evaluating a message, if any of the elements that define a “party” match, then the message is said to include that person. For example, if a party was defined as being the Active Directory user “John Smith” with the Internet mail address jsmith@hotmail.com, a message sent to either jsmith@hotmail.com or any of the email addresses associated with the Active Directory user “John Smith” would be said to include that party.
4.3.5.2 Specifying the Participation

<table>
<thead>
<tr>
<th>To do this…</th>
<th>Select this criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Find messages where at least one of the selected parties is either the sender or recipient of the message. Use if you don’t care whether the parties are senders or recipients.</td>
<td>From or To ANY of these parties</td>
</tr>
<tr>
<td>Find messages where all of the selected parties are either the sender or recipient of the message. Use if you want to match only messages where all the specified parties are participating as either senders or recipients.</td>
<td>From or To ALL of these parties</td>
</tr>
<tr>
<td>Find messages where at least one of the specified parties is the sender of the message. Use if you want to match only messages coming from specific parties.</td>
<td>From ANY of these senders</td>
</tr>
<tr>
<td>Find messages where at least one of the specified parties is the recipient of the message. Use if you want to match only messages received by specific parties.</td>
<td>To ANY of these recipients</td>
</tr>
<tr>
<td>Find messages where all of the specified parties are the recipient of the message. Use if you want to match only messages where all of the parties are recipients.</td>
<td>To ALL of these recipients</td>
</tr>
<tr>
<td>Using the From ANY of these senders criteria to identify the senders, find messages only where one of the specified parties is a recipient of the message.</td>
<td>From ANY of these senders &amp; To ANY of these recipients</td>
</tr>
<tr>
<td>Using the From ANY of these senders criteria to identify the senders, find messages only where all of the specified parties are a recipient of the message.</td>
<td>From ANY of these senders &amp; To ALL of these recipients</td>
</tr>
<tr>
<td>Find messages exchanged between the selected roles or departments. Use if you want to find messages exchanged between any member of a role or department and any member of another role or department.</td>
<td>Between ANY of these role/department pairs</td>
</tr>
</tbody>
</table>

Note: A sender is the name shown in the FROM field of the message. A recipient is a name shown in any of the TO, CC or Bcc fields.

4.3.6 Communication Flow-Based Search Criteria

Search for messages based on whether they were exchanged internally, received from an external address, or sent to an external address. See "Communication Flow-Based Searching" on page 20.

4.3.7 InfoTag-based Scope Criteria

Search for messages tagged with specific InfoTags (used to categorize a message). See "InfoTag-Based Searching" on page 20.
4.4 Saving Search Criteria (Optional)

Your three most recent sets of search criteria are automatically saved and available in the Search & Discovery section, in a system-created folder called **Recent Searches**. Searches are identified by their occurrence (most recent, next most recent and third most recent).

You can also choose to save search criteria explicitly, in a folder with a name you choose.

**To create a folder to organize saved searches:**
1. In the Search & Discovery section, right-click on **Favorite Searches** (to add a top-level folder).
   - or -
   Right-click on the name of an existing folder (to create a sub-folder underneath it).
2. Choose **New Folder**.
3. When prompted, enter a name for the new folder and click **OK**.
   The folder is created.

**Note:** Within a given level, folder names must be unique. For example, you cannot have two folders directly under **Saved Searches** that are both called **Complaints**, but you can have a **Complaints** folder in a **Customer** folder and a **Complaints** folder in an **Internal** folder.

**Note:** To remove or rename a folder, right-click on it and select **Delete or Rename** from the context menu.

**To save search criteria:**
1. Execute a search.
2. Click **Save Search**.
   The Save Search screen appears.
3. In the **Save search in** tree, select the folder in which the search criteria should be saved.
   - or -
   Click **New Folder** and enter a name for the folder in which the search criteria should be saved.
4. In the **Name** field, enter a name for your saved search.

**Note:** Within a given folder, the names of saved searches must be unique.
5. Click **OK**.
   The Save Search screen closes. The folder tree in the Menu updates.

**Note:** To remove or rename a saved search, right-click on it and select **Delete or Rename** from the context menu.
5 Performing Searches

Chapter Overview

This chapter explains how to perform searches using different types of criteria. It includes the following topics:

- Content-Based Searching
- Location-Based Searching
- Attachment-Based Searching
- People-Based Searching
- Date-Based Searching
- Communication Flow-Based Searching
- InfoTag-Based Searching

5.1 Content-Based Searching

To enter individual content-based search criteria:

1. In the Find field, enter the words or phrases (in quotation marks) to search for.
2. Check the parts of the message (body, subject, attachment and/or heading) that should be searched.

To enter a set of keywords as content-based search criteria:

3. Click the button to the right of the Find field.
   The Keywords screen appears.
4. Choose whether the message must contain one ("or") or all ("and") of the keywords.
5. Enter the keywords to search for in the first text box. Multiple words on one line are interpreted as a phrase.

Note: You can paste into the first text box a list of keywords that has been copied from a file.
6. Click Save.
   The keywords you specified appear, in the correct syntax, in the Find field.
To add additional words/phrases for searching, click the ✓ button to the right of the Find field again.

The Keywords screen appears, with the keywords you specified earlier appearing in the bottom portion of the screen.

To add additional keywords, enter them in the first text box.

Choose how the two lists work together: messages must either match both lists (AND) or either list (OR).

Click Save.

Check the parts of the message (body, subject, attachment and/or heading) that should be searched.

5.2 Location-Based Searching

5.2.1 Searching Based on Mailbox

To search all mailboxes or just your mailbox:

1. Click All Mailboxes (just below the Subject/Body/Attachment/Header area of the search criteria).

   A new screen appears.

2. To search all mailboxes, click All mailboxes.
   - or -
   To search just your mailbox, click My Mailbox.

3. Click Save.

   The selection screen closes.
To search specific mailboxes by group:

1. Click **All Mailboxes** (just below the Subject/Body/Attachment/Header area of the search criteria).
   
   A new screen appears.

2. Click **Only search in the following mailboxes**.

3. Enter the group name in the field.
   
   If you know the specific name, enter it. If you are not sure of the name, enter a partial name and click **Check Name**. Either the name becomes underlined (indicating it can be added) or a list of suggested groups appears for you to choose from.
   
   All mailboxes belong to members of that group are included in the search.

4. Click **Save**.
   
   The selection screen closes.

To search specific mailboxes by user:

1. Click **All Mailboxes** (just below the Subject/Body/Attachment/Header area of the search criteria).
   
   A new screen appears.

2. Click **Only search in the following mailboxes**.

3. Enter the name of the user that owns the mailbox you want to search.
   
   If you know the specific name, enter it. If you are not sure of the name, enter a partial name and click **Check Name**. Either the name becomes underlined (indicating it can be added) or a list of suggested names/groups appears for you to choose from. For names, the list includes two tabs: one for current names, one for deleted names.

4. Repeat until all mailboxes are added.

**Note:** The mailboxes that you can see are controlled by the permissions assigned to your user account.

5. Click **Save**.
   
   The selection screen closes.
5.2.2 Searching Based on Retention Series or Legal Hold

To search based on retention series or legal hold:

1. Click **Active Archive**.
   
   A new screen appears.

2. Choose the scope of the search. To search:
   - within a specific retention series, select it from the retention list
   - both the active archive and all legal holds, click **Active archive and all legal hold** (Discovery Administrators only)
   - just legal holds, click **All legal holds** (Discovery Administrators only)
   - within a specific legal hold, select it from the holds list and choose whether or not you want to show only items manually added by users.

3. Click **Save**.

   The selection screen closes.

**Note:** If searching across all legal holds, the same message may be found in several of those holds. As a result, the message will appear several times in the results list.

5.3 Attachment-Based Searching

To enter file-based search criteria:

1. Check the **Has Attachment** checkbox.

2. Choose the scope of the search. To search for messages with:
   - any type of attachment, select `<ANY TYPE>` from the list
   - a specific type of attachment, select a file type from the list
   - a specific type of attachment not on the list, select **Other** from the list and then, in the text area, type the file extensions of attachments to search for.

**Note:** You can enter multiple file extensions with a space between them. Do not enter periods or wildcards, such as `*.*`. 
5.4 People-Based Searching

To enter people-based search criteria:

1. From the list, select the type of participation.

   The screen updates.

   **Note:** For details on these choices, see “Specifying the Parties” on page 11.

2. Click **Add** and, from the drop-down list that appears, select the party for the search.

<table>
<thead>
<tr>
<th>If you chose…</th>
<th>Then you need to…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Person</td>
<td>Specify the name - or - Enter a personal Internet email address for the person.</td>
</tr>
<tr>
<td>Department, Role, Partner</td>
<td>From the Select a … list, choose the department, role or partner.</td>
</tr>
<tr>
<td>(searches for email belonging to the</td>
<td></td>
</tr>
<tr>
<td>people in the selected user group)</td>
<td></td>
</tr>
<tr>
<td>External Person</td>
<td>Enter the person’s Internet email address and click Add. Repeat for additional</td>
</tr>
<tr>
<td></td>
<td>email addresses for the person.</td>
</tr>
<tr>
<td>Display Name</td>
<td>Enter the display name.</td>
</tr>
<tr>
<td>(searches for messages sent or</td>
<td></td>
</tr>
<tr>
<td>received by the person or group</td>
<td></td>
</tr>
<tr>
<td>matching the selected display name)</td>
<td></td>
</tr>
<tr>
<td>Domain</td>
<td>Enter the Internet domain name.</td>
</tr>
<tr>
<td>(searches for messages sent by anyone</td>
<td></td>
</tr>
<tr>
<td>in the selected domain)</td>
<td></td>
</tr>
</tbody>
</table>

3. Click **Save**.

   The screen closes and the selected party is added to the list.
5.5 Date-Based Searching

**To enter Sent or Archive date-based search criteria:**

1. Click Sent and select the type of date criteria:
   - To search based on the date messages were sent, choose Send Date.
   - or -
   - To search based on the date messages were added to the archive, choose Archive Date.
2. Choose one of the following modifiers:

<table>
<thead>
<tr>
<th>To specify…</th>
<th>Choose…</th>
</tr>
</thead>
<tbody>
<tr>
<td>the date that messages must have been sent on</td>
<td>On</td>
</tr>
<tr>
<td>the last date that messages must have been sent on</td>
<td>Before</td>
</tr>
<tr>
<td>the earliest date that messages must have been sent on</td>
<td>After</td>
</tr>
<tr>
<td>the earliest and the latest date that a message must have been sent on</td>
<td>Between</td>
</tr>
<tr>
<td>messages sent during the current week</td>
<td>This Week</td>
</tr>
<tr>
<td>messages sent during the current month</td>
<td>This Month</td>
</tr>
<tr>
<td>messages sent during the current year</td>
<td>This Year.</td>
</tr>
<tr>
<td>messages sent during the last XX days</td>
<td>Last 30 days. Last 90 days Last 365 days</td>
</tr>
<tr>
<td>messages sent during last 90 days</td>
<td>Last 90 days.</td>
</tr>
</tbody>
</table>

The system displays the appropriate number of calendar fields (for example, if you chose “Between”, it will display two fields).

3. Click in the appropriate calendar fields, click on the desired date.
   Use the arrow keys if necessary to navigate through months and years.

**Note:** “Between” date range criteria are inclusive of the end dates. All other date range criteria are exclusive of the specified date. If you specify a search for anything between today and tomorrow, messages from both days will be included. If you specify a search for anything before or after today, today’s messages are NOT included.

**To enter Disposition or Retention date-based search criteria:**

1. Click on Sent and select the type of date criteria:
   - To search based on the date messages can be disposed, choose Target Disposition Date.
   - or -
   - To search based on the date messages were archived for indefinite retention, choose Indefinite Retention.
2. Select a month from the first list and a year from the second list.
5.6 Communication Flow-Based Searching

From the Flow list, choose

- *Internal* (messages sent between people within the company)
- *Inbound* (messages sent from an external address)
- *Outbound* (messages sent by someone within the company to at least one external address)

5.7 InfoTag-Based Searching

In the InfoTag area, click beside one or more InfoTags. Clicking sets one of three possible states:

- selected ✅
- excluded ❌
- not selected ❌

Select InfoTags to retrieve any messages tagged with any of the selected InfoTags (for example, if you select both “News” and “Travel”, you retrieve messages tagged with either of those InfoTags).

Exclude InfoTags to ignore messages tagged with any of the excluded InfoTags.
6  Working with Search Results

Chapter Overview

This chapter explains the various functions that can be performed on messages retrieved by a search. It includes the following topics:

- How Search Results are Presented
- Working with Messages Found by a Search
- Message Properties
- Saving Results in Folders

6.1 How Search Results are Presented

By default, the messages found by the search are listed on the left, and the details of the selected message appear on the right. Use the toolbar to change this: to display the two areas side by side, click ; to display the list above the message details, click .

The list shows basic information about 15 messages at a time, sorted by the criteria specified in your preferences (see “Setting Preferences” on page 6).

To move through the pages of a multi-page result list, use the navigation buttons at the bottom of the list or choose a page number from the Page list.

**Note:** If your search retrieves many matches, consider narrowing your search criteria to avoid having to navigate through pages.

The results list is temporary and will be replaced by your next search. To gather the results for further analysis, use folders, as explained in “Saving Results in Folders” on page 23.
## 6.2 Working with Messages Found by a Search

<table>
<thead>
<tr>
<th>To…</th>
<th>Do this…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the message details</td>
<td>Click on the message in the list.</td>
</tr>
<tr>
<td>Find related messages</td>
<td>Right-click on the message in the list and choose <em>Find Related in Archive</em> (see “Finding Potentially Related Messages” on page 43).</td>
</tr>
<tr>
<td>Turn highlighting on and off (If you searched for words or phrases, the part of the message containing the words or phrases that matched your search criteria is underlined in yellow)</td>
<td>On the toolbar, click 🍀</td>
</tr>
<tr>
<td>Print a single message</td>
<td>Display the message details and, on the toolbar, click <em>Print</em>.</td>
</tr>
<tr>
<td>Print multiple messages</td>
<td>Select the messages in the list and, on the toolbar, click <em>Print</em>.</td>
</tr>
<tr>
<td>Download the message’s attachment</td>
<td>Display the message details and click on the attachment name. Depending on your browser configuration, you either see the attachment in a new browser window or are prompted to save or open it.</td>
</tr>
<tr>
<td>Retrieve a message to your inbox</td>
<td>Display the message details and, on the toolbar, click <em>Retrieve</em>. The message is sent to your Outlook inbox automatically.</td>
</tr>
<tr>
<td>Retrieve multiple messages to your inbox</td>
<td>Select the messages in the list and, on the toolbar, click <em>Retrieve</em>. The messages are sent to your Outlook inbox automatically.</td>
</tr>
<tr>
<td>View the properties of the message</td>
<td>On the toolbar, click <em>Properties</em>. The multi-tab Message Properties screen, explained below, appears.</td>
</tr>
</tbody>
</table>
| Change the sort order                                               | Click anywhere in the heading of the list and choose, from the menu that appears, the desired sort order:  
  - rank (most relevant first)  
  - sent (newest first, oldest first)  
  - size of message (largest first)  
  - size of attachment (largest first). “Rank” sorts messages based on how closely they match the search criteria. A message’s ranking is represented by stars, with four stars representing the highest ranking (closest match). |
| Copy the message to a folder                                        | See “Saving Results in Folders” on page 23.                                                   |
6.3 Message Properties

Message properties are shown in the following tabs:

- The General tab shows a message's size, the time/date it was sent, received and archived, and other information.
- The Recipients tab shows the people who received the message (Discovery users only).
- The Header tab shows the SMTP header of the message.
- The Audit Trail tab shows the audit trail for the message (Discovery users only).

6.4 Saving Results in Folders

6.4.1 About Folders

Each time you perform a search, since the archive's contents have most likely changed, the search results will likely differ. To save a snapshot of the results of a particular search performed at a specific time, you can create a folder. A folder does not contain the messages themselves, just links to messages in the archive. This means:

- adding items to or deleting them from a folder does not affect the archive
- once a message has been removed from the archive it can no longer be accessed from a folder, even if the folder still has a link to that message
- future searches using the same criteria as used to create the folder in the first place do not affect the folder contents, even if those searches retrieve additional messages

Folders exist in a hierarchy of folder/sub-folder. Within a given level, folder names must be unique. For example, you cannot have two folders directly under My Folders called News, but you can have a News folder within an Industry folder as well as a News folder within a Company folder.

Folders can contain the results of several searches: you either copy or move messages from one folder to another or add new search results to an existing folder. If a message added to a folder already exists in the folder, a duplicate will not be made.

To view the contents of a folder, you simply click on the folder name. The same functions that are performed on search results can be performed on a folder's contents: see “Working with Search Results” on page 21.
6.4.2 Creating Folders

To add items to a new or existing folder:

1. Execute a search and, on the toolbar, click **Copy to Folder**. The Copy To Folder screen appears.

2. Select the folder to which you want the messages added.
   - You can create a folder as well: select a location, and click **New Folder** to create a new folder under that location.
   - **Note:** You cannot add items to **My Folders** itself, only to the folders that it contains.

3. Choose what should be included in the folder:
   - only the most recent xx results
   - all results
   - only the selected items.

4. Click **Save**.
   - The Copy To Folder screen closes and the copy process begins in the background. A confirmation message appears when the copy is complete.

**Note:** Depending on the number of items in the search results, it may take several minutes for all of the items to be added to the folder. When you view the contents of a folder, if items are still being copied to that folder, a progress icon appears in the header.

To create an empty folder for future use:

1. In the Search & Discovery section, right-click on **My Folders** (to add a top-level folder).
   - Or -
   - Right-click on the name of an existing folder (to create a sub-folder underneath it).

2. Choose **New Folder**.

3. When prompted, enter a name for the new folder and click **OK**.
   - The folder is created.
6.4.3 Managing Folders

To remove or rename a folder
1. In the Search & Discovery section, right-click on the folder you want to rename or delete.
2. Choose Delete or Rename.
   - If you chose Rename, the name becomes modifiable.
   - If you chose Delete, you are prompted to confirm a deletion.

To copy items from one folder to another:
1. Execute a search, save the results in a folder, and open that folder.
2. Select the messages you want to copy to another folder.
3. Right-click and choose Copy to Folder.
   - The Copy To Folder screen appears.
4. Select the folder to which you want the messages added
   - You can create a folder as well: select a location, and click New Folder to create a new folder under that location.

Note: You cannot add items to My Folders itself, only to the folders that it contains.

5. Choose whether items should be copied or moved to the selected folder.
6. Click Save.
   - The Copy To Folder screen closes and the copy process begins in the background.

To check the status of the copy process:
1. In the Search & Discovery section, click on the name of the folder that you copied messages to.
   - A list of the messages contained in the folder appears. A title area shows the name of the folder.
   - An icon appears beside the folder name if there are still items being copied to the folder.
2. Click on the icon.
   - The Copy To Folder Status screen appears. Here you can see the description of what is currently being copied to the folder.

To delete items from a folder:
1. In the Search & Discovery section, click on the name of the folder that you copied messages to.
   - A list of the messages contained in the folder appears.
2. Select one or more messages.
3. On the toolbar, click Delete.
   - You are prompted to confirm the deletion, and the items are removed from the folder.

Note: Deleting items from a folder does not remove them from the archive.
7 Creating and Modifying Legal Holds

Chapter Overview

This chapter explains how to create the different types of legal holds. Using these functions requires special access rights that may not be available to all users. For background information on the role of legal holds in the legal discovery process, see “About Legal Discovery” on page 7.

This chapter includes the following topics:

- About Legal Holds
- Types of Legal Holds
- Assigning Permissions for Legal Hold Access
- Choosing a Legal Hold Type Working with Ad-Hoc Legal Holds Working with People-Based Legal Holds
- Managing Legal Holds

7.1 About Legal Holds

A legal hold stores copies of messages in the active archive that need to be retained for legal purposes. As a result, disposing of messages from the active archive does not affect the legal hold’s content. Once a matter is complete, you can release the hold, making the messages available for disposition. (Disposition is explained in Policy Creation and Management.)

The contents of legal holds can be searched (see “About Searching” on page 8) and exported (see “Exporting Messages” on page 32).

Access to specific legal holds can be restricted to only specified users.

7.2 Types of Legal Holds

7.2.1 Ad-Hoc Legal Holds

An ad-hoc legal hold contains all messages that meet the criteria specified in the rules associated with the legal hold. For example, you can specify that the legal hold is to contain all messages exchanged between two specific parties. The rules used to populate ad-hoc legal holds are the same as used in policies and are explained in Policy Creation and Management.

When it is created, this type of legal hold begins adding messages, as they are archived, based on the rule criteria. It does not automatically capture historical messages, although you can search for messages, place them in a folder, and manually add them to the legal hold.

Note: If the messages being manually added to the ad-hoc legal hold already exist in that hold, the messages will be duplicated.

7.2.2 People-Based Legal Holds

A people-based legal hold contains messages belonging to specific users. When it is created, MessageLabs Email Archiving Service populates a people-based legal hold with messages from the active archive and all other legal holds that belong to those users. It will continue to add messages on a go-forward basis.
7.3 Assigning Permissions for Legal Hold Access

Users and groups can be given permissions to search, view the definition of and/or modify the definition of a specific legal hold. As the creator of a legal hold, by default, you have all these permissions.

To assign permissions:

1. Open the legal hold’s **Permissions** tab.
2. Make the legal hold modifiable by clicking **Modify**.
3. Click **Add** and choose whether to add a user or a group.
   A new screen appears.
4. Enter the name of the user or group.
   If you know the specific name, enter it. If you are not sure of the name, enter a partial name and click **Check Name**. Either the name becomes underlined (indicating it can be added) or a list of suggested names/groups appears for you to choose from. For names, the list includes two tabs: one for current names, one for deleted names.
5. Check all the appropriate permissions.
6. Click **Save**.

**Note:** Discovery Administrators automatically have all rights to all legal holds.

7.4 Choosing a Legal Hold Type

<table>
<thead>
<tr>
<th>Feature</th>
<th>Ad-Hoc</th>
<th>People-Based</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contains messages that…</td>
<td>Match rules.</td>
<td>Belong to specific AD user.</td>
</tr>
<tr>
<td>Historical mail captured?</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>When rules change…</td>
<td>Content unchanged</td>
<td>Content added or removed</td>
</tr>
<tr>
<td>Content can be manually added?</td>
<td>Yes (from a folder)</td>
<td>No</td>
</tr>
<tr>
<td>Users can see which of their messages are in a hold and add other messages?</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Duplicate messages appear in hold?</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Copyright © MessageLabs 2009
7.5 Working with Ad-Hoc Legal Holds

7.5.1 Creating Ad-Hoc Legal Holds

1. In the Policy section, click **Manage Holds**. The Hold Manager screen appears.
2. Click **Add**. You are prompted to choose the type of legal hold you want to create.
4. On the General tab, enter a **Name** for the legal hold.
   
   **Note:** Legal hold names must be unique.
5. On the Permissions tab, identify users who can work with this legal hold entry. For instructions, see "Assigning Permissions for Legal Hold Access" on page 27.
6. In the Settings menu, click **Identification Rules** and define the rules to be used to populate the legal hold. For details on these rules, see the Policy Creation and Management document.
7. Click **Save**. The screen closes and the hold is created.
7.5.2 Manually Adding Messages to Ad-Hoc Legal Holds

1. In the Search & Discovery section, click on the name of the folder containing the messages you want to add to the hold.
   A list of the messages in the folder appears.

2. Right-click on the folder and choose Add to Hold.
   The Add to Hold screen appears.

3. From the Add items to list, choose the legal hold to which items should be added.

   Note: Messages in the folder that are also already in the hold are duplicated in the hold.

4. Click Hold.
   The Add to Hold screen closes and the messages are copied, in the background, into the legal hold.

   Note: Depending on the number of items in the folder, it may take minutes or hours for all of the items to be copied to the hold.
   If you attempt to hold more than 10,000 messages, the add to hold request must be authorized by MessageLabs operations.

7.5.3 Impact of Modifying Ad-Hoc Legal Holds

Changes to the rules for the legal hold do not affect existing contents of the hold.
7.6 Working with People-Based Legal Holds

7.6.1 Creating People-Based Legal Holds

1. In the Policy section, click Manage Holds. The Hold Manager screen appears.
2. Click Add. You are prompted to choose the type of legal hold you want to create.
3. Choose People-based Legal Hold and click Next. The People-Based Legal Hold Entry screen appears.
4. On the General tab, enter a Name for the legal hold.
   Note: Legal hold names must be unique.
5. On the Permissions tab, identify users who can work with this legal hold entry. For instructions, see "Assigning Permissions for Legal Hold Access" on page 27.
6. In the Settings menu, click Identification Rules and add the users whose messages are to be included in the hold. If you know the specific name, enter it. If you are not sure of the name, enter a partial name and click Check Name. Either the name becomes underlined (indicating it can be added) or a list of suggested names appears for you to choose from. The list includes two tabs: one for current names, one for deleted names.
7. Click Save. The screen closes and the hold is created.

7.6.2 Impact of Modifying People-Based Legal Holds

Adding an Active Directory user to the hold’s identification rules adds content for that user to the hold. Deleting a user from the hold’s identification rules disposes content for that user from the hold.
7.7 Managing Legal Holds

To modify a legal hold:
1 In the Search & Discovery section, click Manage Holds.
   The Hold Manager screen appears, showing a list of holds and their status.
2 Click on the legal hold for which you want to see information and, on the toolbar, click Properties.
   The Hold Properties screen appears.
3 Click Modify and make the appropriate changes.

Note: As explained earlier in this chapter, modifications to different types of legal holds have different consequences.

To monitor the progress of adding messages to a hold:
1 In the Search & Discovery section, click Manage Holds.
   The Hold Manager screen appears, showing a list of holds and their status.
2 Click on the legal hold for which you want to see information and, on the toolbar, click Properties.
   The Hold Properties screen appears.
3 In the Settings menu, click Status.
   Two tabs of status information appear:
   • the Events tab shows when requests to add items to the hold were placed and what their current status is
   • the Status Info tab, which shows statistics related to the legal hold

Note: If your hold includes more than 10,000 items, the hold event may show up as “blocked”. Contact MessageLabs Service Center to authorize the hold event to continue.

To release a hold:
1 In the Search & Discovery section, click Manage Holds.
   The Hold Manager screen appears.
2 Click on the legal hold that you want to release and on the toolbar, click Release Holds.
   A warning screen appears.
3 Enter a comment.
4 Click Release Hold.
   A confirmation window appears.
5 Click OK.
   The legal hold is marked as released. If you have been granted permission to authorize disposition of messages from the archive, the messages associated with the hold are disposed of automatically. If not, the legal hold will appear in the disposition screens, where an appropriate user can authorize disposition of the messages in the hold.

Note: Adding items to a hold makes a copy of them. The original item is left in the archive and is retained according to its original retention period. As a result, disposing of messages in a hold does not impact the original copy of the message.
8 Exporting Messages

Chapter Overview

This chapter explains how to export the contents of folders so that messages they contain can be viewed by individuals using Outlook. It includes the following topics:

- Encryption’s Role in the Export Process
- Understanding the Export Process
- Exporting Messages from a Folder
- Viewing Exported Messages within Outlook
- Managing the Export Progress

8.1 Encryption’s Role in the Export Process

Messages are stored in MessageLabs Email Archiving Service in encrypted form, and the encryption key is required to decrypt the data into a readable form. This key is maintained on the Archiving Appliance as an integral part of allowing you to search the archive. When you export data from the archive, the MessageLabs Network gathers the messages to be exported, but the data remains in encrypted form until it is processed by the Archiving Appliance.

8.2 Understanding the Export Process

Messages must be placed in a folder before they can be exported. For instructions on working with folders, see “Saving Results in Folders” on page 23.

Note: For batch search users, messages are always found in a folder.

Exporting messages is done via an export job. When you initiate an export in the user interface, the job is queued for processing in the background. You can check its status at any time. You do not need to be logged into MessageLabs Email Archiving Service for the export to be processed.

Messages in the folder are exported to an Outlook Personal Folders file (PST). This allows the messages to be viewed and managed using Microsoft Outlook. All of the richness of the original message is maintained because the data remains in email format. Multiple PST files will be created if you export more than 1GB of data (since each PST file has a maximum size of 1GB).
8.3 Exporting Messages from a Folder

To export the contents of a folder:

1. In the Search & Discovery section, click on the name of the folder containing the messages you want to export.
   The result list shows a list of the messages in the folder.
2. Right-click on the folder name and choose Export.
   The Export Folder screen appears, showing the estimate length of time the export will take.

3. Enter a name and, optionally, description for the export job.

   Note: Export names must be unique. Currently there is only one export file type.

4. Choose what appliance you want to use for the export.
5. Click Export.
   The Export screen closes and the export process begins in the background.

   Note: Depending on the number of items in the folder, it may take minutes or hours for all of the items to be exported.

6. While the export process is underway, you can monitor its progress.
   Follow the steps in “Managing the Export Progress” on page 34.
7. When the export process is complete, click View Jobs, then My Completed Jobs.
   The My Completed Jobs screen appears.
8. Click on the export job that has the data you want to download and, on the toolbar, click Download.
   The export job file list dialog is displayed.
9. Click Download Now beside the file you want to download.
10. When prompted by the browser, click Save and navigate to the location where the file should be saved.
    The download process starts. When the download is complete, the PST files of exported data are in the directory specified. To view the exported messages in Outlook, follow the procedure below.
8.4 Viewing Exported Messages within Outlook

To view the PST file containing exported messages within Microsoft Outlook:

1. Open Microsoft Outlook.
2. On the File menu, select Open, then select Outlook Data File.
   The Open Outlook Data File screen appears.
3. Select the .pst file you want to open, then click OK.
   The Open Outlook Data File screen closes. The name of the folder associated with the data file
   appears in the Folder List.
4. Select the name of the folder in the Folder List.
   The contents of the exported data appear within Microsoft Outlook.

Note: To view the Folder List, on the Go menu, click Folder List.

8.5 Managing the Export Progress

User Managers can view and delete any job belonging to any user.

To monitor the progress of an export job:

1. In the Search & Discovery section, click View Jobs, then My Pending Jobs.
   The Exported Data screen appears. For each job, you can see the export status.
2. Click on the export job for which you want to see information.
3. Click Properties.
   The Export Item Properties screen appears. From here you can see when the job was created, and
   each time its status changed.

To cancel an export job:

1. In the Search & Discovery section, click View Jobs, then My Pending Jobs.
   The Pending Jobs screen appears.
2. Click on the export job that you want to cancel then, on the toolbar, click Delete.
   A confirmation window appears.
3. Click OK.
   The job is cancelled.

Note: You can only cancel an export job that is not in the "Ready" state.

To delete an export job and any downloadable data:

1. In the Search & Discovery section, click View Jobs, then My Completed Jobs.
   The My Completed Jobs screen appears.
2. Click on the export job that you want to delete.
3. On the toolbar, click Delete.
   A confirmation window appears.
4. Click OK.
   The job, and any exported data, is removed.
Chapter Overview

This chapter introduces concepts and procedures for systematic review of the content of messages using the optional MessageLabs Email Archiving Service Supervision functions.

This chapter includes the following topics:

- About Supervision
- For Reviewers: Passing and Failing Messages
- For Senior Reviewers: Supervision Interface
- For Senior Reviewers: Review Tasks
- For Senior Reviewers: Issue Investigation and Management Tasks

9.1 About Supervision

9.1.1 Your Role in Supervision

As a Supervision user, you are responsible for reviewing messages to determine if they comply with your company’s policies. The messages you will review fall into three general categories:

- messages that the system has identified and flagged as potentially violating a specific policy
- messages that the system has randomly picked for review
- messages that another reviewer has flagged as potentially violating a specific policy

Messages that require review appear in a review queue. You see only those messages that you are allowed to review (for example, only messages that belong to people who report to you).

Note: Messages sent by an internal person (an employee) are considered to be owned by the sender, not by those who received them. Messages sent into the company from external people (non-employees) are considered to be owned by the first internal party on the To, cc or bcc lines.

In environments with a review team, all team members see the same queue. Opening a message for review locks the message: other team members cannot review it.

In addition to the message content, messages seen in the review queue indicate what, if any, policies they may have violated, and, if appropriate, the risk level associated with that violation.
9.1.2 Reviewing Messages

Your system may have been set up for standard review or hierarchical review.

9.1.2.1 Standard Review

In standard review, the messages you see are those that belong to a set of users, whether or not they may have violated a specific policy. You can pass or fail these messages, removing them from the queue. When you fail a message, you indicate the policies you believe it has violated.

9.1.2.2 Hierarchical Review

In hierarchical review, you may be either a general reviewer or an expert reviewer.

If you are a general reviewer, you see only messages the system has randomly selected. You can pass or fail these messages. Passing a message removes it from the queue, failing it may escalate it to an expert reviewer (for example, a legal specialist) to review, depending on the policies you indicate the message may have violated.

If you are an expert reviewer, you see only messages that have been flagged (by the system or another reviewer) as potentially violating the specific policies for which you are an expert. Passing a message may remove it from the queue or, if the message is flagged as potentially reviewing multiple policies, may make it available for the review of another expert reviewer. Failing a message removes it from the queue.

9.1.3 Types of Reviewers

You may be either a reviewer or a senior reviewer.

If you are a reviewer, you see only a single message a time, from oldest to most recent. You simply choose to pass or fail a message and do not perform any other functions.

If you are a senior reviewer, you can perform review functions on messages that you choose from list. You can also perform other monitoring and resolution processes, including batch processes.

Note: Batch processes, which generally defeat the purpose of supervision, are typically used to clear the review queue of repeat messages (such as SPAM) or to clear the queue in the event of a backlog.
9.2 For Reviewers: Passing and Failing Messages

To pass messages:
1. In the Supervision section, click **Review Messages**.
   The next message that you are able to process appears showing, at the top, a list of any policies it may have violated.
2. To pass the message without comments, on the toolbar, click **Pass** or click the arrow next to **Pass** and choose **Pass Without Comments**.
   -or-
   To pass the message with comments, click the arrow next to **Pass** and choose **Pass With Comments**. Add your comments in the screen that appears.
   The message is flagged as a pass (not violating any policy) and the next message appears for processing.

   **Note**: In a hierarchical review process, the message may still be seen by another reviewer if policy violations for which you are not an expert have been identified.

To fail messages:
1. In the Supervision section, click Review Messages.
   The next message that you are able to process appears showing, at the top, a list of any policies it may have violated.
2. Click **Fail/Escalate**.
   The Review Violations and Comments screen appears, listing the policies that your company requires messages to comply with.
3. Check the checkbox beside each policy that you feel the message violates.
4. In the **Comments** field, enter comments that explain your choice.
   Comments may appear in email notifications sent to interested parties.
5. Click **OK**.
   The Review Violations and Comments screen closes. The message is flagged as violating the selected policy entries, any email notifications that are configured for the selected policies entries are sent and the next message appears for processing.

   **Note**: Even if you fail a message, it may still be escalated if other higher-priority policy violations for which you are not an expert have been identified.
### Area Description

<table>
<thead>
<tr>
<th>Area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review Messages</td>
<td>Displays the next available message for you to review.</td>
</tr>
<tr>
<td>Message List</td>
<td>Displays a list of all messages available to be reviewed.</td>
</tr>
<tr>
<td>Deferred Message List</td>
<td>Displays messages for which review has been deferred.</td>
</tr>
<tr>
<td>Passed Message List</td>
<td>Displays list of messages passed by any reviewer. You can choose to fail such messages.</td>
</tr>
<tr>
<td>Failed Message List</td>
<td>Displays list of messages failed by any reviewer and for which all the appropriate remedial action has not been taken. You can choose to pass such messages.</td>
</tr>
<tr>
<td>Closed Message List</td>
<td>Displays list of messages failed by another reviewer and subsequently closed, indicating the issue has been resolved.</td>
</tr>
<tr>
<td>Ignored Message List</td>
<td>Displays list of messages which have been ignored.</td>
</tr>
<tr>
<td>Queue Status</td>
<td>Shows status information for each reviewer, including the number and age of items available for each reviewer.</td>
</tr>
<tr>
<td>Unreviewable Messages</td>
<td>Shows details of circumstances that resulted in messages that could not be reviewed being placed in the queue. Usually this is because no reviewer has been assigned permissions to review such messages. This list indicates what changes need to be made in order to have those messages processed.</td>
</tr>
</tbody>
</table>

**Note:** The default sort order for each list can be set using Preferences (see “Setting Preferences” on page 6).
Click on any list to open it. The display is the same for all lists:

<table>
<thead>
<tr>
<th>Functions available for selected message.</th>
<th>Use to filter messages (for example, to show just messages that violated a specific policy).</th>
</tr>
</thead>
<tbody>
<tr>
<td>messages in opened list.</td>
<td>Displays supervision history for message.</td>
</tr>
<tr>
<td></td>
<td>Potential violations by selected message.</td>
</tr>
<tr>
<td></td>
<td>Selected message.</td>
</tr>
</tbody>
</table>

### 9.4 For Senior Reviewers: Review Tasks

**To review and, optionally, process messages:**

1. In the Supervision section, click the appropriate list. A list of the appropriate messages (for example, passed messages) appears.
2. Click on the messages that you want to work with.

**Note:** Use the Control or Shift keys to select multiple messages, as you would in a Windows application.

The message details appear, showing any potential violations previous reviewers, or the system, have identified.

3. Choose a function to perform on the message (see below).

<table>
<thead>
<tr>
<th>To…</th>
<th>Do this…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Find related messages</td>
<td>Right-click on the message in the list and choose Find Related (see “Finding Potentially Related Messages” on page 43).</td>
</tr>
<tr>
<td>Print messages</td>
<td>Select the messages to be printed and, on the toolbar, click <em>Print</em>.</td>
</tr>
<tr>
<td>Download the message’s attachment</td>
<td>Display the message details and click on the attachment name. Depending on your browser configuration, you either see the attachment in a new browser window or are prompted to save or open it.</td>
</tr>
<tr>
<td>Retrieve messages to your inbox</td>
<td>Select the messages to be retrieved and, on the toolbar, click <em>Retrieve</em>. The messages are sent to your Outlook inbox automatically.</td>
</tr>
<tr>
<td>View the properties of the selected message.</td>
<td>On the toolbar, click <em>Properties</em>. The multi-tab Message Properties screen, explained below, appears.</td>
</tr>
<tr>
<td>To...</td>
<td>Do this...</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Change the sort order                    | Click anywhere in the heading of the list and choose, from the menu that appears, the desired sort order.  
|                                          | The “default” sort order presents messages in this order, from oldest to newest in each category:  
|                                          | • Messages failed (escalated) by another reviewer  
|                                          | • Message the system suspects of violating a policy  
|                                          | • Randomly selected messages  
|                                          | You can also sort by send date (newest or oldest first).                   |
| Pass or fail the message                  | See instructions below.                                                   |
| Defer processing the message             | Select the message to be deferred and, on the toolbar, click Defer. You are prompted to add comments explaining the deferral. Any existing suspected policy violations remain intact. |
| Comment on the message                    | Select the message and, on the toolbar, click Comment. You are prompted to enter comments. |
| Ignore the message                        | Right-click on the message and choose Ignore. You are prompted to enter comments.  
|                                          | **Note:** Ignored messages are not considered processed, and therefore do not impact the percentages in reports. |
| Display the message's supervision history | Click ![icon](image) in the header bar of the open message. A list of the supervision actions taken on the message, including added comments, appears. |

**Note:** You are often prompted to enter comments. These comments may appear in email notifications sent to interested parties.

**To pass messages:**

1. Select the messages you want to pass.
2. To pass the messages without comments, on the toolbar, click the arrow next to Pass and choose Pass Without Comments.
   - or -
   To pass the messages with comments, click the arrow next to Pass and choose Pass With Comments. Add your comments in the screen that appears.

**Note:** If you have a single message selected, clicking Pass means passing without comments. If you have multiple messages selected, clicking Pass means passing with comments. The same comment applies to all selected messages.

The messages are flagged as passed (not violating any policy) and the view pane is updated.
To fail or escalate messages:
1. Select the messages you want to fail or escalate.
2. On the toolbar, click Fail/Escalate.
   A new screen appears, listing the policies that your company requires messages to comply with.
3. Check the checkbox beside each policy that the messages violate.

   Note: When you fail multiple messages, all of them are assigned the same violations.
4. Enter comments that explain your choice.
   Comments may appear in email notifications sent to interested parties.
5. Click OK.
   The new screen closes. The message is flagged as violating the selected policies, any email
   notifications that are configured for the selected policies are sent and the view pane is updated.

9.5 For Senior Reviewers: Issue Investigation and Management Tasks

9.5.1 Tracking Issues to Resolution

Indicating that a message has violated a specific policy is only the first step in resolving the issue. To ensure that the policy
violation is addressed, further steps (such as training or disciplinary action) are necessary. This process is supported by
MessageLabs Email Archiving Service.

Messages, whether passed or failed, are moved to a specific list that can be viewed. Furthermore, messages in these lists can
have a comment attached to them. For a passed message, the comment can be useful to indicate the reasons for passing a
message that others might find problematic. For a failed message, the comment can be used to track steps taken to remedy
the situation.

Once the issue is entirely resolved, the message can be marked as “closed”. This removes it from the failed messages list,
leaving that message to reflect only outstanding issues.

9.5.2 Closing a Failed Message

Close failed messages once action has been taken to resolve the issue. This makes it easier to identify issues that have not
been dealt with yet.

   To close a failed message:
1. Open the Failed Messages list and select the messages you want to close.
2. On the toolbar, click Close.
   A new screen appears, prompting for your comments about the closed message.
3. Enter review comments.
4. Click OK.
   The message is moved to the Closed Messages list.
9.5.3   Forwarding or Retrieving Messages

You can either retrieve a message to your Inbox for further work or can forward the message to another party, internal or external, for their input. The recipient sees the original message as an attachment. When the recipient opens the attachment, they see a link to the message in the archive. Clicking on this link allows them to log into MessageLabs Email Archiving Service, and go directly to the message.

To forward or retrieve a message:
1. Select the messages you want to forward or retrieve.
2. On the toolbar, click Retrieve.
   The Retrieve screen appears.
3. To retrieve the message to your inbox, select Retrieve to my inbox.
   -or-
   To forward it to someone else, select Forward to and enter the SMTP of the recipient. Optionally, enter comments to be used in the body of the message the recipient sees.
4. Click OK.
   A confirmation message appears.
9.5.4 Finding Potentially Related Messages

While reviewing a message you may encounter suspicious activity that warrants further investigation. To aid this investigation, you can search the archive for messages with similar information.

To find potentially related messages:

1. Right-click on a message and choose **Find Related in Archive**. The Find Related in Archive screen appears.

2. Choose when you want to find:
   - messages that have a similar subject line
   - messages that were sent within specified number of days
   - messages sent/receive by any of these parties.

3. Click **OK**. A search is performed and the results are displayed to you. You can perform any of the usual functions on these messages.
Chapter Overview

This chapter describes how to use the audit trail to see information on specific activities performed by users. It includes the following topics:

- About the Audit Trail
- Viewing the Audit Trail

10.1 About the Audit Trail

Discovery users can use the audit trail to view:

- Search criteria entered by users, including user name and date.
- Messages viewed by users, including user name, date and MessageLabs Email Archiving Service function used to view the message.
- Attachments viewed by users, including message the attachment belongs to.
- Supervision† events carried out, including all the details available from the Supervision function.

They can also view any message associated with an activity by clicking on the entry in the audit trail.

Note: The audit trail for a specific message can be viewed by right-clicking on the message in the results list. See “Working with Search Results” on page 21 for details on working with the results list.

10.2 Viewing the Audit Trail

To view the audit trail:

1. From the Setup section, click View Audit Trail. The Audit Trail screen appears.
2. Optionally, display information only for a specific user by enabling the Performed by Specific option and entering a name.
3. Optionally, specify the kind of activities you want to view by checking the appropriate items in the list on the right.
   Discovery users can see Searches, Message View and Attachment View activities, while User Managers can see Login (successful or unsuccessful) activities only. You can choose one or several activities to display.
4. Optionally, specify a time limitation for the activities by choosing from the Event Date list. Depending on what you choose, you may be prompted for more information. For example, if you choose an Event Date of “On”, you are prompted to choose the date.
5. Click Update List. A list of the selected activities, for the selected users, on the selected date, appears.

To sort the list, click anywhere in the header and choose a sort option.
<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active archive</td>
<td>The full contents of the archive. Does not include any messages that have been disposed of from the archive but remain in legal holds.</td>
</tr>
<tr>
<td>Batch Search</td>
<td>Service that allows batch searching only, with the search taking place as a background process. Search results are placed in a folder for further analysis. Some functions are not available in this service.</td>
</tr>
<tr>
<td>Department</td>
<td>A MessageLabs Email Archiving Service user group, representing users who belong to an organizational unit.</td>
</tr>
<tr>
<td>Discovery User</td>
<td>MessageLabs Email Archiving Service user who can search archived messages in any mailbox.</td>
</tr>
<tr>
<td>Disposition</td>
<td>Process of removing a message from the archive when its disposition date has been reached.</td>
</tr>
<tr>
<td>External person</td>
<td>Someone who does not work for your company.</td>
</tr>
<tr>
<td>InfoTag</td>
<td>Metadata assigned to a message to characterize it for searching and policy entry use.</td>
</tr>
<tr>
<td>Internal person</td>
<td>Someone who works for your company.</td>
</tr>
<tr>
<td>Legal hold</td>
<td>Container for messages that have reached the end of this disposition period but need to be retained for legal purposes.</td>
</tr>
<tr>
<td>Partner</td>
<td>A MessageLabs Email Archiving Service user group, representing external users such as lawyers or customers. Rules can apply to partners.</td>
</tr>
<tr>
<td>Pass/fail</td>
<td>Used in MessageLabs Email Archiving Service Supervision. Reviewers determine if messages pass (do not contravene acceptable use policy entries) or fail (contravene acceptable use policy entries).</td>
</tr>
<tr>
<td>Retention period</td>
<td>The period of time a message is intended to be retained, under normal circumstances. Determined by the retention policies active at the time the message was archived.</td>
</tr>
<tr>
<td>Retention series</td>
<td>Messages archived according to the same retention policy.</td>
</tr>
<tr>
<td>Role</td>
<td>A MessageLabs Email Archiving Service user group, representing users with similar job functions. Rules can apply to roles.</td>
</tr>
<tr>
<td>Supervision user</td>
<td>A MessageLabs Email Archiving Service user who can review and evaluate other person’s messages. Depending on privileges, this user may also be able to perform other review functions such as batch processing and reviewing messages processed by other reviewers, or be able to view reports about the number and nature of violations of the corporate electronic communications policy.</td>
</tr>
<tr>
<td>User group</td>
<td>Role, department (internal person) or partner (external person).</td>
</tr>
<tr>
<td>User manager</td>
<td>A MessageLabs Email Archiving Service user who can assign privileges to other users and who can create and manage roles and departments.</td>
</tr>
</tbody>
</table>
access, 5
ad-hoc legal holds
  about, 26
  adding messages to, 29
  creating, 28
  effects of modifying, 29
archive date, searching by, 19
attachment, downloading from message list, 39
attachment, downloading from results list, 22
attachment-based search criteria
  about, 10
  using, 17
audit trail
  about, 45
  viewing, 45
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
cancel export, 34
Closed Message List area, 38
closing messages, 41
commenting on messages, 40
failure messages
  reviewers, 37
  senior reviewers, 41
filtering message list, 39
finding related messages, 43
folders
  about, 23
  copying items between, 25
  creating, 24
  deleting items from, 25
  removing, 25
  renaming, 25
forwards messages, 42
general reviewer, 36
encryption, 32
expert reviewer, 36
export job, 32
exporting messages
  about, 32
  cancel, 34
  delete, 34
  encryption, 32
  monitoring progress, 34
  performing, 33
  viewing, 34
defaults, setting, 6
Deferred Message List area, 38
deferring processing of messages, 40
delete exported messages, 34
displaying found message, 22
disposition date, searching by, 19
E
encryption, 32
expert reviewer, 36
export job, 32
exporting messages
  about, 32
  cancel, 34
  delete, 34
  encryption, 32
  monitoring progress, 34
  performing, 33
  viewing, 34
F
Failed Message List area, 38
failing messages
  reviewers, 37
  senior reviewers, 41
filtering message list, 39
finding related messages, 43
folders
  about, 23
  copying items between, 25
  creating, 24
  deleting items from, 25
  removing, 25
  renaming, 25
forwards messages, 42
general reviewer, 36
Copyright © MessageLabs 2009
hierarchical review. about, 36
highlight in found message, 22
Ignored Message List area, 38
ignoring messages, 40
inbox, retrieving messages from message list, 39
inbox, retrieving messages from results list, 22
InfoTag-based search criteria
   about, 12
   using, 20
job, export, 32
legal holds
   about, 26
   access to, 27
   adding messages to ad-hoc, 29
   ad-hoc, about, 26
   choosing type, 27
   creating ad-hoc, 28
   creating people-based, 30
   effects of modifying ad-hoc, 29
   effects of modifying people-based, 30
   modifying, 31
   monitoring progress of, 31
   people-based, about, 26
   releasing, 31
   searching, 17
   types of, 26
location-based search criteria
   about, 10
   using, 15
mailboxes, searching specific, 15
message list
display, 39
filter, 39
printing messages, 39
sort order, 40
Message List area, 38
message ownership, 35
messages
closing (senior reviewers), 41
commenting on, 40
deferring process of, 40
downloading attachment from message list, 39
downloading attachment from results list, 22
failing (reviewers), 37
failing (senior reviewers), 41
finding related, 43
finding related (senior reviewers), 42
forwarding (senior reviewers), 43
ignoring review of, 40
passing (reviewers), 37
passing (senior reviewers), 40
printing from message list, 39
printing from results list, 22
retrieving to inbox from message list, 39
retrieving to inbox from results list, 22
reviewing. See supervision
reviewing (senior reviewers), 39
supervision history, 40
viewing properties of in message list, 39
viewing properties of in results list, 22
messages, exporting. See exporting
messages, searching. See searching
opening screen, setting, 6
overview, 4
participants, searching for, 18
Passed Message List area, 38
passing messages
reviewers, 37
senior reviewers, 40
people-based legal holds
   about, 26
   creating, 30
   effects of modifying, 30
people-based search criteria
   about, 11
   using, 18
phrases, searching for, 14
preferences, 6
printing messages from message list, 39
printing messages from results list, 22
properties of message, 23
PST file, 32

Q
Queue Status area, 38

R
retention date, searching by, 19
retention series, searching, 17
retrieving messages to inbox from message list, 39
retrieving messages to inbox from results list, 22
Review Messages area, 38
review queue, 35
reviewer
   about, 36
   tasks, 37
reviewing messages. See supervision
reviewing messages, senior reviewers, 39

S
search criteria
   saving, 13
   types, 10
search results
   display, 21
   displaying message, 22
   highlight in, 22
   printing messages, 22
   saving in folders, 23
   sort order, 22
   working with, 21
searching
   about, 8
   basic steps, 9
   by date, 19
   for attachments, 17
   for content, 10
   for participants, 18
   for phrases, 14
   for words, 14
   legal hold, 17
   retention series, 17
   saving results in folders, 23
   saving search criteria, 13
   search criteria types, 10
   specific mailboxes, 15
senior reviewer
   about, 36
   tasks, 39
sent date, searching by, 19
sort order in message list, 40
sort order in search results, 22
sort order, default, 6
standard review about, 36
steps in searching process, 9
supervision
   about, 35
   commenting on messages, 40
   deferring process of messages, 40
   hierarchical review, 36
   history, 40
   ignoring messages, 40
   interface, 38
   issue investigation and management, 41
   message list display, 39
   review queue, 35
   standard review, 36

Copyright © MessageLabs 2009
tasks of reviewer, 37
tasks of senior reviewer, 39
tracking issues, 41
what gets reviewed, 35

U
Unreviewable Message List area, 38
user interface, 5

W
words, searching for, 14
www.messagelabs.com
info@messagelabs.com

Freephone UK
0800 917 7733

Toll free US
1-866-460-0000