Email Archiving Service Overview and Setup Guide

This guide is for the IT administrator – the person that sets up the appliance and deals with Exchange and Active Directory.

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  
   1.1 About this Guide 3  
   1.2 Intended Audience and Prerequisite Knowledge 3  
   1.3 Other Sources of Information 3  
   1.4 Contacting Support 3  

2 Introduction to MessageLabs Email Archiving Service  
   2.1 MessageLabs Email Archiving Service Overview 4  
   2.2 A Hybrid Approach to SaaS Archiving 5  
   2.3 System Requirements 6  

3 How MessageLabs Email Archiving Service Works  
   3.1 MessageLabs Email Archiving Service Uses Journaling Mailboxes 7  
   3.2 How Journaling Mailboxes Are Populated 8  
   3.3 Consequences of Using Different Methods for Populating Journaling Mailboxes 9  
   3.4 How Methods of Populating Journaling Mailboxes Work Together 9  
   3.5 How Users Interact with Archived Messages 9  

4 Network Communication and Security 11  
   4.1 About Data Encryption 11  
   4.2 Appliance Connectivity 12  
   4.3 Connecting Through a Proxy Server 12  

5 Planning For MessageLabs Email Archiving Service 13  
   5.1 Understanding Appliance Purposes 13  
   5.2 Basic Product Architecture (Single Appliance) 14  
   5.3 Using Multiple Appliances 15  
   5.4 Supporting External Access to MessageLabs Email Archiving Service 18  

6 Steps in Setting up MessageLabs Email Archiving Service 20  

7 Preparing Your System 22  
   7.1 Creating a User Account and Journaling Mailbox 22  
   7.2 Optionally, Configuring Journaling 25  
   7.3 Optionally, Creating and Configuring Managed Custom Folders 27  
   7.4 Configuring Active Directory 29  
   7.5 Creating a Test User 31  

8 Installing and Configuring Appliance 32  
   8.1 Connecting Appliance 32  
   8.2 Configuring First Appliance 33  
   8.3 Confirming Configuration 34  
   8.4 Exporting Encryption Key 35  
   8.5 Configuring Additional Appliances (If Required) 35  
   8.6 Changing Appliance Configuration 36  
   8.7 Resetting the Archiving Appliance to its Default Configuration 36
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.8</td>
<td>Temporarily Suspending Archiving from a Journaling Mailbox</td>
<td>36</td>
</tr>
<tr>
<td>9</td>
<td>Configuring External Access</td>
<td>37</td>
</tr>
<tr>
<td>9.1</td>
<td>About Configuring External Access</td>
<td>37</td>
</tr>
<tr>
<td>9.2</td>
<td>Load Balancing and Fault Tolerance on the Proxy Server</td>
<td>37</td>
</tr>
<tr>
<td>9.3</td>
<td>Installing the Archive Proxy</td>
<td>37</td>
</tr>
<tr>
<td>9.4</td>
<td>Setting up the OWA Server</td>
<td>38</td>
</tr>
<tr>
<td>10</td>
<td>Setting up User Access</td>
<td>39</td>
</tr>
<tr>
<td>10.1</td>
<td>MessageLabs Email Archiving Service Security Groups</td>
<td>39</td>
</tr>
<tr>
<td>10.2</td>
<td>Granting Access to MessageLabs Email Archiving Service</td>
<td>40</td>
</tr>
<tr>
<td>10.3</td>
<td>Granting Access to Additional Mailboxes</td>
<td>41</td>
</tr>
<tr>
<td>11</td>
<td>Giving Access to Archive from Outlook/OWA</td>
<td>42</td>
</tr>
<tr>
<td>11.1</td>
<td>Overview</td>
<td>42</td>
</tr>
<tr>
<td>11.2</td>
<td>Preconditions</td>
<td>42</td>
</tr>
<tr>
<td>11.3</td>
<td>Setting Up Accounts for Outlook Folder Creator</td>
<td>43</td>
</tr>
<tr>
<td>11.4</td>
<td>Running Outlook Folder Creator</td>
<td>45</td>
</tr>
<tr>
<td>11.5</td>
<td>Scheduling Outlook Folder Creation</td>
<td>46</td>
</tr>
<tr>
<td>12</td>
<td>Setting Up Stubbing</td>
<td>47</td>
</tr>
<tr>
<td>12.1</td>
<td>About Stubbing</td>
<td>47</td>
</tr>
<tr>
<td>12.2</td>
<td>About the Stubbing Process</td>
<td>47</td>
</tr>
<tr>
<td>12.3</td>
<td>About the Stubbing Account and Form</td>
<td>48</td>
</tr>
<tr>
<td>12.4</td>
<td>About Stubbing Policies</td>
<td>48</td>
</tr>
<tr>
<td>12.5</td>
<td>Overview of Stubbing Configuration Steps</td>
<td>49</td>
</tr>
<tr>
<td>12.6</td>
<td>Creating User Account for Stubbing</td>
<td>49</td>
</tr>
<tr>
<td>12.7</td>
<td>Creating Organizational Forms Library</td>
<td>50</td>
</tr>
<tr>
<td>12.8</td>
<td>Publishing Stubbing Forms</td>
<td>52</td>
</tr>
<tr>
<td>12.9</td>
<td>Configuring the Appliance for Stubbing</td>
<td>53</td>
</tr>
<tr>
<td>12.10</td>
<td>Working with the Stubbing Policy</td>
<td>53</td>
</tr>
<tr>
<td>12.11</td>
<td>Enabling or Disabling Stubbing</td>
<td>56</td>
</tr>
<tr>
<td>13</td>
<td>Troubleshooting MessageLabs Email Archiving Service</td>
<td>57</td>
</tr>
<tr>
<td>13.1</td>
<td>Using the Audit Trail to View Login Activity</td>
<td>57</td>
</tr>
<tr>
<td>13.2</td>
<td>Solving Common Problems</td>
<td>57</td>
</tr>
<tr>
<td>13.3</td>
<td>Troubleshooting User Directory Issues</td>
<td>58</td>
</tr>
<tr>
<td>13.4</td>
<td>Troubleshooting Archiving Issues</td>
<td>61</td>
</tr>
<tr>
<td>14</td>
<td>Glossary</td>
<td>62</td>
</tr>
<tr>
<td>15</td>
<td>Index</td>
<td>63</td>
</tr>
</tbody>
</table>
1 Preface

1.1 About this Guide

This guide introduces MessageLabs Email Archiving Service, provides useful background information about it and explains how to set it up.

1.2 Intended Audience and Prerequisite Knowledge

This guide is intended for use by IT staff who manage the Exchange Server environment and will be responsible for setting up and maintaining MessageLabs Email Archiving Service.

1.3 Other Sources of Information

This guide covers procedural information for MessageLabs Email Archiving Service setup and configuration. For other information, see:

**Online Help:** Every screen in the 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.

**Policy Creation and Management:** Explains how to set up your organization’s electronic messaging policy. Intended for users responsible for policy management, such as compliance and records management staff.

**Legal Discovery and Supervision:** Explains how to search the archive using the MessageLabs Email Archiving Service web interface. Also explains how to carry out discovery and supervision activities.

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

**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 to MessageLabs Email Archiving Service

Chapter Overview

This chapter provides background information about MessageLabs Email Archiving Service. It includes the following topics:

- MessageLabs Email Archiving Service Overview
- A Hybrid Approach to SaaS Archiving
- System Requirements

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 A Hybrid Approach to SaaS Archiving

MessageLabs Email Archiving Service represents a new approach to outsourcing: the hybrid solution. It provides an integrated archiving solution with robust search and discovery, supervision and enforcement features.
2.2.1 The Archiving Appliance

The Archiving Appliance is a sealed fixed-purpose server (in standard 1U rack mount form) that is installed within your corporate network behind your firewall, to provide the tight integration and security typically only afforded to internal systems.

The appliance provides integrates with Microsoft Exchange to ensure reliable, native format message archiving. Its integration with Active Directory facilitates unified login and access control management.

Since the appliance is the only holder of your encryption keys (for more information, see “About Data Encryption” on page 11), any processing that involves encryption or decryption happens on the appliance.

2.2.2 The MessageLabs Network

This highly secure, reliable and scalable infrastructure is based on a distributed search and storage architecture. This is where your data resides, in encrypted format. The vast majority of search processing and all of the storage is maintained on the MessageLabs Network, reducing overhead and maintenance headaches.

The archive securely stores your electronic messages and is accessible either through the web interface, or, for end-user searching functions, through Outlook/OWA.

2.3 System Requirements

The appliance must be connected as described in “Appliance Connectivity” on page 12.

For users who will access the user interface, a Windows PC with Internet Explorer version 6 or higher is needed. Internet Explorer must be configured to allow JavaScript and popups.

**Note:** Limited search functionality is available for users using Firefox.

Microsoft Exchange must be installed, with the following versions and service packs supported:


**Note:** External access, including OWA access, is available for Exchange 2003 and 2007 only.

Exchange custom managed folders and organization-wide journaling (Hub Transport) require Enterprise CALs for Exchange 2007.
3  How MessageLabs Email Archiving Service Works

Chapter Overview

This chapter explains the details of how MessageLabs Email Archiving Service works to solve different business challenges. It includes the following topics:

- MessageLabs Email Archiving Service Uses Journaling Mailboxes
- How Journaling Mailboxes Are Populated
- Consequences of Using Different Methods for Populating Journaling Mailboxes
- How Users Interact with Archived Messages

3.1  MessageLabs Email Archiving Service Uses Journaling Mailboxes

To populate the archive, the Archiving Appliance retrieves messages from specific mailboxes on your Exchange Server: these are called journaling mailboxes. It copies groups of messages into a “batch” subfolder of the journaling mailbox, then retrieves the messages, encrypts them and sends them to the archive. When the appliance receives confirmation from the archive that the batch of messages has been fully archived, it deletes the batch subfolder from the journaling mailbox. This “pull and confirm” process ensures that no information is lost, even in the event of a network or appliance failure.
3.2 How Journaling Mailboxes Are Populated

3.2.1 Populating Journaling Mailboxes Using Microsoft Exchange Journaling

This method is useful for legal discovery and compliance needs: all messages are captured, regardless of user action.

Exchange journaling (available for Exchange 2000, 2003 or 2007) places a copy of each message that is sent or received into a journaling mailbox. In Exchange 2000/2003, message journaling is enabled for a mailbox store (a database used to organize multiple mailboxes). In Exchange 2007, message journaling can be enabled either for individual mailbox databases (each of which contains multiple mailboxes) or for the entire organization.

3.2.2 Populating Journaling Mailboxes Using Exchange Managed Folders

This method is useful for record management purposes. Users identify different classes of critical business messages that should be archived.

Microsoft Exchange 2007 allows administrators to deploy a special set of managed folders to the Outlook or OWA interface for end users. These folders facilitate consistent organization of information across user mailboxes. Users choose, either manually or via rules, messages to place in these folders. Folders can be configured to place messages in a journaling mailbox.

3.2.3 Populating Journaling Mailboxes Using MessageLabs Email Archiving Service Stubbing

This method is useful to optimize storage, reducing the storage needs of the Exchange system.

Stubbing is an optional background process that replaces email attachments (which are stored in Exchange) with a much smaller “stub” that points to a copy of the attachment that is stored in the archive. Sometimes the original attachment cannot be located — for example, it may pre-date journaling, have changed since journaling began, or be in a mailbox that does not use journaling. In that case, MessageLabs Email Archiving Service can place a copy of the attachment in the journaling mailbox so it can be archived. The original attachment can then be stubbed. Special retention policies can be defined for stored attachments.

3.2.4 Importing Messages into the Archive

MessageLabs Email Archiving Service can import legacy messages and attachments from a variety of sources directly into the archive.
3.3 Consequences of Using Different Methods for Populating Journaling Mailboxes

<table>
<thead>
<tr>
<th></th>
<th>Journaling</th>
<th>Managed Folders</th>
<th>Stubbing Attachment Capture</th>
<th>Import</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>What is archived?</strong></td>
<td>All messages sent or received from point of implementation onward</td>
<td>All messages users place into a managed folder, from point of implementation onward</td>
<td>Attachments to messages not already archived</td>
<td>Any imported messages</td>
</tr>
<tr>
<td><strong>What can be stubbed?</strong></td>
<td>Only messages sent or received from point of implementation onward</td>
<td>Not applicable</td>
<td>Any messages (including historical mail)</td>
<td>Any imported messages</td>
</tr>
</tbody>
</table>

3.4 How Methods of Populating Journaling Mailboxes Work Together

Different methods of populating journaling mailboxes can work in combination with each other to meet specific business requirements.

For example, to archive both existing mail from user mailboxes and any new messages sent/received, use the import service plus Exchange journaling. Once messages have been imported, you can optionally enable stubbing, which will then be able to process all attachments.

Another common use is to archive all messages for a short period of time while allowing end users to identify business records that should be retained for longer periods. This requires using both Exchange journaling and managed folders.

3.5 How Users Interact with Archived Messages

3.5.1 Searching for Messages

MessageLabs Email Archiving Service provides powerful search functionality that allows users to find messages in the archive. Users use search criteria, such as a word or phrase contained in the message, to find relevant messages. Messages found through a search can be retrieved into the user’s mailbox for forwarding or other purposes.

3.5.2 Exporting Messages to PST

Messages found through searching can be exported to an Outlook Personal Folder file (PST). All of the richness of the original message is maintained because the data remains in email format. The PST files can be shared with an outside legal team or regulators.

3.5.3 Creating and Managing Legal Holds

It is sometimes necessary to retain a specific set of messages beyond their original retention period, usually for legal matters. Authorized users can copy such messages from the archive into a specific container, called a legal hold, ensuring that messages remain intact while the normal archive operations continue. Once the matter is closed, the legal hold can be removed and its contents disposed of.
3.5.4 Reviewing Messages for Compliance (Supervision)

Supervision functions allow your company to designate individuals who can review messages of other users. Messages can be evaluated for a variety of purposes, including compliance with regulations and conformance to industry standards. MessageLabs Email Archiving Service identifies messages that may not be in compliance with policies and practices. It can also perform a random selection of messages. Both identified and randomly selected messages are placed in a review queue for evaluation by authorized reviewers.

3.5.5 Accessing Stubbed Attachments

Attachments to messages are replaced with a “stub” The message appears unchanged to the user, except that the stubbed attachment appears as an HTM file instead of the original attachment format (such as PDF). This allows the original attachment to be retrieved, if necessary, from the archive rather than from Exchange.
4 Network Communication and Security

Chapter Overview

This chapter explains communication and security requirements for MessageLabs Email Archiving Service. It includes the following topics:

- About Data Encryption
- Appliance Connectivity
- Connecting Through a Proxy Server

4.1 About Data Encryption

During archiving, all of your data is encrypted using encryption keys unique to you. A proprietary approach to working with your data ensures maximum security and privacy. In this approach, your Archiving Appliance stores your encryption keys, but does not have the ability to read your data. As a result, your data can never be viewed without access to both your appliance (which resides within your network) and the MessageLabs Network.

As the MessageLabs Network will only accept requests from IP addresses tied to the appropriate Archiving Appliance, even theft of your appliance doesn’t compromise the security of your data.

Since all data within the MessageLabs Network is encrypted using your key, even if intruders penetrated MessageLabs’ heavily secured infrastructure, they would only see meaningless encrypted data. Certified duplicate copies of your data are maintained in separate data centers to further guard against modifications.
4.2 Appliance Connectivity

4.2.1 Network Requirements

The appliance requires outbound Internet connectivity with a static IP address that is accessible internally. The appliance needs to connect to the Internet, but the MessageLabs Network does not need to connect to the appliance.

4.2.2 Connectivity Options

The appliance talks to the MessageLabs Network through one of several connectivity options, including:

- HTTPS port 443
- HTTPS port 443 with a router or firewall-based access control list (see below).

4.2.3 Router or Firewall Configuration (optional)

For maximum security, MessageLabs highly recommends that you configure your router or firewall with access control lists that prevent the Archiving Appliance from communicating with anything other than the MessageLabs Network. See the documentation for your router or firewall for instructions on setting up access control lists. Your rules should be configured as follows:

<table>
<thead>
<tr>
<th>Source</th>
<th>IP address of the Archiving Appliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>Contact MessageLabs Professional Services to get the list of destination IP addresses for the data center that services your account.</td>
</tr>
<tr>
<td>Port</td>
<td>443</td>
</tr>
</tbody>
</table>

4.3 Connecting Through a Proxy Server

The appliance can connect to the MessageLabs Network through your corporate proxy server. However, this is not recommended, since performance may be affected.
5 Planning For MessageLabs Email Archiving Service

Chapter Overview

This chapter outlines considerations to be taken into account when preparing to implement MessageLabs Email Archiving Service. It includes the following topics:

- Understanding Appliance Purposes
- Basic Product Architecture (Single Appliance)
- Using Multiple Appliances
- Supporting External Access to MessageLabs Email Archiving Service

5.1 Understanding Appliance Purposes

Some environments may benefit from using multiple appliances. Each appliance can serve one or more of the following purposes:

- archiving messages
- serving the user interface
- exporting messages
- stubbing attachments.

In a single-appliance environment, one appliance fulfills all these purposes. In a multi-appliance environment, purposes can be split across the available appliances. Each purpose must be assigned to at least one Archiving Appliance, and all purposes must be performed at each separate location.

When choosing how to distribute purposes across appliances, keep in mind that archiving, exporting and stubbing are background batch processes, so it is acceptable that they build a backlog periodically. Search and other user interface tasks are interactive, requiring immediate responsiveness, so you may want to isolate them from batch processing.
5.2 Basic Product Architecture (Single Appliance)

Although additional Archiving Appliances may be necessary for a high volume of data or geographically-separated local area networks, the basic concepts of the architecture that must be understood before expanding to multiple appliances.

A single Archiving Appliance at a location with one Exchange Server

The basic installation, which is appropriate for a small to medium-sized company, consists of a single appliance that archives messages from a single Exchange Server. The above figure illustrates this arrangement.

While this is the simplest configuration, it illustrates a key concept. The appliance must connect to the Exchange Server and Active Directory locally, not over a wide area network connection. If you have multiple locations with their own Exchange Servers, you will need at least one appliance at each location.
5.3 Using Multiple Appliances

The basic configuration described above suits most purposes. However, other options might be needed for environments with a high volume of data or geographically-separated local area networks.

Note: Since configuration data is stored centrally, multiple appliances automatically synchronize their configuration.

5.3.1 Multiple Appliances in a Single Location with a Single Exchange Server

Four Archiving Appliances at a single location

The above figure illustrates a situation where the volume of email traffic or search usage patterns requires extra processing power, which is achieved by assigning specific purposes to separate appliances (see “Understanding Appliance Purposes” on page 13).

Note: Your company’s encryption key is generated during the configuration of your first appliance. All other appliances must be configured with the same encryption key.
5.3.2 Multiple Exchange Servers and Archiving Appliances at a Single Location

You are not restricted to just one journaling mailbox (or Exchange Server) when configuring appliances. The following figures are representative of cases where there are multiple appliances and multiple journaling mailboxes. To simplify the diagrams, only two appliances and two Exchange Servers (each with one journaling mailbox) appear, but in practice there could be more of each. Also, the single appliances shown in the figures could easily be expanded to multiple appliances with specific purposes, as was shown in the previous example.

In the case shown above, each Archiving Appliance archives messages from a single journaling mailbox and stubs attachments from a single Exchange Server. This arrangement is satisfactory when both Exchange Servers are equally busy, with relatively little fluctuation in their loads.

When issues of load balancing arise, another configuration (shown above) is possible. Load balancing can be achieved by connecting both appliances to the journaling mailboxes on both servers. (In this scenario, both appliances can also be configured to stub attachments in both Exchange Servers: stubbing is explained in “Setting Up Stubbing” on page 47.)
5.3.3 Multiple Exchange Servers and Archiving Appliances at Multiple Locations

If you have multiple office locations (sites), each with their own Exchange environment, you will need multiple appliances.

Multiple locations

Each location can be modeled on any of the previous shown examples. All locations in a site store messages in a single archive, providing unified enterprise searching for legal discovery purposes. You can balance loads by adjusting the number of appliances at each location and assigning specific purposes to them, remember that the appliances at each location must provide complete coverage for all the Archiving Appliance purposes: see “Understanding Appliance Purposes” on page 13.
5.4 Supporting External Access to MessageLabs Email Archiving Service

5.4.1 Considerations for External Access

MessageLabs Email Archiving Service supports external access for users wanting to search the archive and/or retrieve stubbed attachments from outside the corporate network. Access may be through the web interface, Outlook or OWA. For security reasons, the Archiving Appliance should never be placed outside your firewall, so this access is handled through an HTTP proxy (strictly speaking, this is a "reverse proxy"). Access is provided via the OWA server, since it already has a connection to the internal network and the public Internet.

**Note:** If your environment contains more than one OWA server that resides behind a load balancer, the proxy needs to be installed on each of those servers. Consult with MessageLabs professional services before proceeding.

This section describes several alternative configurations for external access, using the proxy provided by MessageLabs. The MessageLabs Email Archiving Service proxy installs on your OWA server, allowing it to use the same DNS entry and digital certificate as that server. It can load-balance requests between any number of appliances at a location. The exception to this load balancing is the MessageLabs supervision process, which caches, on an appliance, the messages to be reviewed. As a result, a reviewer’s session will be locked to the first appliance they connect to.

For stubbing, the proxy provides the publicly available URL that allows original attachments to be retrieved, via an appliance, from the Archive where they exist.

5.4.2 Using a Single Exchange Server Running OWA

In the configuration illustrated below, a single Exchange Server runs OWA. Users access OWA by connecting directly to the Exchange Server, which is where the MessageLabs Email Archiving Service proxy will be installed.

![Single Exchange Server Running Outlook Web Access (OWA)]
5.4.3 Front End Exchange Server Running OWA

In the configuration illustrated below, two Exchange Servers are used:

- A front end Exchange Server, residing between two firewalls, is used for external access.
- A back end Exchange Server, behind a firewall, is used for internal access.

Typically the front end Exchange Server acts as the SMTP mail gateway and does not hold any mailbox databases: these are on the back end Exchange Server, which is also where journaling takes place. The MessageLabs Email Archiving Service proxy is installed on the front end Exchange Server. This configuration provides greater security.

If your environment contains more than one OWA server which resides behind a load balancer, the proxy needs to be installed on each of those servers.
Steps in Setting up MessageLabs Email Archiving Service

Before you begin, choose your architecture, taking into account your business needs (several example architectures are explained in the previous chapter). Be sure your network connectivity has been set up correctly (see "Appliance Connectivity" on page 12).

Phase 1 of setting up MessageLabs Email Archiving Service involves setting up a single Archiving Appliance, creating a test user and giving that user access to MessageLabs Email Archiving Service. This lets you confirm everything is working correctly before adding more users.

<table>
<thead>
<tr>
<th>What To Do</th>
<th>For More Details, See…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create journaling mailbox(es). This is necessary</td>
<td>Creating a User Account and Journaling Mailbox on page 22</td>
</tr>
<tr>
<td>regardless of how the mailboxes will be populated.</td>
<td></td>
</tr>
<tr>
<td>Optionally, configure journaling in Exchange.</td>
<td>Optionally, Configuring Journaling on page 25</td>
</tr>
<tr>
<td>This should be done a few days prior to the appliance</td>
<td></td>
</tr>
<tr>
<td>being installed so some messages are ready forarchiving.</td>
<td></td>
</tr>
<tr>
<td>Optionally, create managed folders.</td>
<td>Optionally, Creating and Configuring Managed Custom Folders on page 27</td>
</tr>
<tr>
<td>Configure Active Directory and set up a test user to</td>
<td>Configuring Active Directory on page 29</td>
</tr>
<tr>
<td>be used when confirming that archiving is operating</td>
<td>Creating a Test Directory on page 31</td>
</tr>
<tr>
<td>correctly.</td>
<td></td>
</tr>
<tr>
<td>Install and configure the first appliance.</td>
<td>Installing and Configuring Appliance on page 32</td>
</tr>
<tr>
<td>Confirm that archiving is operating correctly.</td>
<td>Confirming Configuration on page 34</td>
</tr>
<tr>
<td>Set up user groups.</td>
<td>Policy Creation and Management</td>
</tr>
<tr>
<td>Create your electronic messaging policy.</td>
<td>Policy Creation and Management</td>
</tr>
</tbody>
</table>

Phase 2 involves making MessageLabs Email Archiving Service functions available to users.

<table>
<thead>
<tr>
<th>What To Do</th>
<th>For More Details, See…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optionally, set up remote access.</td>
<td>Configuring External Access on page 37</td>
</tr>
<tr>
<td>Optionally, set up DNS entry for appliance.</td>
<td>Although users can access MessageLabs Email Archiving Service by typing the IP address of the appliance in their browser’s address bar, it is easier for them if you create a DNS entry for the appliance.</td>
</tr>
<tr>
<td>Give users access to MessageLabs Email Archiving Service functions.</td>
<td>Setting up User Access starting on page 39</td>
</tr>
<tr>
<td></td>
<td>Supporting External Access to MessageLabs Email Archiving Service on page 18</td>
</tr>
</tbody>
</table>
Phase 3 is necessary only if you are using optional functions or multiple Archiving Appliances.

<table>
<thead>
<tr>
<th><strong>What To Do</strong></th>
<th><strong>For More Details, See...</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>If using multiple appliances, install them.</td>
<td>Connecting Appliance on page 32</td>
</tr>
<tr>
<td>Configure the additional appliances and, optionally, change the configuration of the first one.</td>
<td>Configuring Additional Appliances on page 35</td>
</tr>
<tr>
<td>If using the optional Stubbing function, configure it.</td>
<td>Setting Up Stubbing on page 47.</td>
</tr>
<tr>
<td>If using the optional Supervision function, configure supervision review.</td>
<td>Legal Discovery and Supervision</td>
</tr>
</tbody>
</table>
7 Preparing Your System

Chapter Overview

This chapter explains the steps necessary to prepare for MessageLabs Email Archiving Service installation and configuration. It includes the following topics:

- Creating a User Account and Journaling Mailbox
- Optionally, Configuring Journaling
- Optionally, Creating and Configuring Managed Custom Folders
- Configuring Active Directory
- Creating a Test User

7.1 Creating a User Account and Journaling Mailbox

You need to create a new user account and a mailbox to be used as the journaling mailbox. If you have separate Exchange Servers, you may need a separate user account/mailbox per storage group and/or Exchange Server.

*Note:* The journal account should not have any size restrictions applied to it. In addition, no Exchange Server rules should be applied to the account, especially rules that might move or delete messages from the account or move them to another folder such as “Junk Mail”.

Copyright © MessageLabs 2009
7.1.1 Creating a User Account and Journaling Mailbox on Exchange 2000/2003

To create a new user account and journaling mailbox:

2. Connect to the domain in which you want to create the user.
3. Right-click the organizational unit in which you want to create the user and choose New, then User.
4. Enter a full name and user login name. For example, MessageLabs Email Archiving Service or, in the case of multiple journaling mailboxes, MessageLabs Email Archiving Service_nn, where nn is a sequence number for the journaling mailbox.
5. Click Next and enter and verify a password. Set the username must change password, user cannot change password and password never expires options in accordance with your company’s policies.
   Record the login name and password: you will need them when you configure the Archiving Appliance.
6. Click Next and ensure that the Create an Exchange e-mail address check box is checked.
7. Click Next, then Finish. The user account and mailbox are created.
8. Right-click on the new user and choose Properties.
10. Click Add and enter the name of the new user.
   Note: The journaling mailbox must be configured to only receive mail from itself.
11. Click Check Names, then OK, twice.
12. Log in to the new account using OWA so Exchange will initialize the mailbox.

Note: If you allow the password to expire, you must change it manually and reconfigure the appliance each time it changes.
7.1.2 Creating a New User Account and Journaling Mailbox for Exchange 2007

To create a new user account and journaling mailbox:

1. On your primary Exchange Server, open the Exchange Management Console.
2. In the tree, expand **Recipient Configuration**.
3. Right-click on **MailBox** and choose **New Mailbox**.
4. Select **User Mailbox** and click **Next**.
5. Select **New User** and click **Next**.
6. Choose the **Organizational Unit** in which you want to create the account.
7. Enter the full user name and a user login name. For example, **MessageLabs Email Archiving Service**.
8. Enter and verify a password. Set the **username must change password, user cannot change password** and **password never expires** options in accordance with your company’s policies.
9. Record the login name and password: you will need them when you configure the Archiving Appliance.
10. If you allow the password to expire, you must change it manually and reconfigure the appliance each time it changes.
11. Click **Next**. For **Mailbox Settings**, leave the **Alias** at its default, ensure the correct **Server**, **Storage Group** and **Mailbox database** are selected.
12. Click **Next**. Confirm the configuration summary settings are correct.
13. Click **New**. Exchange System Manager will attempt to create the user account and mailbox.
14. Once the wizard has completed successfully, click **Finish**.
15. In the tree, click **Mailbox**. A list of mailboxes will be displayed.
16. Right-click on the mailbox and choose **Properties**.
17. On the Mail Flow Settings tab, select **Message Delivery Restrictions**.
18. Click **Properties**.
19. For **Accept message from**, select **Only senders in the following list** and click **Add**.
20. Select the mailbox created earlier.
21. For **Reject message from**, ensure **No senders** is selected.
22. Click **OK**, twice.
23. Log in to the new account using OWA so Exchange will initialize the mailbox.
7.2 Optionally, Configuring Journaling

This step is not necessary if MessageLabs Email Archiving Service is being used just for stubbing, or for managed folders without use of Exchange journaling.

*Note:* If it is to be used, journaling should be configured about one or two days before the appliance is installed, so that some messages are ready for archiving.

7.2.1 Understanding Exchange Journaling

7.2.1.1 Exchange 2000/2003

In Microsoft Exchange 2000/2003, message journaling needs to be enabled for a mailbox store (a database used to organize multiple mailboxes). The contents of an entire store are archived, so if you want to archive only a subset of mailboxes, move them to a separate store for which journaling can be enabled. Of the three types of journaling that can be enabled, MessageLabs Email Archiving Service uses Bcc journaling.

7.2.1.2 Exchange 2007

In Microsoft Exchange 2007, message journaling can be enabled either for individual mailbox databases (each of which contains multiple mailboxes) or for the entire organization.

The contents of an entire database are archived, so if you want to archive only a subset of mailboxes, move them to a separate database for which journaling can be enabled.

If you choose to enable journaling for the entire organization, you use a Journal Agent on the Hub Transport server, through which all messages pass, to specify the location of the organization’s journaling mailbox. Mailboxes can be identified through a filter based on security group name.

7.2.2 Configuring Exchange Journaling (Exchange 2000/2003)

MessageLabs Email Archiving Service uses the Bcc journaling feature in Exchange to copy all the messages to the journaling mailbox. Before you enable Bcc journaling, you must enable standard journaling on each mailbox store in your organization for which you want Bcc journaling enabled. Enable journaling only on those mailbox stores that you want to archive.

Bcc journaling is standard journaling with the added ability to capture Bcc recipients, so standard journaling needs to be enabled first. Once Bcc journaling is enabled, Exchange captures all recipients (including Bcc recipients) that are known at the originating server. In order to enable Bcc journaling, you must set a registry key.

*To enable standard journaling:*

1. On the Exchange Server that has the mailboxes that you want to archive, open Exchange System Manager.
2. Expand *Servers*, expand `<your Exchange Server>`, then expand `<storage group>`.
3. Right-click the mailbox store and choose *Properties*.
4. On the General tab, select *Archive all messages sent or received by mailboxes on this store* and then click *Browse* to specify a mailbox as the journaling mailbox.
5. Select the journaling mailbox (as set up above, for example: `messagelabs@yourdomainname.com`).

All journaled messages for senders on this mailbox store will now be sent to the specified mailbox.
To enable Bcc journaling:

**Note:** Failure to enable Bcc journaling will result in messages being archived without the Bcc recipient information.

6 On the Exchange Server that has the mailboxes you want to archive, open Regedit.

7 Add the **Parameters** key (if it doesn’t already exist) in the following location: 
   `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeTransport\Parameters`

8 Add the following registry value within the **Parameters** key:
   - Value name: `JournalBCC`
   - Data type: **Dword**
   - Data value: 1

**Note:** The information about setting the registry key is contained in the Microsoft® Knowledge Base article 810999, “XADM: Bcc Information Is Lost for Journaled Messages in Exchange 2000.”
   [http://go.microsoft.com/fwlink/?LinkId=3052&kbid=810999](http://go.microsoft.com/fwlink/?LinkId=3052&kbid=810999)

9 Once the additional registry key and value are added, restart the SMTP service and the Microsoft Exchange Information Store service so that the changes will be recognized.

**Note:** For more information on the journaling feature, see the following Microsoft reference article

### 7.2.3 Configuring Exchange Journaling (Exchange 2007)

You can choose one of the following options:

- Configure your mailbox databases to point to the journaling mailbox you created. Enabling journaling for individual mailbox databases requires you to configure the mailbox databases to point to the corresponding journaling mailbox.
- Enable journaling for the entire enterprise by creating a journaling rule to send messages from the Hub Transport Server to this journaling mailbox.

**Note:** Hub Transport-level journaling is only supported in the Enterprise version of Exchange 2007.

**To configure journaling for individual mailbox databases:**

1 In the Exchange Management Console, expand **Server Configuration**, then click **Mailbox**.

2 Right-click the mailbox database and choose **Properties**.
   The Mailbox Database Properties screen appears.

3 On the General tab, enable the **Journal Recipient** checkbox.

4 Click **Browse** and choose the mailbox created in the previous procedure, then click **OK**.
   All journaled messages for senders in this mailbox database will now be sent to the specified mailbox. Repeat these steps for each mailbox database to be journaled.
To configure journaling for the entire enterprise:

**Note:** You can set up rules to only journal messages for specific mailboxes, if desired. Hub Transport-level journaling is only supported in the Enterprise version of Exchange 2007.

1. In the Exchange Management Console, expand *Organization Configuration*, then click *Hub Transport*.
2. In the Toolbox Actions pane, click *New Journaling Rule*.
   
   The New Journaling Rule screen appears.
3. Enter a name for the journaling rule in the *Rule name* field.
4. Click *Browse* in the Journal e-mail address area and choose the mailbox created in the previous procedure.
5. Click *OK*. Make sure the *Global* option (in the Scope area) is enabled.
6. Click *New*, then *Finish*.

7.3 Optionally, Creating and Configuring Managed Custom Folders

For an explanation of managed folders, see “Populating Journaling Mailboxes Using Exchange Managed Folders” on page 8. This feature is available only in Exchange 2007.

Creating and configured managed custom folders involves the following steps:

- Step 1: Create managed custom folders.
- Step 2: Configure managed folders.
- Step 3: Create managed folder mailbox policies that will be used to deploy managed folders to users. A single policy can deploy multiple folders.

**Note:** This policy should not be confused with MessageLabs Email Archiving policies: the managed folder mailbox policy is used to link managed folders to a user’s mailbox.

- Step 4: Apply managed folder mailbox policies to user mailboxes.
- Step 5: Schedule the Managed Folder Assistant, which creates managed folders and enforces content settings for existing ones.

You can choose whether to use managed folders on their own or as part of journaling. Using them with journaling allows users to “re-archive” a copy of key items that need to be kept longer than normal.
To create a managed custom folder:
1. On your primary Exchange Server, open the Exchange Management Console.
2. Expand Organization Configuration.
3. Right-click on MailBox and choose New managed Custom Folder.
   The New Managed Custom Folder screen appears.
4. Enter an internal name (seen within the Exchange Management Console or Exchange Management Shell) in the Name field.
5. Enter a display name (seen within Outlook or OWA) in the Display the following name field.
6. Optionally, specify a storage limit for the folder.
7. Optionally, add an explanatory comment to be displayed to users and choose whether or not users can minimize the comment.
8. Click New.
   The Completion screen appears.
9. Click OK.

To configure managed content settings:
1. On your primary Exchange Server, open the Exchange Management Console.
2. Expand Organization Configuration and click Mailbox.
3. Open the Managed Custom Folders tab.
   A list of the existing managed folders of the appropriate type appears.
4. Right-click on a managed folder and choose New managed Content Settings.
   The New Managed Content Settings screen appears.
5. Enter a descriptive name (seen within the Exchange Management Console or Exchange Management Shell) in the Name of the managed content settings field.
6. Choose from the Message type list the type of items to be included as managed content. The list includes specific items (tasks, notes, voicemail, etc.) as well as an All Mailbox Content choice.
7. Optionally, specify how long messages in the managed content folder should be retained and when the retention period begins (for example, "when delivered").

**Note:** Unlike MessageLabs Email Archiving retention periods, which determine how long a message must be kept, the managed folders retention period simply determines an action to take once that period has elapsed. Managed folders are swept nightly for items that have reached their retention limit. Messages can be deleted from a managed folder at any time, even before the retention period has elapsed.

8. Specify what to do once a message has reached the retention period (for example, move the items to a specific managed custom folder). A nightly process assesses each message and applies this action as necessary.
   **Note:** This retention period is not related to the MessageLabs Email Archiving retention period.
9. Click Next.
   The Journaling screen appears.
10. Enter the email address assigned to the journaling mailbox.
11. Click Next, then OK.
To create managed folder mailbox policies:
1. On your primary Exchange Server, open the Exchange Management Console.
2. Expand Organization Configuration and click Mailbox.
3. Right-click the Mailbox object and choose New Managed Folder Mailbox Policy. A New Managed Folder Mailbox Policy wizard appears.
4. Enter a name for the policy.
5. Add managed folders to the policy by clicking Add, choosing from the available folders and click OK.
7. Click Finish.

To apply managed folder mailbox policies to user mailboxes:
1. On your primary Exchange Server, open the Exchange Management Console.
2. Expand Recipient Configuration and click Mailbox.
3. Right-click on the user mailbox you want to apply a managed folder mailbox policy to and choose Properties.
4. Click the Mailbox Settings tab.
6. Select the policy to be applied to the user mailbox. Click OK until you return to the main EMC window.

To schedule the Managed Folder Assistant:
1. On your primary Exchange Server, open the Exchange Management Console.
2. Expand Server Configuration and click Mailbox.
3. Right-click on the appropriate mailbox server and choose Properties. The server properties screen appears.
4. Click the Messaging Records Management tab.
5. Click Customize and schedule the managed folder assistant as you would other scheduled functions.

7.4 Configuring Active Directory

Configuring Active Directory involves:

- Setting up the account assigned to the Archiving Appliance.
- Setting up security groups for MessageLabs Email Archiving Service.

7.4.1 Setting up Account Assigned to the Archiving Appliance

The appliance needs an account that can access a local Domain Controller. In most cases, this will be one of the user accounts associated with a journaling mailbox.

To ensure that the appliance can see all of the mailboxes that Exchange can see, this account must be added to the Exchange Domain Servers group (for Exchange 2000/2003) or the Exchange Servers group (for Exchange 2007), as described below.
To add the account to the appropriate Exchange Servers group:

1. Open the Active Directory Users and Computers MMC snap-in.
   The Microsoft Management Console opens for configuration of Active Directory Users.

2. On the Action menu, click Find.
   The Find Users, Contacts and Groups screen appears.

3. In the Name field, enter the name of the account that the appliance should use to connect to AD and click Find Now, then double-click on the appropriate account.
   The User Properties screen appears.

4. Click the Member Of tab, then click Add.
   The Select Groups screen appears.

5. For Exchange 2000/2003, enter Exchange Domain Servers then click Check Name.
   For Exchange 2007, enter Exchange Servers, found within “Microsoft Exchange Security Groups”.
   The group name is added to the list.

6. Click OK, twice.
7.4.2 Setting Up MessageLabs Email Archiving Service Security Groups in Active Directory

Users must be part of at least one of the MessageLabs Email Archiving Service security groups to gain access to the user interface, whether through the browser or through Outlook/OWA.

Users log in to the MessageLabs Email Archiving Service user interface using their standard Windows user name and password. During the authentication process, the appliance checks to see if the user is a member of one of the predefined Active Directory security groups. The security groups users belong to determine what functions they have access to.

All MessageLabs Email Archiving Service security groups must be created, whether or not they will actually be used.

To set up MessageLabs Email Archiving Service-specific Active Directory security groups:
1. Open the Active Directory Users and Computers MMC snap-in.
   The Microsoft Management Console opens for configuration of Active Directory Users.
2. Connect to the domain in which you want to create the groups.
3. Right-click on the domain and choose New, then Group.
4. In the Group Name field, enter the group name (see list of required group names below).
5. If your company has multiple domains, set the Group Scope to Universal, otherwise set the Group Scope to Global.
6. Set the Group Type to Security.
7. Click Next and ensure that the Create an Exchange Email Address option is not selected.
8. Click Next, then Finish.
9. Repeat for each of the following Active Directory security groups, whether or not all groups will actually be used:
   - MessageLabs Policy Managers
   - MessageLabs Archive Export Users
   - MessageLabs User Managers
   - MessageLabs Archive Report Users
   - MessageLabs Archive Search Users
   - MessageLabs Archive Discovery Users
   - MessageLabs Archive Discovery Administrators
   - MessageLabs Archive Disposition Users
   - MessageLabs Supervision Reviewers
   - MessageLabs Supervision Senior Reviewers
   - MessageLabs Supervision Report Users

7.5 Creating a Test User

For testing purposes, create a user who is a member of all of the MessageLabs Email Archiving Service security groups you just created. In order to test configuration, the test user should be able to send and/or receive email messages.
8 Installing and Configuring Appliance

Chapter Overview

This chapter explains how to install and configure Archiving Appliances. It includes the following topics:

- Connecting Appliance
- Configuring First Appliance
- Confirming Configuration
- Exporting Encryption Key
- Configuring Additional Appliances (If Required)
- Changing Appliance Configuration
- Resetting the Archiving Appliance to its Default Configuration
- Temporarily Suspending Archiving from a Journaling Mailbox

8.1 Connecting Appliance

You will need:

- access to electrical power
- access to network jack
- monitor (with a resolution of 1024 x 768)
- keyboard
- mouse.

**Note:** The monitor, keyboard and mouse can be removed when the appliance has been configured. They are needed only for access to the configuration interface.

**To connect the Archiving Appliance:**

1. Connect the power cord to an outlet.
2. Attach the appliance to an active network jack.
   The network cable plugs into the LAN 1 port on the rear of the appliance.
3. Connect the monitor, keyboard and mouse.
4. Ensure that the appliance is powered on and is showing the logon window.
8.2 Configuring First Appliance

Even if you plan to use multiple appliances, you should configure the first one and confirm archiving is operating properly before setting up the other appliances.

To configure the first Archiving Appliance:

1. Log on to the appliance, entering `config` as the user name and `P@ssw0rd` as the password. Agree to the license agreement that appears.

   The Network Configuration screen appears.

2. Configure network connection settings: enter the **IP Address**, **Subnet mask** and **default gateway address** you wish to assign to the appliance.

   **Note**: The static IP address locates the appliance on the local area network. Using the **Obtain IP Address Automatically** option is not recommended.

3. Click **Next**.

   The Proxy Configuration screen appears.

4. If the appliance is communicating to the MessageLabs Network via a proxy server (not recommended), click **This appliance must connect to the Internet via a proxy server** and enter connection details. Otherwise, leave the default option selected.

5. Click **Next**.

   The appliance attempts to connect to the MessageLabs Network, and displays a warning if a problem is detected.

   **Note**: If MessageLabs Professional Services are assisting you with appliance configuration, you can log out of the appliance interface at this time.

6. Enter or confirm your customer ID.

   This unique identifier is provided by MessageLabs.

   **Note**: This field may have been populated already, but you should confirm that the customer ID is correct.

7. Click **Next**.

   The Appliance Name screen appears, prompting for a location and name for the appliance as well as time zone and regional settings.

8. Enter location information:

   a. From the **Location** list, choose one of the configured locations.
   b. Enter an **Appliance Name**. You can assign any name you choose.
   c. Enter the appliance’s **Serial Number**. The serial number is on the sticker on the back of the appliance.
   d. From the **Time Zone** list, select a time zone for the appliances.
   e. From the **Date Settings** list, select the appropriate date settings option. The date settings affect date/time formatting in the user interface.

9. Click **Next**.

   You are prompted to generate the encryption key.

10. Click **Next**.

    The encryption key is generated.

11. Enter Active Directory information:

    a. From the **Active Directory Environment** list, choose **Single Domain** or **Multiple Domain**.
    b. In the **Domain Address Controller** field, enter the IP address or DNS name for the local Domain Controller.
    c. In the Connect As area, fill in the **Domain**, **Name** and **Password**.

12. Click **Next** and enter Journaling Mailbox information:

    a. In the **Exchange Server Address** field, enter the IP address or the fully qualified domain name for the Exchange Server that contains the journaling mailbox.
    b. In the Journaling Mailbox area, specify the **Domain**, **Name** and **Password** for the journaling mailbox.
Click **Next**.
The appliance validates the appliance configuration and the Active Directory and Exchange settings.

14 In the **Send validation Results to** field, enter an email address to which a status report should be sent.

Several validations are performed and a summary of the results is sent to the specified address.

15 Confirm configuration and export the encryption key by following the procedures below.

### 8.3 Confirming Configuration

To confirm that the appliance has been installed and configured correctly, you need to access the MessageLabs Email Archiving Service user interface and perform a basic search. Use the test user you set up earlier (see page 31) for this purpose: the user account must be a member of all MessageLabs Email Archiving Service security groups.

**To log in to the MessageLabs Email Archiving Service user interface:**

1. Open your web browser.
2. Enter the IP address 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.
3. Enter your test user name and password and click **Enter**.
   - The Home screen and Menu appears:

![MessageLabs Email Archiving Service user interface](image)

4. In the Search & Discovery section, click Standard Search.
5. Leaving search criteria blank, click **Search**.
   - For more details on searching, see Finding Your Own Messages.
6. Ensure that some results appear.
8.4 Exporting Encryption Key

During configuration of your first appliance, your company’s unique encryption key was generated for you. You should export this key to a safe place where it will be backed up. If you require additional appliances, the key will be needed for all other appliances.

1. Click **Setup**, then **Key Export/Validation**
   The Key Export/Validation screen appears.
2. Click **Export Key** and choose a destination from which the key will be backed up.
3. To validate the exported encryption key, ensuring it is correct, click **Browse** and navigate to your key file, then click **Validate**.
   If validation does not work, export the key again and repeat the validation. If validation continues to fail, contact MessageLabs support immediately.
4. If you plan to add additional appliances, copy the encryption key to a removable device (such as a USB key) to use when configuring them.

8.5 Configuring Additional Appliances (If Required)

The configuration process is the same for additional appliances as it was for the first appliance (see page 33), with a few exceptions.

8.5.1 Importing Encryption Key

Instead of being prompted to generate the encryption key, you are prompted for the location of the encryption key that was exported from the first Archiving Appliance. All appliances for your company share the same key.

8.5.2 Choosing Purpose of Appliance

You are prompted to choose the purpose of this appliance.

The first appliance was automatically configured to perform all purposes. Additional appliances can be configured to perform just specific purposes (remember, at least one appliance must be configured to perform each purpose at each separate location; see “Understanding Appliance Purposes” on page 13).

If you chose the archiving purpose for this appliance, you can select one of the existing journaling mailboxes or select Other. If you select Other, you are prompted to add a journaling mailbox.

- In the Exchange Server Address field, enter the IP address or the DNS name for the Exchange Server that contains the journaling mailbox.
- In the Journaling Mailbox group, specify the Domain, Name and Password for the journaling mailbox.
8.6 Changing Appliance Configuration

Generally speaking, once an appliance is configured you only need to change its configuration if you are going to use stubbing, or if you are configuring multiple appliances for different purposes. If you are assigning specific purposes to additional appliances, you may need to change the configuration of the first appliance as well: it was automatically configured to perform all purposes.

Unlike initial configuration (done with a wizard), changing the configuration involves choosing from the menu in the appliance’s interface.

\[\text{Note: When updating password information for a journaling mailbox, a stubbing account or Active Directory access, any other references to that account will automatically be updated.}\]

For the most part, modifying an appliance’s settings simply means changing values originally set during configuration and saving the new settings. Settings include:

- network settings
- appliance name settings (including serial number or date/time, but not location)
- journaling mailbox settings (only for appliance configured to perform the archiving purpose)
- directory settings
- purpose (see below)

\[\text{Note: If you need to change the Archiving Appliance’s location you must reset the appliance and re-enter all the setup information.}\]

**To change the purpose of the Archiving Appliance:**

1. In the Archiving Appliance user interface, click **Appliance Purpose**.
2. Check the checkboxes next to the purposes you want to assign to the appliance.

If you choose the archiving purpose, a list of the Exchange journaling mailboxes configured for this location appears. Check the mailboxes that this appliance is to archive or check **Other** and follow the instructions as for the first appliance: see “Configuring First Appliance” on page 33.

If you choose the stubbing purpose, a list of Exchange Servers in this location that are configured for stubbing appears. Check those that are to be assigned to the appliance or click **Add** and follow the instructions in the “To configure stubbing” procedure on page 53.

8.7 Resetting the Archiving Appliance to its Default Configuration

1. In the Archiving Appliance user interface, click **Reset**.
2. Choose **Reset the appliance**.
   The configuration reverts to what it was when you first installed the appliance.

8.8 Temporarily Suspending Archiving from a Journaling Mailbox

Suspending archiving can be useful when upgrading your MessageLabs Email Archiving Service installation. It prevents MessageLabs Email Archiving Service from accessing the journaling mailbox until you remove the suspension. The journaling mailbox continues to receive messages. Any messages currently being processed will be archived, but no additional messages will be retrieved from the journaling mailbox.

1. In the Archiving Appliance user interface, click **Journaling Mailboxes**.
   A list of the journaling mailboxes currently configured for this appliance appears.
2. Select a journaling mailbox and click **Pause**.

\[\text{Note: To resume archiving, click Play.}\]
9 Configuring External Access

Chapter Overview

This chapter explains how to set up user access to the archive from outside the corporate network. This is an optional step. It includes the following topics:

- About Configuring External Access
- Load Balancing and Fault Tolerance on the Proxy Server
- Installing the Archive Proxy
- Setting up the OWA Server

9.1 About Configuring External Access

Configuring external access requires running an installation wizard on each front-end Exchange Server that users will access. Contact MessageLabs Professional Services before performing this installation. In particular, since the process installs an ISAPI filter for IIS, you need to restart the World Wide Web Publishing Service (W3SVC) used by OWA. You should choose a time for the installation so it has the least amount of impact on users. The installation does not make changes to OWA itself.

Note: If you experience problems with OWA, you can disable the archive proxy from the ISAPI Filters tab for the default web site within the IIS management interface.

9.2 Load Balancing and Fault Tolerance on the Proxy Server

If you configure the proxy for multiple appliances (these appliances must perform the purpose of serving the user interface), the proxy will randomly choose among the available appliances to serve each request. If it cannot contact that particular appliance, it will choose an alternate one. For end users, the result will be continued access, even if one of the appliances is not available.

9.3 Installing the Archive Proxy

The Archive Proxy is installed on the front-end server that serves OWA. If there is no front-end server, it is installed on the Primary Exchange Server. The Archive Proxy is responsible for intercepting requests to search the archive and retrieve attachments and redirecting those requests to an appliance.

Note: As the installation of the proxy requires a restart of IIS, you should install the proxy on passive nodes before installing on active nodes. This will reduce the number of failover activities.
To install the archive proxy:
1. Uninstall any previous versions of the Archive Proxy.
2. Log on to the Front-End OWA Server as a user with administrator privileges.
3. Run the archive proxy msi file provided by MessageLabs.
4. Click Next and choose the location for the installed files.
5. Click Next and ensure the Disable OWA Proxy option is cleared. Check this option only if you don’t want users to search or access stubbed content within OWA.
6. If your web server settings prevent unsecured connections, leave the Disallow Unsecure Archive Access option cleared. If your web server settings do not prevent unsecured connections, check the option. This will create a page that redirects users with unsecured connections to the secured site.
7. Click Next and enter the hostnames of your Archiving Appliances.
8. Click Next, then Install.
9. To complete the installation, click Yes. This will restart the World Wide Web Publishing Service (W3SVC).
10. When installation is complete, you are prompted to validate the Archive Proxy Extensions. Check the checkbox and click Finish.

To check the status/configuration of the proxy:
1. Point your browser to https://mail.mycompany.com/archiveproxystatus, where mail.mycompany.com is the DNS entry for the front end OWA server.
   The Archive Proxy Status web page appears, with a set of links for each appliance and overall status information on the proxy.
2. Click the appropriate link for what you want to verify (for example, Access to UI).
   A new page appears, indicating the status of that function.

9.4 Setting up the OWA Server

The OWA server needs to be set up so it is accessed via the same URL whether the user is inside or outside the company.
10 Setting up User Access

Chapter Overview

This chapter explains how to give users different access rights to MessageLabs Email Archiving Service. It includes the following topics:

- MessageLabs Email Archiving Service Security Groups
- Granting Access to MessageLabs Email Archiving Service
- Granting Access to Additional Mailboxes

10.1 MessageLabs Email Archiving Service Security Groups

For users to gain access to MessageLabs Email Archiving Service, their user accounts must be members of one or more of the following security groups. (You created these security groups in “Setting Up MessageLabs Email Archiving Service Security Groups in Active Directory” on page 31.)

<table>
<thead>
<tr>
<th>Security Group</th>
<th>Access Rights Granted to Members</th>
</tr>
</thead>
<tbody>
<tr>
<td>MessageLabs Archive Search Users†</td>
<td>Members can search for and retrieve archived messages in their mailbox. Can also be granted, through MessageLabs Email Archiving Service’s user interface, access to search in other mailboxes and within specified legal holds. All end users of the archive will be members of this group. These users should read Finding Your Own Messages.</td>
</tr>
<tr>
<td>MessageLabs Archive Export Users†</td>
<td>Members can perform all functions of Archive Search Users, and can also export messages from the archive. They can also search within legal holds that they have been explicitly granted access to. These users should read Legal Discovery and Supervision.</td>
</tr>
<tr>
<td>MessageLabs Archive Discovery Users</td>
<td>Members can search through and export any archived message in any mailbox. They can create legal holds and search within or manipulate legal holds they have been explicitly granted access to. Only a small number of trusted users should be members of this group, typically those involved in providing data to opposing council during legal discovery. These users should read Legal Discovery and Supervision.</td>
</tr>
<tr>
<td>MessageLabs Archive Discovery Administrators</td>
<td>Members can perform all MessageLabs Archive Discovery Users functions, as well as creating, manipulating or searching through all legal holds.</td>
</tr>
<tr>
<td>MessageLabs Supervision Reviewers</td>
<td>Members can review and evaluate other people’s messages. These users should read Legal Discovery and Supervision.</td>
</tr>
<tr>
<td>MessageLabs Supervision Senior Reviewers</td>
<td>Members can perform functions of Supervision Reviewers, as well as reviewing and processing messages reviewed by other reviewers and performing other functions such as batch processing. These users</td>
</tr>
<tr>
<td>Security Group</td>
<td>Access Rights Granted to Members</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MessageLabs Supervision Report Users</td>
<td>Members can view and export reports about the number and nature of violations of the corporate electronic communications policy. Typically, group members include senior executives and members of the legal and compliance department. These users should read Legal Discovery and Supervision.</td>
</tr>
<tr>
<td>MessageLabs Archive Disposition Users</td>
<td>Members can authorize the disposition of messages (removing a message from the archive when its disposition date has been reached). These users should also be members of the Archive Discovery Users security group so they can search for messages available for disposition. These users should read Policy Creation and Management, which contains a chapter about disposition.</td>
</tr>
<tr>
<td>MessageLabs Policy Managers</td>
<td>Members can create and modify the corporate electronic messaging policy. Very few individuals should be members of this group, since changes made to the corporate messaging policy represent a change in business process that typically requires cross-functional agreement. These users should read Policy Creation and Management.</td>
</tr>
<tr>
<td>MessageLabs Archive Report Users</td>
<td>Members can view and export reports about the archive itself. Typically, group members include CIOs or IT department members.</td>
</tr>
<tr>
<td>MessageLabs User Managers</td>
<td>Members can assign privileges to other MessageLabs Email Archiving Service users, above and beyond those configured within Active Directory. Can create and manage roles and departments. These users should read Policy Creation and Management.</td>
</tr>
</tbody>
</table>

### 10.2 Granting Access to MessageLabs Email Archiving Service

To grant users access to the appropriate functions of MessageLabs Email Archiving Service, simply make them a member of the appropriate security group.
10.3 Granting Access to Additional Mailboxes

Archive Search and Archive Export users are given, by default, access only to their own mailboxes. This is suitable for the majority of end users. Some such users, however, may require access to additional mailboxes.

**Note:** This step is not needed for batch search functionality, since only Discovery users, who have access to all mailboxes, can search the archive.

**To grant users access to additional mailboxes:**

1. In the web interface Setup section, click **Users**.
   
   A tabbed list of users’ names appears, in alphabetical order by first name, along with a Search tab. The list includes only users who are members of at least one MessageLabs Email Archiving Service Active Directory security group.

2. Using the Search or alphabetical tabs, locate and then double-click on the name of the person to whom you want to grant access to additional mailboxes.
   
   The User Details screen appears. The General tab of the screen shows, in plain English form, the access rights granted to the user using the process described in “Setting up User Access” on page 39. These rights cannot be modified in this tab.

3. On the Search Scope tab, in the **Additional mailbox or groups of mailboxes** field, enter all or part of the name of the mailbox, or group of mailboxes, this user should have search access to.

   **Note:** Since Archive Discovery users can see all mailboxes in the archive, Search Scope is not a configurable option for such users.

4. Click **Check Name**.
   
   If the name matches, it becomes underlined. If there are multiple names, a suggestion list appears for you to select from: the list includes two tabs, one for Active users, one for Deleted users. The Deleted tab allows you to retain access to a user’s messages even once they are deleted from Active Directory.

5. Click **Add**.

   The mailbox is added to the list in the text field.

6. Repeat for each additional mailbox the user should have access to.

7. Click **Save**.

   The search access to the mailboxes is assigned.
11 Giving Access to Archive from Outlook/OWA

Chapter Overview

This chapter explains how to give users access to the archive from Outlook or, if external access has been configured, OWA. It includes the following topics:

- Overview
- Preconditions
- Setting Up Accounts for Outlook Folder Creator
- Running Outlook Folder Creator
- Scheduling Outlook Folder Creation

11.1 Overview

End users who are part of the Archive Search, Archive Discovery or Archive Export security groups can have access to MessageLabs Email Archiving Service through the familiar Outlook/OWA environment.

**Note:** This feature is not available for batch search implementations.

Access to the archive is handled through a folder added to the mailbox of each appropriate user. The Outlook Folder Creator is used to create this folder, which is typically called "Archive by MessageLabs". The folder allows users to access the archive from their Microsoft Outlook client. It points to the MessageLabs Email Archiving Service Outlook user interface pages provided by the appliance, generally via the Archive Proxy.

The steps involved are as follows:

1. If users are to gain access through OWA as well as or instead of Outlook, install the Archive Proxy (see page 37).
2. Set up accounts for the Outlook Folder Creator (see below).
3. Run the Outlook Folder Creator (see page 45).
   This affects current users only.
4. Optionally, schedule ongoing Outlook folder creation (see page 46).
   This ensures that new users who are members of the appropriate MessageLabs Email Archiving Service security groups automatically gain access to MessageLabs Email Archiving Service from Outlook/OWA.

**Note:** If you do not set up a schedule, you will need to run the Outlook Folder Creator again each time you add users to the Archive Search, Archive Discovery or Archive Export security groups.

11.2 Preconditions

You must have the .NET framework version 2.0 installed on the machine running the Outlook Folder Creator. You can download this directly from Microsoft’s web site. The .NET framework does not need to be installed on end user desktops.

The machine on which the tool is to be run must have Outlook 2003 or 2007 installed. The tool executable must reside locally on the machine from which it will be run. It cannot reside on an external drive or USB memory stick.

The accounts chosen to complete the AD and Exchange tasks must have the correct permissions.
11.3 Setting Up Accounts for Outlook Folder Creator

The MessageLabs Outlook Folder Creator uses accounts for two purposes: to access Active Directory and to access each Exchange Server that hosts mailboxes to be processed. You can use the same account for both purposes, if you wish, but the single account needs to have all the appropriate permissions described below.

The account used to access your Active Directory server or Global Catalog server must have read access to the Configuration Naming Context.

The account used to access the Exchange Server must have write access to all of the mailboxes on the mailbox databases that you want to update. It must be an “Exchange View-Only Administrator” with “Receive As” and “Administer Information Store” permissions in one of the following AD objects:

- <Exchange Organization Container>
- <Exchange Administrative Group>
- <Exchange Server>

The procedures below assume that one account will be used for both purposes.

To set up the appropriate account and permissions in Exchange 2003:
2. Connect to the domain in which you want to create the user.
3. Right-click the organizational unit in which you want to create the user and choose New, then User.
4. Enter a full name and a user login name. For example, MessageLabsFolderCreator.
5. Click Next and enter and verify a password. Set the username must change password, user cannot change password and password never expires options in accordance with your company’s policies. Record the login name and password; you will need them when you configure the Outlook Folder Creator.
6. Click Next and ensure that the Create an Exchange e-mail address check box is checked.
7. Click Next, then Finish.
   The user account and mailbox will be created.
8. Ensure the new account (e.g. MessageLabsFolderCreator) has read access to the Configuration Naming Context and Receive As and Administer Information Store rights:
   a. In ADSIedit, under Configuration, right-click on CN=Configuration, DC=Domain, DC=org and choose Properties.
   b. On the Security tab, click Add, then enter the Active Directory account and check Allow Read.
   c. Click Advanced and, on the Permissions tab, select the new account (e.g. MessageLabsFolderCreator), click Edit and choose This object and all child objects (from the Apply onto list) then click OK.
   d. In ADSIedit, under CN=Microsoft Exchange (which is under CN=Configuration, DC=Domain, DC=ORG, then CN=Services), right-click on the organization and choose Properties.
   e. On the Security tab, click Add and add the new account (i.e. MessageLabsFolderCreator), giving it the “Receive-As” and “Administer Information Store” privileges.
   f. Click Advanced and, on the Permissions tab, select the new account (i.e. MessageLabsFolderCreator) for “Receive-As” permission. Select This object and all child objects (from the Apply onto list).
   g. On the Permissions tab, select the new account for “Administer Information Store” permission. Select This object and all child objects (from the Apply onto list).
In the Exchange System Manager, select the top level, right-click on the new account (i.e. MessageLabsFolderCreator) and choose Delegate Control.

Click Next, then click Add and browse to the new account (e.g. MessageLabsFolderCreator).

From the Role list, choose Exchange View Only Administrator.

Click OK, then Next, then Finish.

To set up the appropriate account and permissions in Exchange 2007:

1. On your primary Exchange Server, open the Exchange Management Console.
2. In the tree, expand Recipient Configuration.
3. Right-click on Mailbox and choose New Mailbox.
4. Select User Mailbox and click Next.
5. Select New User and click Next.
6. Choose the Organizational Unit in which you want to create the account.
7. Enter the full user name and a user login name.
   For example, MessageLabsFolderCreator.
8. Enter a value for password (and verify password). Set the username must change password, user cannot change password and password never expires options in accordance with your company’s policies.
   Record the login name and password; you will need them when you configure the Outlook Folder Creator.
9. Click Next. For Mailbox Settings, leave the Alias at its default and ensure the correct Server, Storage Group and Mailbox database are selected.
10. Click Next. Confirm the configuration summary settings are correct.
11. Click New. Exchange System Manager will attempt to create the user account and mailbox.
12. Once the wizard has completed successfully, click Finish.
13. Under Organization Configuration, click Add Exchange Administrator and browse to the new account (e.g. MessageLabsFolderCreator).
14. From the Role list, choose Exchange View-Only Administrator.
15. Click Add, then Finish.
16. Ensure the new account (i.e. MessageLabsFolderCreator) has read access to the Configuration Naming Context and Receive As and Administer Information Store rights:
   a. In ADSIedit, under Configuration, right-click on CN=Configuration, DC=Domain, DC=org and choose Properties.
   b. On the Security tab, click Add, then enter the Active Directory account and check Allow Read.
   c. Click Advanced and, on the Permissions tab, select the new account (i.e. MessageLabsFolderCreator), click Edit and choose This object and all child objects (from the Apply onto list) then click OK.
   d. In ADSIedit, under CN=Microsoft Exchange (which is under CN=Configuration, DC=Domain, DC=ORG, then CN=Services), right-click on the organization and choose Properties.
   e. On the Security tab, click Add and add the new account (i.e. MessageLabsFolderCreator), giving it the “Receive-As” and “Administer Information Store” privileges.
   f. Click Advanced and, on the Permissions tab, select the new account (i.e. MessageLabsFolderCreator) for “Receive-As” permission. Select This object and all child objects (from the Apply onto list).
   g. On the Permissions tab, select the new account for “Administer Information Store” permission. Select This object and all child objects (from the Apply onto list).
11.4 Running Outlook Folder Creator

MessageLabs’ Outlook Folder Creator gathers information about how to connect to Active Directory and Exchange to allow for the creation of the “Archive by MessageLabs” folder within user’s mailboxes. At the end of the wizard, a configuration file is created and you are prompted to run the process that creates the folder in user’s mailboxes.

Within the wizard, you will be prompted to choose one of the following options:

- specify a specific account the tool should use, in which case the account information is stored in encrypted form in the configuration file
- have the tool run in the account you are logged in to; if you plan to schedule folder creation, the account to use for the schedule can be specified by Windows Scheduler’s “run as” option

Either account needs to have the permissions described in “Setting Up Accounts for Outlook Folder Creator” on page 43.

Note: Vista users must either by logged on as an administrative user or right-click on the tool executable and choose Run As Administrator.

To run the Outlook Folder Creator:

1. Double-click on the MessageLabs Outlook Folder Creator executable and click Next until you are prompted for your Active Directory environment.
2. Click Single Domain Environment.
   - or -
   Multiple Domain Environment (using Global Catalog).
3. Click Next.
   The Enter Active Directory Settings panel appears, with options that vary depending on your environment choice.
4. For single domain environments, enter the address for the Active Directory server.
   - or -
   For multiple domain environments, enter the address for the Global Catalog Server as well as the address for the Active Directory server that contains the MessageLabs Email Archiving Service security groups (if they are not on the Global Catalog server).
5. For either environment, choose whether you want to connect as the current user or select Connect as and enter your domain, user name and password.
6. Click Next.
   The tool connects to Active Directory and reads through the configuration context to find all Exchange Servers in your organization. The Enter Exchange Server Settings panel appears, listing the Exchange Servers found.
7. Check all Exchange Servers whose mailboxes you want to process. To not process mailboxes for a particular Exchange Server, clear the checkbox beside the server name.

Note: Not processing mailboxes for a particular Exchange Server is useful if you have Exchange Servers in multiple geographic locations. You can run the Outlook Folder Tool in each of those locations, focusing on processing mailboxes on the local servers.

8. Click Next.
   For each selected Exchange Server, you are prompted to select the credentials to be used.
9. Choose whether you want to connect as the current user or select Connect as and enter your domain, user name and password.
10. Click Next and save the configuration file.
    If you will schedule folder creation, take note of the path name.
11. Optionally select Run now.
    You will be presented with the set of mailboxes that are members of the Archive Search Users, Archive Export Users or Archive Discovery Users security group.
11.5 Scheduling Outlook Folder Creation

Scheduling folder creation will automatically create the appropriate folder when new users who belong to the Archive Search Users, Archive Export Users or Archive Discovery Users security group are created in the mail system. For more about these security groups, see “Setting up User Access” on page 39.

To set up a schedule for Outlook Folder Creator:

1. In Windows Scheduler, create a job as follows:
   OutlookFolderTool --console configfilename.xml
   where configfilename.xml is the configuration file you created.

2. If your configuration file was set to use “current user”, set the “run as” option to be an account that has the permissions outlined earlier.
12 Setting Up Stubbing

Chapter Overview

This chapter explains how to work with MessageLabs Email Archiving Service Stubbing, an optional function that lets you manage mailbox sizes, removing storage-intensive attachments from Exchange while keeping those attachments accessible to Outlook users.

It includes the following topics:

- About Stubbing
- About the Stubbing Process
- About the Stubbing Account and Form
- About Stubbing Policies
- Overview of Stubbing Configuration Steps
- Creating User Account for Stubbing
- Creating Organizational Forms Library
- Publishing Stubbing Forms
- Configuring the Appliance for Stubbing
- Working with the Stubbing Policy
- Enabling or Disabling Stubbing

12.1 About Stubbing

On a nightly basis (the exact time is an appliance configuration option), a stubbing process visits mailboxes and replaces attachments with stubs, using an administrative account that has permissions to update messages in those mailboxes. The mailboxes this service visits, and the rules it uses to determine what attachments to stub, are defined in a stubbing policy. Unlike archiving, which happens as soon as a message is sent or received, stubbing occurs at a point in the future (for example, 30 days after a message is sent or received).

By default, stubbing stubs only attachments found in the archive. In that case, stubbing does not need to be configured immediately on system setup.

An option is available to have stubbing done on attachments even if they are not in the archive. In that case, stubbing should be configured on system setup.

Stubbing configuration should be done only in consultation with MessageLabs Professional Services.

12.2 About the Stubbing Process

The stubbing process is a background task that runs during the time window defined as part of the Archiving Appliance configuration. During that time window, the stubbing processor logs into the mailboxes identified for stubbing, using an administrative account that has permissions to update messages in those mailboxes.

Once the process has visited all folders identified for stubbing in all mailboxes once, it has completed a “round”. A round may take several days and processing windows to complete, particularly when the stubbing process is run the first time.

To ensure maximum benefit to all mailboxes, and to avoid getting “stuck” on a particularly large mailbox, the stubbing processor stubs a maximum of 100 messages (depending on how many attachments are associated with a message, it may stub more than 100 attachments) per mailbox at a time. It then moves on to the next mailbox that needs to be processed. The system keeps track of where it was, and will cycle back to any mailbox that was not completely processed.

Within a mailbox, the processor works on a folder-by-folder basis, starting with the Deleted Items, then Sent Items, then other folders, leaving the Inbox until last. This mimics the way people typically choose to manage their mailbox sizes.
Once all of the folders for a mailbox have been processed, the system measures the size of the mailbox and compares it to the mailbox storage quota, as configured in Exchange. If you have set up quota-based rules and the mailbox remains larger than the target size, the stubbing processor will begin to process messages in that mailbox based upon size, regardless of their age. Once again, this process works folder-by-folder, in the order described above. After each folder is processed, the mailbox size is calculated. If the mailbox size has reached its target, mailbox processing finishes for the current round. If it has not reached the target, processing continues, based on the quota-based rules.

12.3 About the Stubbing Account and Form

On each Exchange Server that hosts mailboxes, create an account that has permissions to read and modify the mailboxes that will be associated with a stubbing policy.

An Outlook form must be installed on each Exchange Server where stubbing will be performed. This form is used to handle forwarding of stubbed attachments from Outlook. It is installed into an organizational forms library which is then replicated to multiple Exchange Servers. The process involves creating an organizational forms library (if one doesn’t already exist), and installing the stubbing forms.

12.4 About Stubbing Policies

Since stubbing policies are not versioned, you create them as separate stubbing policies, rather than adding them as policy entries to your corporate electronic message policy. Stubbing policies have two main components: the mailboxes that they affect and the rules that apply to those mailboxes.

Stubbing policies identify the mailboxes (of individual users, Active Directory groups, departments or roles) to be affected by that policy and the rules to apply to those mailboxes. You can have as many stubbing policies as you wish, allowing you to apply different stubbing rules to different users. If the same mailbox is potentially affected by more than one stubbing policy (for example, policy X applies to a group that the individual belongs to, and policy Y applies to a role that the individual plays), only one stubbing policy applies to that mailbox. The system chooses which policy to apply based on the order in which the policies are listed in the MessageLabs Email Archiving Service user interface: the first policy in the list that applies to the mailbox is used.

The rules for stubbing policies identify, for each folder (Deleted Items, Sent Items, Inbox, etc.) of those mailboxes, the age of attachments that should be stubbed. For example, you might specify to stub attachments in the Deleted Items folder 20 days after the message was sent and stub attachments in the Inbox folder 30 days after the message was received. You also specify what size (for example, over 1000 KB) of attachments are to be stubbed.

Rules can also specify the target size of the mailbox, based on a percentage of the mailboxes’ storage quota, and what size attachments should be stubbed in order to meet that target size. For example, say Mailbox A has a quota of 100 MB. The stubbing policy says that it should be at 80% of this quota after stubbing. After all attachments qualified by age are stubbed, the mailbox is still 90 MB. The stubbing process continues stubbing (for example, stubbing attachments larger than 500 KB). If after this effort the mailbox is at 80 MB, stubbing is complete for the moment. If the mailbox is still above 80 MB, though, another attempt is made (for example, by stubbing attachments larger than 250 KB). If at the conclusion of that process the mailbox is still above 80 MB, a third and final stubbing is done.

Note: Although it is unlikely, the mailbox may be still above quota when the three passes for quota-based rules are complete.
12.5 Overview of Stubbing Configuration Steps

To configure stubbing:

- If using OWA, install the proxy (see "Configuring External Access" on page 37).
- Create the necessary Exchange accounts for stubbing (see below).
- If one does not exist, create an Organizational Forms Library (see “Creating Organizational Forms Library” on page 50)
- Publish the Outlook form, available from MessageLabs Professional Services (see “Publishing Stubbing Forms” on page 52)
- Change the configuration of an Archiving Appliance to handle stubbing (see “Configuring the Appliance for Stubbing” on page 53).
- Define stubbing policies (see “Working with the Stubbing Policy” on page 53).

12.6 Creating User Account for Stubbing


1. On your primary Exchange Server, open the Active Directory Users and Computers MMC snap-in.
2. The Microsoft Management Console opens for configuration of Active Directory Users.
3. Connect to the domain in which you want to create the account.
4. Right-click the organizational unit in which you want to create the account and choose New, then User.
5. Enter a full name and a user login name. For example, MessageLabs_Archiving_Service_Stubbing_<ExchServerName>.
6. Click Next and enter and verify a password. Set the User must change password at next logon, User cannot change password and Password never expires options in accordance with your company’s policies.
7. Record the login name and password: you will need them when you configure the Archiving appliance for stubbing purposes.
8. Note: If you allow the password to expire, you must change it manually and reconfigure the appliance each time it changes.
9. Click Next and ensure that the Create an Exchange e-mail address check box is checked.
10. Click Next, then Finish. The stubbing account is created.
11. Open the Exchange System Manager on the Exchange Server that the stubbing account was created on.
12. Right-click on the server and choose Delegate control. The Delegate Control wizard appears.
13. Click Add and enter the user name of the stubbing account and click OK.
14. From the Roles list, choose Exchange Administrator.
15. Click Next, then Finish, then OK.
16. Log in to the new account using OWA so Exchange will initialize the mailbox.
12.6.2 Creating a User Account for Stubbing on Exchange 2007

On your primary Exchange Server, open the Exchange Management Console.

1. In the tree, expand Recipient Configuration.
2. Right-click on MailBox and choose New Mailbox.
3. Select User Mailbox, then click Next.
4. Select New User, then click Next.
5. Choose the organizational unit in which you want to create the account.
6. Enter the full user name and a user login name (for example, MessageLabs_Archiving_Service_Stubbing_<ExchServerName>).
7. Enter a value for Password (and Verify Password). Set the User must change password at next logon. User cannot change password and Password never expires options in accordance with your company's policies.
   Record the login name and password: you will need them when you configure the Archiving appliance for stubbing purposes.

   **Note:** If you allow the password to expire, you must change it manually and reconfigure the appliance each time it changes.

8. Click Next. For Mailbox Settings, leave the Alias at its default and ensure the correct Server, Storage Group and Mailbox database are selected.
9. Click Next. Confirm the configuration summary settings are correct.
10. Click New. Exchange System Manager creates the user account and mailbox.
11. Once the wizard has completed successfully, click Finish.
12. In the tree, right-click Organization Configuration and choose Add Exchange Administrator.
13. Browse to select the account created above.
15. Click Add and log in to the new account using OWA so Exchange will initialize the mailbox.

12.7 Creating Organizational Forms Library

An organization forms library allows you to replicate the library and its contents to other Exchange Servers. If you already have an organizational forms library in place, go to the appropriate procedure for installing the stubbing forms: either “Installing Stubbing Forms in Outlook 2003” on page 52 or “Installing Stubbing Forms in Outlook 2007” on page 52.

12.7.1 Creating an Organizational Forms Library in Exchange 2000/2003

**Note:** In the Exchange System Manager, expand Administrative Groups.

1. Expand the node for the administrative group with mailboxes you plan to stub and then expand Folders.
2. Right-click Public Folders and choose View System Folders.
   The system folders for the administrative group appear in the left pane.
3. Right-click EFORMS REGISTRY and choose New, then Organizational Form.
   The General tab of the Properties screen appears.
4. In the Name field, enter a name for the forms library. For example, "MessageLabs Email Archiving Service Stubbing Forms – ENGLISH".
5. From the E-forms language list, choose English.
6. Click OK and verify the permissions that have been set for the forms library so that client computers have permission to access the forms:
   a. Right-click the new library (listed under EFORMS REGISTRY) and choose Properties from the context menu. The Properties screen for the forms library appears.
   b. On the Permissions tab, click Client permissions. The Client Permissions screen appears.
Verify that Default has a Reviewer Role, that the Read items option is selected in the Permissions area, and that Edit items and Delete items are set to None.

On the Client Permissions screen, click Add. The Add Users screen appears.

Choose your account from the list and then click Add. This is the account that you have an Outlook profile for.

Click OK to return to the Client Permissions screen.

Choose your account from the list and then choose Owner from the Roles list.

Click OK to return to the Permissions tab of the Properties screen.

On the Replication tab of the Properties screen, configure the forms library to replicate to any remaining Exchange Servers on which you plan to perform stubbing. For instructions, refer to the Exchange documentation.

Click OK to close the Properties screen.

12.7.2 Creating an Organizational Forms Library in Exchange 2007

Note: An organization forms library allows you to replicate the library and its contents to other Exchange Servers. If you already have an organizational forms library in place, go to the appropriate procedure for installing the stubbing forms. See “Installing Stubbing Forms in Outlook 2007” on page 52.

1. Start Exchange Management Console.
2. Under Server Configuration, select Mailbox.
3. If you do not already have a public folder database, create a new storage group for public folders:
   a. In the Actions pane, click New Storage Group.
   b. Enter the name of the new storage group and click NEW.
   c. Right-click on the new storage group and choose Create New Public Folder Database.
   d. Enter a name, such as “Public Folder Database” and click NEW.
4. Click Toolbox and double-click Public Folder Management Console.
5. In the left pane, click System Public Folders.
6. If you do not already have an E-FORMS REGISTRY:
   a. In the Action pane, click New Public Folder.
   b. Type “EFORMS REGISTRY” as the folder name, and then click NEW.
7. Right-click on the E-FORMS REGISTRY and choose New Public Folder.
8. Enter the name of the new public folder. For example, “MessageLabs Email Archiving Service Stubbing Forms – ENGLISH”.
9. Start Exchange Management Shell and run the following command:
   Add-PublicFolderClientPermission -Identity "/NON_IPM_SUBTREE/EFORMS REGISTRY\MessageLabs Email Archiving Service Stubbing Forms - ENGLISH" -user USERNAME -AccessRights Owner
   Where USERNAME is the user you wish to install the Outlook forms with and Owner permissions.
10. Add the PR_EFORMS_LOCALE_ID property to set the language of the forms folder:
   b. Install the tool on a workstation with Outlook installed and a mail profile where the account belongs to the Exchange Administrators Group.
   c. Start the Microsoft Exchange Server MAPI Editor.
   d. On the Session menu, click Logon and Display Store Table.
   e. Select the MAPI profile for the user specified as the library owner in step 9.
   f. On the MDB menu, click Open public Folder Store, and then click OK.
   g. Expand Public Root, expand NON_IPM_SUBTREE and then expand EFORMS REGISTRY.
   h. Click on the public folder created in steps 6 through 8 (“MessageLabs Email Archiving Service Stubbing Forms – ENGLISH”).
   i. On the Property pane menu, click Modify Extra Properties.
   j. Click Add, and then click Select Property Tag.
Click **PR_EFORMS_LOCALE_ID** in the list, then click **OK**.

Click **OK**, twice.

Double click **PR_EFORMS_LOCALE_ID**, and in the **Unsigned Decimal** box, type “1033” for US English, “2057” for UK English, or “1036” for French.

Select **PR_PUBLISH_IN_ADDRESS_BOOK**, then right-click and select **Edit Property**. Clear **Boolean** and then click **OK**.

Close the **MAPI Editor**.

### 12.8 Publishing Stubbing Forms

The “ArchiveStub.Attachment.oft” is a custom form that is deployed to the Organizational Forms Library in Exchange. When a user opens their Outlook client, the form is downloaded from the Library. This is kept in cache until the user clears the cache or the form is updated in the Library. The form is available from MessageLabs Professional Services.

#### 12.8.1 Installing Stubbing Forms in Outlook 2003

1. Using Outlook 2003 (English version) and the appropriate profile (account specified in the organizational forms library procedure – see “Creating an Organizational Forms Library in Exchange 2000/2003” on page 50), connect to the desired Exchange Server to publish the appropriate Outlook form to the organizational forms folder.
2. In Outlook, choose **Tools**, then **Forms** then **Design a Form**.
3. Choose **User Templates in File System** from the **Look in** list, and click **Browse** to select the **ArchiveStub.Attachment.oft** (Outlook form) file to publish.
4. Click **Open**.
   The Outlook form opens.
5. Choose **Tools**, then **Forms**, then **Publish Form As**.
6. Choose the organizational forms folder (created in the organizational forms library procedure) from the **Look in** list and enter **ArchiveStub.Attachment** in the display name field, then click **Publish**.
   The form is published to the organizational folder and is ready to be used.

#### 12.8.2 Installing Stubbing Forms in Outlook 2007

1. Using Outlook 2007 (English version) and the appropriate profile (account specified in the organizational forms library procedure – see “Creating an Organizational Forms Library in Exchange 2007” on page 51), connect to the desired Exchange Server to publish the appropriate Outlook form to the organizational forms folder.
2. In Outlook, choose **Tools**, then **Forms**, then **Design a Form**.
3. Choose **User Templates in File System** from the **Look in** list, and click **Browse** to select the **ArchiveStub.Attachment.oft** (Outlook form) file to publish.
4. Click **Open**.
   The Outlook form opens.
5. On the Developer tab, click **Publish** and choose **Publish Form As**.
6. Choose the organizational forms folder (created in previous procedure) from the **Look in** list and enter **ArchiveStub.Attachment** in the display name field, then click **Publish**.
7. The form is published to the organizational folder and is ready to be used.
12.9 Configuring the Appliance for Stubbing

This procedure is valid only for Archiving Appliances configured to perform the stubbing purpose. It should be done only in consultation with MessageLabs Professional Services.

1. In the Archiving Appliance user interface, click **Stubbing Settings**.
   
   A list of the Exchange Servers in this location that are configured for stubbing appears.

2. To have this appliance stub attachments from an Exchange Server in this list, click the Exchange Server.
   
   A new screen appears, showing a list of the appliances that process mail for the selected Exchange Server.

   **Note:** If necessary, you can add an Exchange Server by clicking Add new Exchange Server and then entering the name and domain of the Exchange Server and the name and password of the user account created for stubbing purposes.

3. Choose the appropriate appliance and click **Change Schedule**.
   
   A screen appears, showing in visual form all the possible hours in a working week. Click to enable or disable stubbing during specific hours.

   **Note:** Set your stubbing time window to avoid overlapping with automated backup procedures.

4. Enter the Retriever URL, the address to the Archive Proxy (typically the same as the DNS for Webmail). This cannot be an IP address. For example: https://webmail.mycompany.com

5. Click **Save** to confirm the new settings or click **Cancel** to keep the previous settings.

12.10 Working with the Stubbing Policy

For more information about developing policies, see **Policy Creation and Management**.

An individual mailbox can be affected by only a single stubbing policy. If the same mailbox is potentially affected by more than one stubbing policy, the system chooses which policy to apply based on the order in which the policies are listed in the interface. The first policy in the list that applies to the mailbox is used. To change the priority of stubbing policies, select a policy and use the up or down arrow buttons to change its order in the list.

You may also want to create a default stubbing policy that applies to all users. If you place this policy at the bottom of the list, it will affect only those mailboxes not addressed by all the other policies, ensuring that stubbing is defined for everyone in the organization.

**Warning:** If a mailbox that is not being archived is configured to stub attachments for messages in the archive, no stubbing will take place and needless processing effort will result.

12.10.1 Creating Stubbing Policy

**To create a stubbing policy:**

1. In the web interface Policy section, click **Stubbing**.
   
   A list of the currently defined stubbing policies appears.

2. Click **Add**.
   
   The Policy Details screen appears.
3 On the General tab, enter a unique name for the stubbing policy and choose whether or not the policy is enabled.
4 On the Description tab, enter a description for the policy.
5 On the Comments tab, enter comments about the policy.
6 In the Settings menu, click **Users** and choose, in the top list, the users or groups of users to be affected by the policy. In the bottom list, choose the users or groups you do not want affected by the policy.
7 To specify the rules for stubbing in the specified mailboxes, in the Settings menu click **Stubbing Rules** and follow the instructions below.
8 To save the policy, click **Save**.

The policy is added to the list of stubbing policies and will take effect at the next stubbing time window.

**Specifying Stubbing Rules**

**To specify rules for a stubbing policy:**

1 If necessary, open the stubbing policy for modifying and, in the Settings menu, click **Stubbing Rules**.

   The Stubbing Rules screen appears.

2 On the General tab, define what constitutes a "large" attachment.

   The size entered here will be used to determine what size attachment will be stubbed based on the folder-specific rules.

3 Define what size of attachment should never be stubbed.

   Attachments below the specified size will not be stubbed, even if the storage quota for the mailbox has not been met.
To have attachments stubbed even if they are not in the archive, or if the attachment has changed since it was archived, select the Archive a copy of the attachment... option.

**Note:** If you plan to import data, wait until your import task is completed before enabling this option.

Click the tab for a folder (Deleted Items, Sent Items, Inbox or Other Folders). The appropriate folder-specific tab appears. For example:

To indicate messages in this folder may be stubbed, check the Stub attachments for messages in... option.

Enter the age large attachments must reach before being stubbed.

Enter the age other attachments must reach before being stubbed.

**Note:** For the Inbox, you specify four ages: two that apply to messages that have been read and two that apply to messages that have not been read.

Repeat for each appropriate tab.

If desired, enter quota-based rules (see below).

**To specify quota-based rules for a stubbing policy:**

**Note:** These rules only take effect if the mailbox has a "prohibit send and receive" quota defined in Exchange that determines the maximum size of an individual mailbox.

If necessary, open the policy and, in the Settings menu, click Stubbing Rules, then click the Mailbox Quota tab.

To indicate you want quotas considered when stubbing attachments, check the Stub additional attachments... option.

Enter the percentage of the storage quota that stubbing should achieve.

Enter the size of the attachments that should be stubbed for the message quota process. Enter three separate sizes, one for each sequential stubbing pass.
12.11 Enabling or Disabling Stubbing

Temporarily disabling stubbing for the entire system can be useful when upgrading your MessageLabs Email Archiving Service installation or when doing maintenance on your Exchange system. Disabling an individual stubbing policy can be useful if you are not ready to deploy stubbing to all users.

To activate or suspend stubbing for the entire MessageLabs Email Archiving Service system:
1. In the Policy section, click **Stubbing**.
   A list of the currently defined stubbing policies appears.
2. Click **Suspend Stubbing/Active Stubbing**.

   **Note:** The name toggles, depending on whether stubbing is currently enabled or disabled.
3. When prompted, confirm or cancel.

To enable or disable an individual stubbing policy:
1. In the Policy section, click **Stubbing**.
   A list of the currently defined stubbing policies appears.
2. Select a stubbing policy and click **Edit**.
   The Policy Details screen appears.
3. In the General tab, clear the **Enabled** checkbox.
13 Troubleshooting MessageLabs Email Archiving Service

Chapter Overview

This chapter explains commonly performed maintenance procedures. It includes the following topics:

- Using the Audit Trail to View Login Activity
- Solving Common Problems
- Troubleshooting User Directory Issues
- Troubleshooting Archiving Issues

13.1 Using the Audit Trail to View Login Activity

User Manager Users can use the audit trail to view:

- Successful logins.
- Unsuccessful login attempts.

*Note:* The audit trail for a specific message can be viewed by right-clicking on the message in the results list.

1. In 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. Check one or both of **Login Successful** or **Login Unsuccessful**.
4. Optionally, specify a time limitation for the activities by choosing from the **Event Date** list.
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.

13.2 Solving Common Problems

MessageLabs Email Archiving Service processes messages prior to storing them in its secure archive. Occasionally, the content of the message, or an attachment, or references to users and groups in Active Directory, can't be processed properly. When this happens the message is put aside.

To index messages, all senders and recipients must be known. The Archiving Appliance must be able to resolve addresses into the corresponding Active Directory entries in order to assign the appropriate search permissions. Similarly, distribution lists must be expanded to the actual set of recipients.

In rare cases, the appliance may not recognize some component in the message. As an example, this can happen if the message itself is corrupted.

When these types of issues occur, the message is put aside in a sub-folder of the journaling mailbox so that processing of other messages can proceed. The MessageLabs Email Archiving Service user interface’s **Setup** menu section contains a **Status and Issues** subsection that help you to investigate the problems and if necessary submit them to MessageLabs for further evaluation. To generate a CSV file of your current data for support purposes, click **Download** from this section.

If you have referenced an Active Directory group, either from your roles/departments or through review privileges or stubbing policies, changes to those groups are synchronized nightly. To see a list of those groups and when they were last synchronized, from the **Status and Issues** section, click **Group Synchronization Status**.
13.3 Troubleshooting User Directory Issues

If the Archiving Appliance cannot access specific properties for an Active Directory user, such as the MailboxGUID property, the message cannot be fully indexed. Similarly, if the appliance cannot access the Group Members property for a distribution list, the appropriate set of users and mailboxes cannot be assigned to the message. Other issues may occur, but the two just mentioned are the most likely. The problem is usually solved by assigning the proper permissions to the account that the Archiving Appliance uses to access Active Directory, or by mapping deleted users to information that already exists in the archive about those users.

The archiving process attempts to gather additional information for each Exchange address referenced in a message. This information is normally gathered from Active Directory. When a user (or mailbox) is deleted, however, Active Directory no longer contains the required information, so the archiving process records the address as an issue, and puts the message aside. On a weekly basis, MessageLabs Email Archiving Service attempts to automatically resolve this type of issue. A process scans the archive to see if it can find older messages that were successfully archived for each problematic Exchange address. If it finds a match, a deleted user mapping is created. Once all mappings have been updated, all messages put aside for user directory issues are moved to the reprocess queue where they can be reviewed and reprocessed.

While the automated mapping process attempts to deal with the majority of issues related to deleted users, there will still be cases where manual mapping is required. For example, if a message that arrives in the journaling mailbox references a user that has never been archived before, the automated mapping process can't gather the required information. To address this, the manual mapping tools attempt to provide suggestions by searching the archive based on display name, allowing you to map messages to another mailbox that is a replacement mailbox for that user, or to opt to treat the user as an external address. You can investigate archiving issues and perform mapping if you are a member of the User Managers group.
To view a list of issues related to Active Directory:

1. In the Setup section, in Status and Issues, click **User Directory Issues**.

   A list of issues appears, on three tabs: Current Issues, Deleted User Mapping and Deleted Group Mapping.

   The Current Issues tab *Display Name* column contains those names that the Archiving Appliance cannot resolve. The *Issue Description* column gives information about the type of problem. There are many possibilities, among which are:
   - Unable to read Display Name
   - Unable to read Group Members
   - Unable to access object

2. Click on the user that has an issue, then click **Details** on the toolbar.

   The *Issue Details* screen appears, giving additional information about the issue. The screen lists the Active Directory account and the display name of the message that contains the problem. It also shows you the steps to take to resolve the issue.

3. Follow the instructions given in the Issue Details screen.

   Performing the actions given in the screen should rectify the problem.

4. Repeat steps 2 and 3 for each item in the **User Directory Issues** list.

5. Click OK.

To mark users as deleted:

1. In the Setup section, in Status and Issues, click **User Directory Issues**.

2. On the Current Issues tab, click on the user or group that you want to mark as deleted.

3. Click **Mark User as Deleted**.

   The *Mark as Deleted User* dialog appears.

4. Click **Process as Internal Address** or **Process as External Address**

5. Enter the *SMTP address* and *Mailbox GUID* for the user, or *SMTP address* for the group
   - or, for internal address –
     Click **Find Suggestions** and select the correct name from the list

6. Click OK.
**To mark groups as deleted:**

1. In the Setup section, in Status and Issues, click **User Directory Issues**.
2. On the Current Issues tab, click on the group that you want to mark as deleted.
3. Click **Mark Group as Deleted** on the toolbar.
   
   The **Mark as Deleted Group** dialog appears.

4. Enter the **SMTP address** for the group
   - or –
   
   Click **Find Suggestions** and select the correct name from the list
5. Click **OK**.

**To reprocess messages:**

1. When all issues have been addressed, click **Reprocess Messages** in the toolbar.
   
   The messages are validated. A screen appears that informs you that messages are being reprocessed. Note that messages that are more than 30 days old do not get submitted for supervision review.
2. Click **OK**.
   
   Further issues may occur as a result of reprocessing. If so, repeat the steps in this procedure.

**To view a list of users/groups that have been marked as deleted:**

1. In the Setup section, in Status and Issues, click **User Directory Issues**.
2. Click the Deleted User Mappings or Deleted Group Mappings tab.
   
   A list of mapped users/groups appears, with user information on one tab and group information on another.

**Note:** To edit a user/group that has been marked as deleted, click on it and click **Edit**.
13.4 Troubleshooting Archiving Issues

Archiving issues arise when the Archiving Appliance cannot process the message because:

- some of the senders and recipients are unknown
- the message is flagged as a special type that MessageLabs Email Archiving Service wasn’t designed to archive
- the message itself is corrupted in the mail system.

The Journal Folder Status screen shows how many messages are currently in the processing queue as well as the number of messages that have been detected as having issues of a particular type. By knowing the journaling mailbox and the type of issue encountered, you can use the Archiving Issues screen to view all the messages that fall in this category.

To determine if there are archiving issues:
1. From the Setup section, in Status and Issues, click Journal Folder Status.
   The Journal Folder Status screen appears. Every journaling mailbox monitored by the Archiving Appliance is listed. Within each mailbox group there is an entry for the number of issues. If that number is zero, there are no issues. The number is a link to a page that lists issue types and the number of messages having that type of issue.
2. Click the number.
   The Issue Type screen appears. Note the journaling mailbox name and the issue types.
   You use this information to view specific messages using the Archiving Issues screen.

To view a list of messages in a journaling mailbox that have a specific issue type:
1. From the Setup section, in Status and Issues, click Archiving Issues.
   A dropdown list becomes active, allowing you to choose a journaling mailbox.
2. Choose a journaling mailbox that has an archiving issue.
   The Archiving Issues screen appears.
3. Select an issue type from the Issue Type list.
   A list of messages matching the issue type appears or, if you choose Message Class Type in the Issue Type list, the Message Class Type list appears. A list of messages appears after you choose a message class type from the list.
4. Select a message and review it to determine what caused the issue.
   You may want to view multiple messages in an attempt to determine the cause of the issue.
5. If you wish to submit the message to MessageLabs for further analysis, click Submit Message on the toolbar.
   A screen appears, allowing you to select the amount of information you submit. For reasons of privacy, you may not want to submit the message body. Since a message body rarely causes an issue, removing it from the information you send to MessageLabs should not hinder the analysis.
6. Check the items you want to submit, and add comments if necessary.
   Include those items that you suspect are the cause of the issue.
7. Click Submit.
   The message is submitted to MessageLabs for analysis. A screen appears that confirms that the message has been submitted for evaluation.
8. If necessary, continue to analyze other issues. Use the Journal Mailbox and Issue Type lists to choose the issue you want to analyze next.
<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access rights</td>
<td>Rights that give users access to specific MessageLabs Email Archiving Service functions. Set by making users members of specific MessageLabs Email Archiving Service security groups in Active Directory.</td>
</tr>
<tr>
<td>Appliance</td>
<td>See Archiving Appliance.</td>
</tr>
<tr>
<td>Archive</td>
<td>MessageLabs Email Archiving Service function that stores electronic messages for specific retention periods.</td>
</tr>
<tr>
<td>Batch Search</td>
<td>Service that allows batch searching only, placing the search results 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. Rules can apply to departments.</td>
</tr>
<tr>
<td>Journaling Mailbox</td>
<td>Mailbox that records messages flowing into and out of an organization. Accessed by Archiving Appliance to retrieve messages for processing.</td>
</tr>
<tr>
<td>MessageLabs Network</td>
<td>Where data resides, in encrypted format.</td>
</tr>
<tr>
<td>Purpose</td>
<td>Archiving Appliances perform specific purposes (archiving, user interface, exporting, stubbing). Any appliance can serve all or some of these purposes.</td>
</tr>
<tr>
<td>Real-Time Search</td>
<td>Service that allows searching in real-time, placing the search results in the results list for further analysis.</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>Security group</td>
<td>MessageLabs Email Archiving Service-specific Active Directory group. Used to control access to MessageLabs Email Archiving Service functions.</td>
</tr>
<tr>
<td>Stub</td>
<td>Method of reducing storage size by replacing stored attachment with link to original attachment stored in the archive.</td>
</tr>
<tr>
<td>Stubbing</td>
<td>Optional functions that manage mailbox sizes by replacing large attachments with links to the archive.</td>
</tr>
<tr>
<td>Stubbing Policy</td>
<td>A policy used to determine what mailboxes, and what folders in those mailboxes, to stub, and what size of attachments to stub.</td>
</tr>
<tr>
<td>Stubbing time window</td>
<td>Configured time period during which stubbing takes place.</td>
</tr>
<tr>
<td>Supervision</td>
<td>Optional functions used to design, edit, maintain and perform reviews of messages for acceptable use.</td>
</tr>
</tbody>
</table>
A
access to functions, 39
Active Directory, configuring, 29
appliance
about, 6
changing configuration, 36
choosing purpose, 35
configuring, 33
configuring additional, 35
configuring first, 33
configuring for stubbing, 53
connecting, 32
connectivity, 12
purposes, 13
resetting, 36
using multiple, 15
Archive Discovery Administrators, about, 39
Archive Discovery Users, about, 39
Archive Disposition Users, about, 40
Archive Export Users, about, 39
archive proxy, installing, 37
Archive Report Users, about, 40
Archive Search Users, about, 39
archive, how users use, 9
Archiving Appliance. See appliance
archiving process, about, 27
audit trail, 57
C
configuration
appliance, 33
router or firewall, 12
confirming configuration, 34
corporate proxy server use, 12
E
encryption key
exporting, 35
importing, 35
encryption, about, 11
Exchange journaling
about, 27
how used, 8
Exchange managed folders
configuring, 27
Exchange managed folders, how used, 8
exporting encryption key, 35
exporting messages, about, 9
external access
about, 37
considerations for, 18
scenarios, 18
F
fault tolerance, 37
firewall configuration, 12
H
HTTPS ports, 12
I
importing encryption key, 35
J
journaling mailbox
creating, 22
temporarily suspending, 36
journaling mailboxes
how populated, 8
use of, 7
journaling, configuring, 25
L
legal holds, about, 9
load balancing, 37

Copyright © MessageLabs 2009
managed folders. See Exchange managed folders
MessageLabs Network, about, 6
multiple appliances, 15

network requirements, 12

organizational forms library for stubbing, 50
Outlook Folder Creator
  running, 45
  scheduling, 46
  setting up accounts for, 43
overview of features, 4
OWA server, setting up, 38

Policy Managers, about, 40
product architecture, 14

requirements, system, 6
router configuration, 12

searching, about, 9
security groups
  about, 39
  configuring, 31
setup steps, 20
stubbing
  about, 47
  account, 48
  configuration steps, 49
  configuring appliance for, 53
  disabling, 56
  enabling, 56
  form, 48
  form, publishing, 52
  how used, 8
  organizational forms library for, 50
  policy, 53
  policy, about, 48
  process, 47
  publishing forms for, 52
  user account for, 49
  user view of, 10
Supervision Report Users, about, 40
Supervision Reviewers, about, 39
Supervision Senior Reviewers, about, 39
supervision, about, 10
system requirements, 6

technical support, 3
troubleshooting
  archiving, 60
  common problems, 57
  User Directory, 58

URL for user access, 20
user access, 39
user access URL, 20
user account for stubbing, 49
user account, for journaling mailbox, 22
User Managers, about, 40
www.messagelabs.com
info@messagelabs.com

Freephone UK
0800 917 7733

Toll free US
1-866-460-0000