



MessageLabs®
Now part of Symantec

Be certain

Email Continuity Administrator Guide

For Lotus Notes® Environments

Licensed Customer Confidential

Legal Notices

Copyright© 1998-2009 Dell MessageOne, Inc. All Rights Reserved.

Information in this document is subject to change without notice. All names of companies, organizations, persons, or other entities, and all sample data used in content and examples is fictitious and not meant to represent any real company, organization, person, or actual data.

No part of this publication may be reproduced, modified, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise without the prior written permission of Dell MessageOne, Inc. Reproduction prohibitions do not extend to distribution among the employees of licensed customers or for use in activities conducted by Dell MessageOne partners in the course of sales, marketing, training, or support.

MessageOne is a registered trademark and “Business Continuity that makes Business Sense,” EMS, SyncManager, RedirectorSink, RedirectorController, RecoveryManager, and OneSwitch are trademarks of Dell MessageOne, Inc.

MessageLabs® and the MessageLabs logo are trademarks of MessageLabs Ltd.

Research in Motion, RIM, and BlackBerry are trademarks/registered trademarks of Research in Motion Limited.

All other trademarks are the property of their respective owners.

This product uses certain third-party software. Relevant licensing information is provided in the MESSAGEONE LICENSE file in the installation directory.

Dell MessageOne® EMS Email Continuity, offered by MessageLabs as Email Continuity is the sole intellectual property of Dell MessageOne, Inc., and includes proprietary technology for which Dell MessageOne, Inc., has applied for one or more U.S. patents.

Table of Contents

| | |
|---|------------|
| Task Reference | v |
| About This Book | vii |
| Intended Audience | vii |
| Viewing the Document | vii |
| Conventions | viii |
| Product Documentation | viii |
| 1 About the Service | 1 |
| About Email Continuity | 1 |
| 2 Preinstallation | 5 |
| Communications Requirements | 5 |
| Networking Requirements | 5 |
| Firewall Requirements | 6 |
| Proxy Requirements | 6 |
| SMTP Message Gateway Requirements | 6 |
| Gateway Requirements | 6 |
| Mail Routing Inbound—Store and Forward | 7 |
| Mail Routing—Outbound During Activation | 8 |
| Hardware Requirements | 8 |
| Software Requirements | 8 |
| Service Software | 9 |
| Supported Operating Systems | 9 |
| Supported Messaging Software | 9 |
| Server Software Requirements | 10 |
| Lotus Notes Environments | 10 |
| Account Requirements | 11 |
| Lotus Environments Account Requirements | 11 |
| Virtualization | 11 |
| 3 Installation and Configuration | 13 |
| Installing Service Software | 13 |
| Configuring the SyncManager | 16 |
| 4 Administration | 21 |
| Logging Into the Administration Console | 21 |
| Administration Console Home | 22 |
| Readiness Checks | 24 |
| User Administration | 24 |
| Searching User Information | 25 |
| Resetting User Passwords | 26 |
| Resetting an Individual User's Password | 26 |
| Resetting Multiple Passwords By Template | 26 |
| Resetting Multiple Passwords by CSV Import | 28 |
| Changing Status for Multiple Users | 31 |
| Updating a User's Contact Information | 32 |
| Defining User Sets | 32 |
| Assigning Super Administrator Privileges | 33 |
| Assigning Email Continuity Administrator Privileges | 35 |
| Assigning Help Desk Privileges | 36 |
| Reviewing Login Status | 37 |
| Exporting Users' Contact Information | 39 |
| Excluded Users | 40 |

| | |
|---|-----------|
| Enabling BlackBerry Forwarding | 42 |
| Configuring a BlackBerry for Use with BlackBerry Forwarding | 42 |
| Mailboxes and Aliases | 44 |
| Adding Mailboxes (Users) Manually | 44 |
| Creating Aliases | 44 |
| Mailing Lists | 45 |
| Notification | 45 |
| Welcoming New Users | 45 |
| Sending Reminders | 48 |
| Managing Fault Alerts | 50 |
| Managing Transition Alerts | 50 |
| Sending Custom Notifications | 51 |
| Viewing Audit Reports | 52 |
| Activation Reports | 52 |
| Test Reports | 53 |
| Modifying System Settings | 53 |
| Configuring Email Routing | 53 |
| Routing for Forwarded Mail | 54 |
| Routing for Outbound Mail During an Activation | 54 |
| Changing the Email Disclaimer | 55 |
| Sync Notify Settings | 55 |
| Customizing the Home Page | 56 |
| Customizing the Welcome Process | 57 |
| Changing Your Account Settings | 58 |
| Accessing Your Mailbox | 58 |
| Viewing Undeliverable Mail in the Dropbox | 58 |
| Changing Your Password | 58 |
| Testing Email Continuity | 59 |
| 5 Activation | 61 |
| Activating Email Continuity | 61 |
| 6 Recovery | 63 |
| Starting Recovery from an Activation | 63 |
| Restoring Mail to Users' Mailboxes | 64 |
| Completing Recovery from an Activation | 72 |
| Index | 75 |

Task Reference

| | |
|---|----|
| To prepare Lotus Notes Environment for use with Email Continuity: | 10 |
| To install service software: | 13 |
| To launch the SyncManager Setup Wizard manually:..... | 16 |
| To configure the SyncManager: | 16 |
| To configure distributed synchronization with SyncManager: | 19 |
| To log into the Administration Console:..... | 22 |
| To search user information:..... | 25 |
| To reset a user's password: | 26 |
| To change multiple users' passwords: | 26 |
| To create a password import CSV file: | 28 |
| To import passwords by CSV file: | 30 |
| To change status flags for users: | 31 |
| To edit a user's contact information:..... | 32 |
| To create a user set:..... | 32 |
| To create a super administrator:..... | 34 |
| To remove super administrator privileges: | 35 |
| To assign administrative privileges to an account: | 35 |
| To remove administrative privileges from an account: | 36 |
| To grant a user Help Desk privileges: | 36 |
| To remove Help Desk privileges from an account:..... | 37 |
| To review login status:..... | 37 |
| To generate a CSV spreadsheet of emergency contact data for all users: | 40 |
| To exclude a user: | 40 |
| To remove individual users from the Excluded list (reinstate them in the system):..... | 41 |
| To remove multiple users from the Excluded list (reinstate them in the system): | 41 |
| To set up a BlackBerry device:..... | 43 |
| To add a mailbox (user) to Email Continuity:..... | 44 |
| To create an alias: | 44 |
| To view mailing lists and members of each list: | 45 |
| To send a welcome message to one or more users:..... | 47 |
| To automatically send welcome messages to new users:..... | 48 |
| To send a reminder: | 49 |
| To add a user to the fault alerts list: | 50 |
| To remove a user from the fault alerts list: | 50 |
| To add users to the transition alerts list:..... | 51 |
| To remove a user from the transition alerts list: | 51 |
| To send a custom message: | 51 |
| To view an Activation report: | 53 |
| To view a Test report:..... | 53 |
| To configure the path for forwarded mail:..... | 54 |
| To configure the path for outbound mail during an activation:..... | 54 |
| To add disclaimer text to the end of each message sent by the service: | 55 |
| To configure the user/ mailing list deletion percentage at which a warning message is sent: | 55 |
| To hide the Preferences section of the Home page: | 56 |
| To enable individual links in the Preferences section of the Home page: | 56 |
| To change the text displayed to end users in each state of Email Continuity: | 57 |
| To select pages to include in the welcome wizard: | 57 |
| To access your webmail account during an activation: | 58 |
| To view undeliverable mail during an activation: | 58 |
| To change your password: | 58 |

| | |
|---|----|
| To start a test of Email Continuity:..... | 59 |
| To start recovery from a test:..... | 60 |
| To activate Email Continuity: | 61 |
| To initiate recovery: | 63 |
| To restore email after an activation: | 65 |
| To complete recovery from an activation:..... | 73 |

About This Book

Intended Audience

This book describes actions reserved for those with administrative privileges. Its content assumes that you are an administrator for the product and have a strong general knowledge of system and network administration. Depending on how the product is configured for your organization, some features described in the documentation may not be available to you.

Viewing the Document

This document is provided as an Adobe Portable Document Format (PDF) file. For best results, use Adobe Acrobat Reader software, v6.0 or later, for viewing this document. You can download the latest version of this application at no cost from Adobe Systems, Inc. (www.adobe.com).

Within the document, cross-references and web site addresses are active hyperlinks. These links display as blue, underscored text. Click the text of any cross-reference to go to the referenced location within the document. To return to the previous location, use the **Back** button in the PDF reader interface.

Click any web link to launch your default web browser and go to the indicated web site location.

Conventions

The documentation uses certain typographical conventions to make references to product elements easier to recognize and understand. These are described in the following table.

Table A-1 Typographical Conventions

| Display Format | Definition | Examples |
|----------------------------------|--|---|
| blue, underscore | A hyperlink to either another location within the document or to a web site. | For more information, see "Viewing the Document" on page vii . |
| bold | Name of a screen, section, pane, box, or option in the user interface. | On the Select Permissions page, locate the Access Info pane of the User Account panel. |
| | The name of an executable file. | To begin the installation, double-click setup.exe . |
| <i>Bold italic</i> | The name of a menu, button, or tab. | From the Start menu, select Programs . |
| serif | An entry you must type manually. | At the command prompt, type <code>cmd</code> . |
| | A value you type in a box or select from a list. | From the Filter drop-down list, select <code>Starts with</code> . |
| | A field value that appears in the user interface. | The Source field now reads <code>Imported from File</code> . |

Product Documentation

The following documentation is available for Email Continuity:

- *Email Continuity Administrator Guide*
This book is a comprehensive document for installing, configuring, and administering Email Continuity.
- *Email Continuity Online Help*
This material explains to users how to configure and update their user profiles, and use the webmail interface to read and send email.
- Location-Specific Network Settings
This document provides IP addresses and Message Transfer Agent (MTA) information based on the location of the MessageLabs data center.
For the latest version of any document, contact Support.

1 About the Service

About Email Continuity

Email Continuity is an alternative email service that takes the place of your primary email system during an outage. When the service is activated, users can access their email through an easy-to-use web-mail interface.

Email Continuity consists of the following components:

Table 1-1 Components

| Component | Description | Location |
|------------------|---|---------------------------------------|
| Email Continuity | A hosted, backup email system. The process of switching users to the backup system is called <i>activation</i> or <i>activating the service</i> . | Hosted at the MessageLabs data center |
| SyncManager™ | Software that synchronizes directory and contact information. | Installed in customer's environment. |
| RecoveryManager™ | Software that, when run, restores mail into the primary mail system after activation. This process is called <i>recovery</i> . | Installed in customer's environment. |

Data transfer between your organization's email system and the Data Center is shown in [Figure 1-1](#).

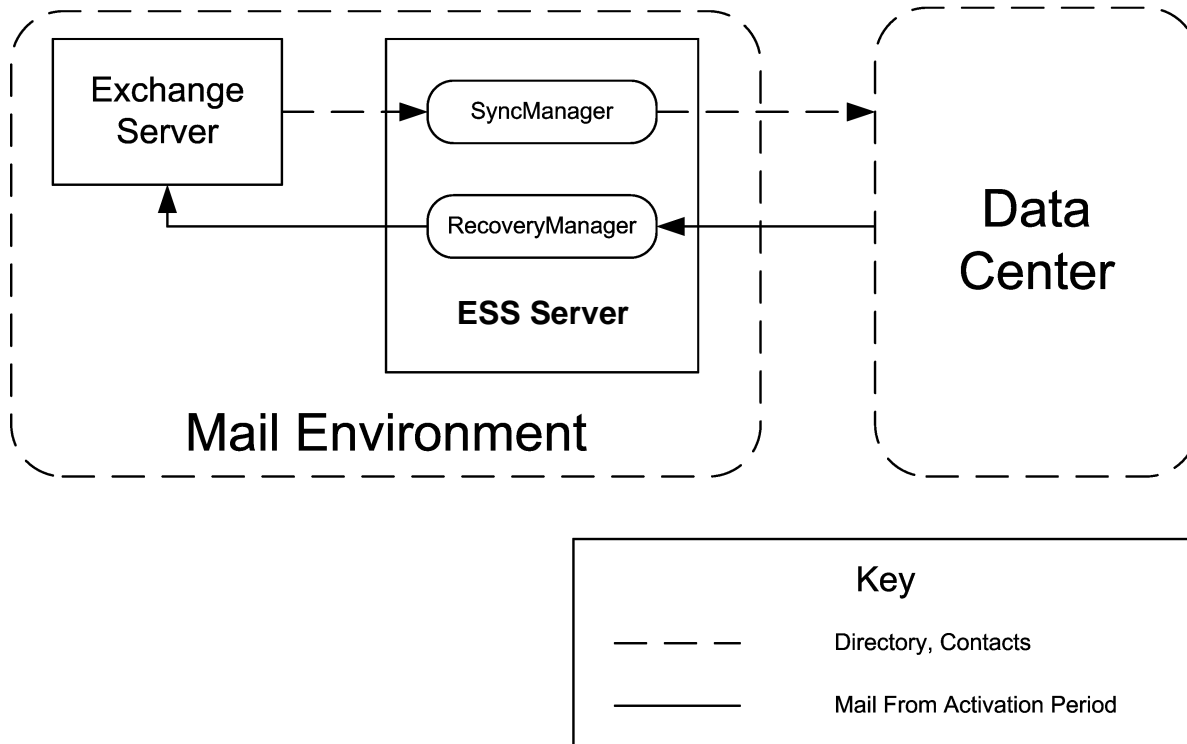


Figure 1-1 Email Continuity Data Transfer

Once the necessary components have been installed, use of the service is simple. Prior to an activation of the service, the SyncManager sends directory information to the data center. During an activation, users can send and receive their email online through the webmail interface. After the primary email system has been restored, the RecoveryManager imports the email messages sent and received

during the activation period into the primary mail system. Email Continuity is always in one of three states: READY, ACTIVE, or RECOVERY. These are shown in [Figure 1-2](#).

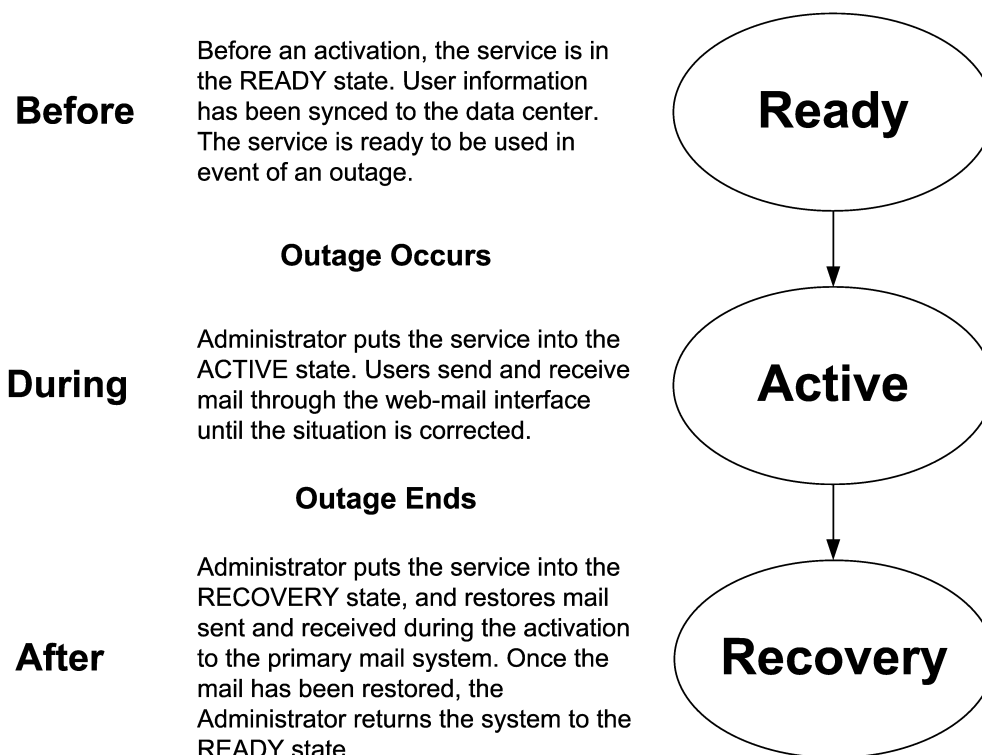


Figure 1-2 Email Continuity States

To change the text that appears to users on the web-mail Home Page in each of the three states, see ["Customizing the Home Page" on page 56](#).

2 Preinstallation

Before you install service software, make sure that your servers meet the installation requirements and that you have all the tools and information described in this chapter.

Communications Requirements

This section outlines the networking, firewall, proxy, and email gateway requirements.

NOTE **Location-specific Settings**

Communication requirements involve settings specific to a data center, such as Internet Protocol (IP) addresses and Message Transfer Agents (MTAs). When any of the following sections refer to *location-specific settings*, refer to the Network Settings document provided to you by Support.

CAUTION **MX Record Configuration**

MessageLabs does **not** configure or maintain your MX records. Ensure that your MX records are correctly configured so that messages are correctly routed through the Email Continuity service during an outage of your primary mail system. **If your MX records are incorrectly configured, mail could be delayed or lost during an activation.**

Your Support representative can assist you in setting up and testing your MX record configurations. Inform your Support representative immediately if there have been any changes in your system environment that could impact mail flow to and from the Email Continuity service.

Support recommends that you run a test activation of the Email Continuity service quarterly to validate your MX record configurations and mail routing results.

Networking Requirements

The networking requirements are:

- 1 The machine on which you install the SyncManager (called the *primary controller* or *ESS server*) must have internet access through secure hypertext transfer protocol (HTTPS), using port 443 outbound.
- 2 Connection to the internet and Microsoft Internet Explorer (v6 or 7) for performing functions in the Administration Console. If you are installing on a newly provisioned machine, run the Microsoft Internet Connectivity Wizard before you install service software.

- 3 For end users accessing the web-mail interface, supported browsers are Internet Explorer (v6 or 7) or Firefox.
- 4 Domain name service (DNS) must be configured to connect to the Domino servers the service supports. However, you cannot install the SyncManager component on a Domino server.

Firewall Requirements

Most organizations' networks include a firewall that restricts both outbound and inbound traffic based on specific rules. Make any necessary adjustments to your firewall's configuration to ensure that it allows outbound traffic for the ESS server to the location-specific IP addresses on port 443.

Proxy Requirements

If you use a proxy server, set the proxy server rules to allow communication from the ESS server to the location-specific IP addresses provided by Support.

SMTP Message Gateway Requirements

If you use an SMTP gateway server, ensure its configuration accepts inbound messages from the location-specific IP addresses provided by Support. If your gateway server blocks all inbound messages that use one of your domains in the **From:** field, add an exception to this rule to accept messages originating from the location-specific IP addresses. For example, if your domain is company.com and you block all inbound mail with an SMTP address of anything@company.com as spam, the exclusion list for this policy should include the location-specific IP addresses.

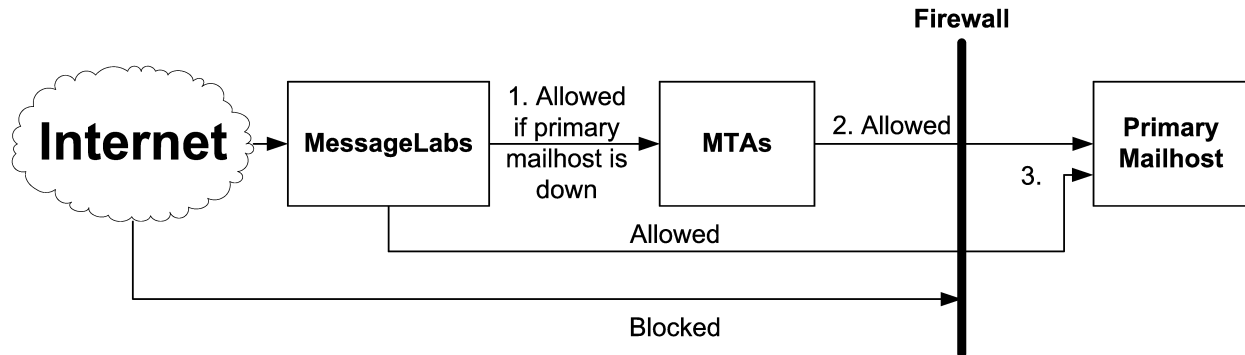
Gateway Requirements

Configure your gateway to failover automatically to the location-specific message transfer agent (MTA).

Configure your corporate mailhost to:

- 1 Accept inbound SMTP connections from the IP addresses provided by Support.
- 2 Allow the IP addresses provided by Support to be valid sending IP addresses.

Be sure that you provide the hostname or IP address of your mailhost(s) to Support so that the data center can be configured to send email directly to your organization.



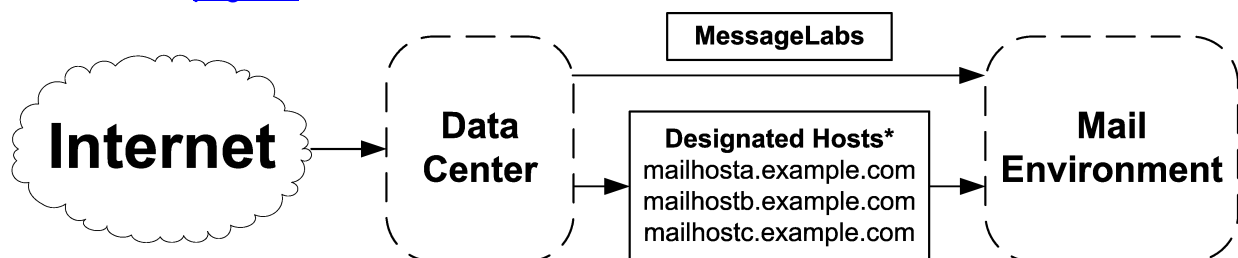
1. Configure MessageLabs to send mail to Email Continuity when the primary mailhost is down by listing the Email Continuity MTA as a backup mail record within the MessageLabs configuration.
2. Configure Email Continuity to send mail directly to the primary mailhost instead of through the MX record (to prevent mail looping).
3. Configure the firewall to allow inbound SMTP traffic (port 25) for the Email Continuity servers. This rule is the same as the firewall rule that allows inbound mail from MessageLabs.

Figure 2-1 Mail Routing with MessageLabs

Mail Routing Inbound—Store and Forward

If your primary mail system has gone down, and your organization has not activated Email Continuity, MessageLabs performs a *store and forward* service and attempts to deliver your mail.

To configure email routing for inbound mail, see ["Routing for Forwarded Mail" on page 54](#)



*You can designate a series of hosts through which to forward mail.

Figure 2-2 Routing for Inbound (Forwarded) Mail

Mail Routing—Outbound During Activation

When Email Continuity is active, by default it uses the MX records of mail recipients to deliver outgoing mail. However, if your organization uses MessageLabs for outbound services, or you have a need to route outgoing mail through a different host, you can configure the system to use a designated series of hostnames or IP addresses (*hops*) to determine the path your outgoing email takes while Email Continuity is active. To configure the series of hosts, see ["Mail Routing—Outbound During Activation" on page 8](#).

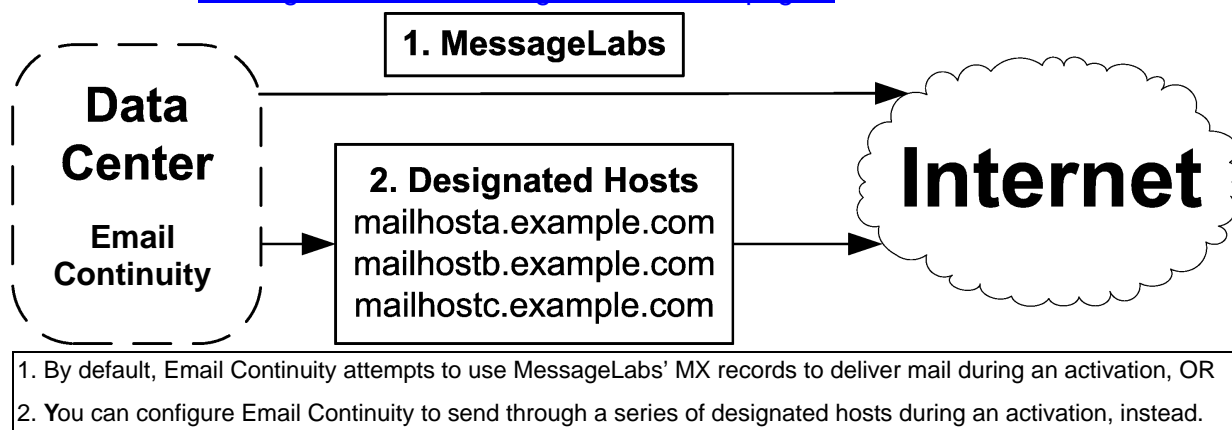


Figure 2-3 Outbound Mail Routing During Activation

Hardware Requirements

Verify that the server you plan to use as the primary controller (the *ESS server*) has the following minimum hardware:

Table 2-1 Minimum Hardware Requirements

| Component | Minimum Required |
|------------|---|
| Processor | Pentium® III, 500 MHz |
| Memory | 256 MB RAM (512 MB recommended) |
| Disk Space | Up to one-half gigabyte, depending on the number of users |

Email Continuity typically does not require a dedicated server.

Software Requirements

Before you begin an installation, you must install each required software component on the ESS server. Which components are required depends on the email environment you use, and which features your organization uses. A Support

representative will provide an appropriate software package, and walk you through the actual installation process when the preinstallation requirements have been met.

Service Software

- 1 **Service software**—Download the install package from the location provided by Support.
- 2 **Service root account username and password**—You must use the *service root account* or a valid *super administrator* account (created by your organization's service root account) for authentication of the SyncManager with the data center servers. If you do not have the service root account username and password, contact Support.

Supported Operating Systems

The ESS server must use one of the operating systems described in [Table 2-2](#).

Table 2-2 Supported Operating Systems

| Server | Operating System | Notes |
|--------------------------------|---|--|
| Email Security Services Server | Windows Server 2003/ Windows Server 2008 | 64-bit is only supported for Windows Server 2008 |

Supported Messaging Software

You must install a supported version of both Lotus server and client software on your mail server. Email Continuity works with Lotus Domino 5.0.11 and later. The supported versions of Lotus Notes client software are:

- Lotus Notes 5.0.11 and later
- Lotus Notes 6 and 7 (all versions)

Server Software Requirements

Lotus Notes Environments

Table 2-3 Software Requirements for Lotus Notes Environments

| Software | Notes |
|---|--|
| .NET Framework v 3.5 SP1 | If not already present on the ESS server, the installation package provided by Support includes this software. After installation, you may need to reboot the computer before you can proceed with the SyncManager Wizard. |
| Lotus Notes Client v5.0.11 or later | For proper operation, install only one instance of the Lotus Notes client server. See below for preparation instructions. |
| Registered Lotus Notes account with a minimum of editor access on all mail files the installation will support. | |

To prepare Lotus Notes Environment for use with Email Continuity:

- 1 Configure a Domino server (if not already done) for use with Email Continuity.
- 2 Install the Notes client software.
- 3 Log in to the client as a user with appropriate permissions for running the product.
- 4 Using the Notes client, log in, configure (if needed), and connect to a Domino server.
- 5 Close the Lotus Notes application.

The Notes client does not need to be running on the machine for the product to function. However, the Lotus Notes account does require a minimum of editor access on the access control list (ACL) of all mail files to be supported by the product.

After you install and setup the Lotus Notes client software, verify proper configuration of name resolution. The product must resolve the names of Domino servers to IP addresses.

- 6 If you use Lotus Notes 6, you must follow additional setup steps to work around a known installation problem resulting from improper registration of a Lotus Notes dynamic-linked library (DLL) file. The workaround process for this requires that you manually register the DLL file. To do this

- a. Open a command prompt window.
- b. At the command prompt, change to the Lotus Notes program directory. For example, to change directories to the default install location for Lotus Notes, type:

```
cd D:\Program Files\Lotus\Notes
```

- c. Click **Enter**.

NOTE Lotus Tech Note on DLL Registration Issue

Refer to Lotus Tech Note 1112239 for additional information on the Lotus Notes 6 DLL registration issue.

- d. At the command prompt, type :

```
regsvr32 nlsxbe.dll
```

- e. Click **Enter**.

Account Requirements

Lotus Environments Account Requirements

Table 2-4 Account Requirements, Lotus Environments

| Account | Notes |
|---------------------|---|
| ESS Service Account | A <i>service account</i> , under which all service processes run, must be created on the ESS server. This group must be a member of the domain and the local administrator group on the ESS server. |

Virtualization

Email Security Services can be virtualized under the following conditions:

- 1 Email Continuity is supported on the VMware Infrastructure virtualization platform. Other platforms may function properly but are not supported.
- 2 Your virtual environment must adhere to the same requirements as a non-virtual environment, as defined in the following sections:
 - ["Communications Requirements" on page 5](#)
 - ["Hardware Requirements" on page 8](#)

- ["Software Requirements" on page 8](#)
- 3 When you build each virtual machine (VM), you must use the following configurations:
 - Under **Network Type**, choose **Bridged Networking**.
 - Under **Specify Disk Capacity**, check **Allocate All Disk Space Now**.
 - 4 After your VM is built, adjust its memory allocation to reflect the requirements specified under ["Hardware Requirements" on page 8](#).

3 Installation and Configuration

Installing Service Software

To install the software, you must log in as the *service root* account (assigned by Support), or as a *super administrator* account (created by your organization's service root account). If you do not have the root account login and password information, contact Support.

The software uses an InstallShield Wizard. The wizard installs:

- .NET v. 2.0 SP1, if not already installed
- SyncManager
- RecoveryManager

The appropriate software package for your installation is provided to you by Support.

WARNING Upgrading to 6.0 or later versions

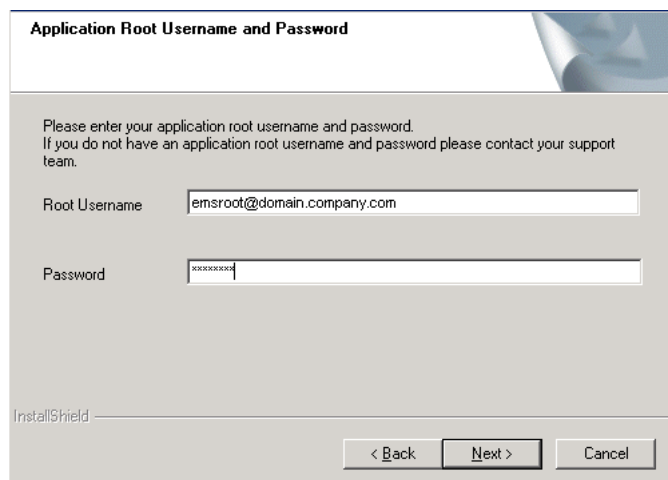
If you are upgrading to 6.0 or 6.1 from any 5.x version of the software, you must first remove (uninstall) all Email Continuity and Historical Mail (ActiveMailbox) software prior to installing the 6.x version.

For more information, or assistance with the upgrade, call Support.

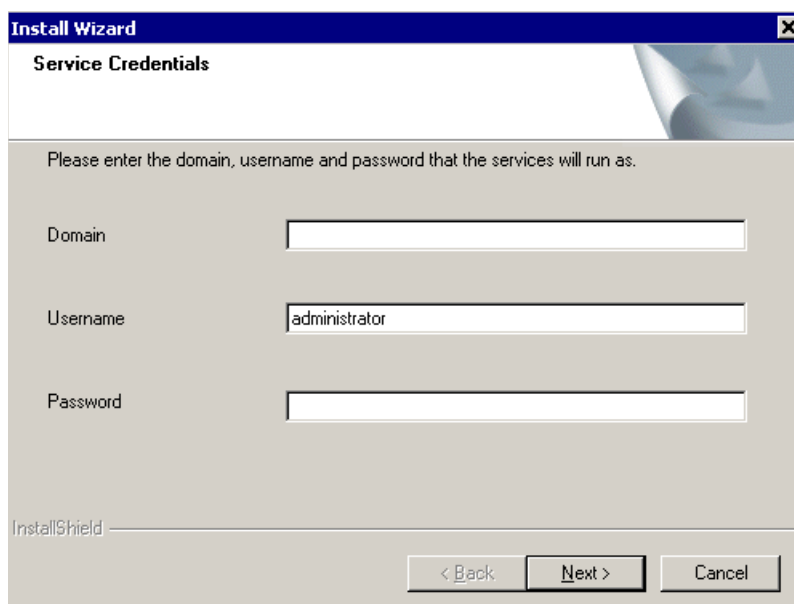
To install service software:

- 1 On the ESS server, log in using the service account you created to meet preinstallation requirements.
- 2 Open the installation software folder, and double-click the **setup.exe** file.
- 3 If the .NET Framework software needs to be installed, the **Microsoft .NET Framework Setup Wizard** appears.
 - a. In the **Welcome** dialog box, click **Next**.
 - b. In the **End-User License Agreement** dialog box, review the software license for the .NET Framework application. To agree to the license terms and continue with installation, select the **I accept the terms of the License Agreement** check box, and then click **Install**.
 - c. In the **Setup Complete** dialog box, click **Finish**.
 - d. Reboot the computer if the installation requires it. After the reboot, the installation process automatically restarts.
- 4 The InstallShield Wizard Welcome window appears. Click **Next**.

- 5 In the **Application Root Username and Password** window, log in with the user name and password of the service root account or a valid super administrator account, then click **Next**.



- 6 In the **Service Credentials** dialog box, identify the service account that accesses your primary email environment, and assign the account proper domain permissions. Because you logged in with this account, the installation process automatically populates the **Domain** and **Username** fields with the current domain account information. To complete the login process and set necessary domain permissions:

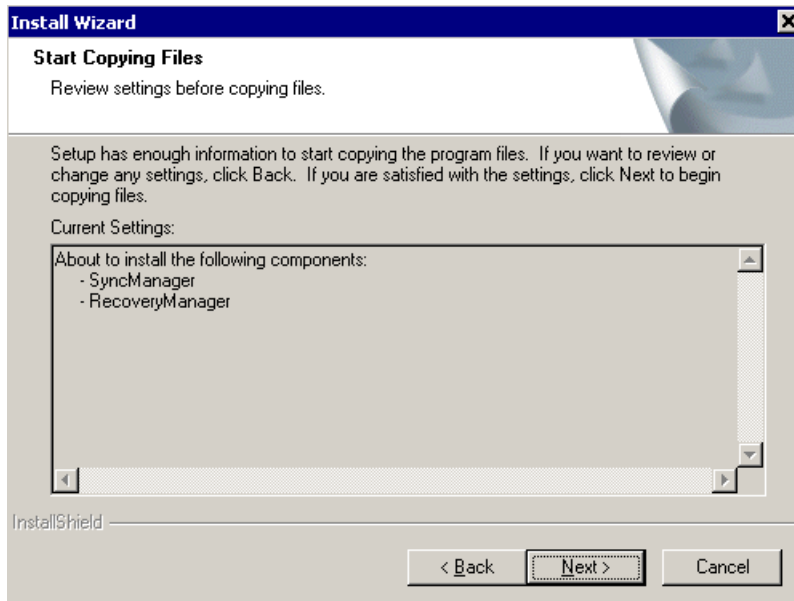


- a. Verify the information in the **Domain** box or, to log in under a different account, enter the appropriate domain information. MessageLabs strongly recommends that you do not use a different account.
- b. Verify the information in the **Username** box or, if needed, change it to correspond with the information in the **Domain** box.
- c. In the **Password** box, enter the password for the account.

d. Click **Next**.

- 7 In the **Destination Folder** dialog box, set the destination folder for installation files. To accept the default install location, click **Next**. To install the product in a different location, click **Browse**, select an alternate location, and then click **Next** in the **Destination folder** dialog box.

- 8 In the **Start Copying Files** dialog box, click **Next**.

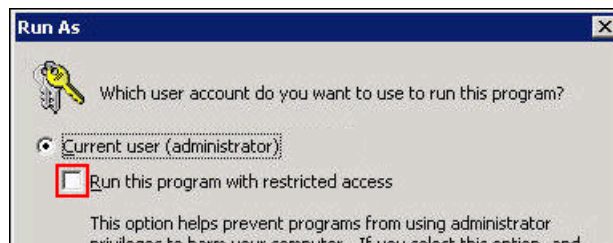


The **Setup Status** window displays installation progress.

- 9 Email Continuity cannot function until you configure the SyncManager. MessageLabs recommends that you configure SyncManager as soon as you complete the installation. To do this, click the **Start SyncManager to configure ESS** check box, then click **Finish**.

NOTE Run With Full Access

If a **Run As** dialog box appears after you click **Finish**, you *must uncheck* (deselect) the box that reads *Run this program with restricted access*. If you do not uncheck this box, the program will not launch properly. If this occurs, relaunch the program manually from the **Start** menu.



-
- 10 If the SyncManager has never been run before, a prompt appears requesting your approval to continue. Click **OK**.

- 11 At this point, the installer might ask you to reboot the system. If the Configure SyncManager Wizard does not appear immediately after rebooting, you can launch it manually, as described on page 16.

Configuring the SyncManager

A SyncManager Setup Wizard guides you through the configuration process, in which you describe your email environment and determine how often the service should synchronize data with your email system. The configuration process performs an initial synchronization. After this process completes, Email Continuity is ready for activation in the event of an outage.

SyncManager synchronizes Directory information, as well as Contacts data if it is stored on the email server.

You can configure the SyncManager either when prompted, at the completion of product installation, or by launching the SyncManager Setup Wizard manually.

To launch the SyncManager Setup Wizard manually:

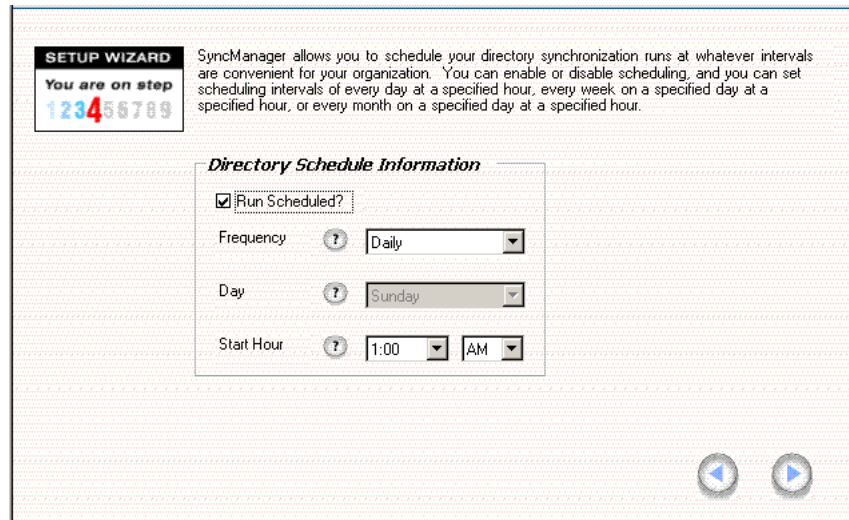
- 1 From the **Start** menu, select **Programs > MessageLabs > SyncManager**.
- 2 The splash screen for the SyncManager displays. A **SyncManager** dialog box also displays. Click **OK**.

To configure the SyncManager:

- 1 Log in to the SyncManager Setup Wizard. You must use the user name and password for the service root account or a valid super administrator account.
- 2 Provide information on your Domino Servers.
 - a. In the **Lotus Notes Settings** section of the window:
 - (1) Enter the name of the **Domino Server** you will use for the directory synchronization.
 - (2) Enter the **Password** for the user ID that is configured in Lotus Notes client on this computer.
 - b. To turn off synchronization of mailing lists (distribution lists), clear the check box at the bottom of the window.
 - c. Click the **Next** arrow.
- 3 The Setup Wizard registers the SyncManager instance with the Email Continuity server. Click **Next**.

4 Schedule directory synchronization.

The **Directory Schedule Information** window allows you to determine how often the SyncManager synchronizes (or 'syncs') directory data with the data center.

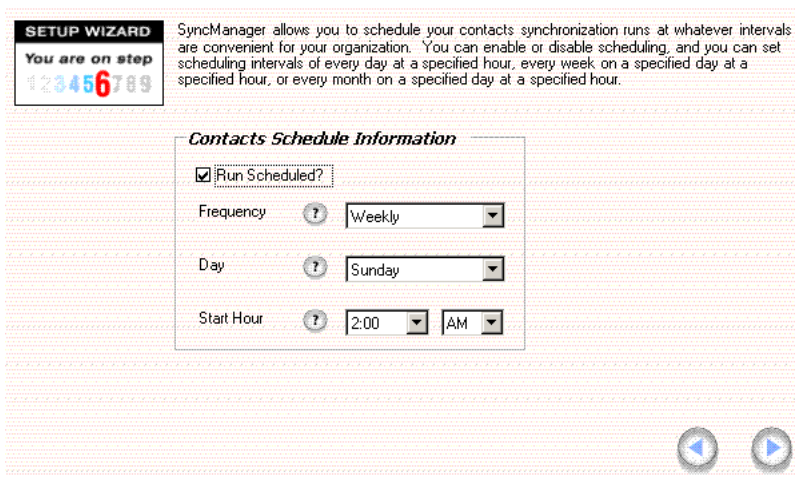


NOTE Actual Synchronization Start Time

When you schedule synchronization processes the actual process runs sometime within the Start Hour you specify.

- a. MessageLabs recommends that you run directory syncs on a regularly scheduled basis. If you do not want your selections for the directory sync process to run regularly, clear the **Run Scheduled?** check box.
 - b. Select a **Frequency**, including **Day** and **Start Hour**. Indicate whether the start hour is AM or PM. (Remember, noon is 12:00 PM and midnight is 12:00 AM.)
 - c. Click the **Next** arrow.
- 5 Identify Lotus mail file settings. The configuration wizard automatically detects the Lotus Notes mail file settings, based on the information you provided.
- Click the **Next** arrow.

- 6 In the **Contacts Schedule Information** dialog box, schedule the synchronization of users' contact data. Because this process is more intensive than the directory synchronization, you should schedule it for non-peak-load times and, preferably, weekly frequency. The process does not modify any of the data.



- a. Select a **Frequency**, including **Day** and **Start Hour**. Indicate whether the start hour is AM or PM. (Remember, noon is 12:00 PM and midnight is 12:00 AM.)
- b. Click **Next**.

NOTE **Avoid Sync Process Overlap**

Schedule directory and contact synchronization processes so that they do not overlap. Allow sufficient time for one to complete before the next begins.

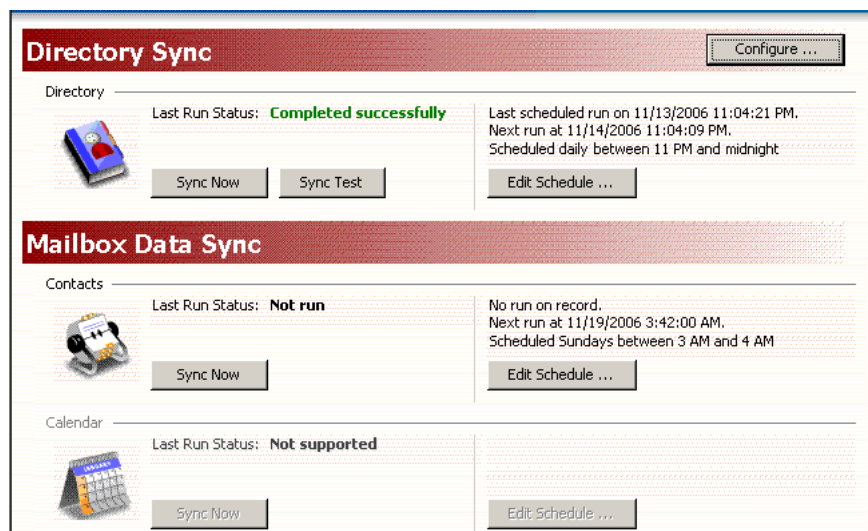
- 7 Calendar data synchronization is not available with the Lotus Notes platform. In the **Calendar Schedule Information** window, click the **Next** arrow.
- 8 To perform the initial Directory data synchronization between SyncManager and the data center, click the **Next** arrow.
- 9 A **Directory Sync Status** dialog box provides information about the progress of the initial synchronization. Depending on the size of your user base, the process may take a few minutes

When the synchronization completes, SyncManager creates a user account for each current user in your primary email system. The final window's Status message displays the number of accounts created, as well as additional information. Note the total number of accounts created. This should be approximately equal to the total number of mailboxes in the supported system or systems. If there is a difference that is more than you

expected, you may need to exclude mailboxes that are for resources (such as conference rooms) rather than for people. For information on excluding mailboxes, see ["Excluded Users" on page 40](#).

Click the **Next** arrow.

- 10 The SyncManager is ready for use. Click the **Next** arrow to launch the SyncManager summary screen.



If other synchronizations are available to you, you can run them at this time. After you have configured the SyncManager, you should set a deletion threshold percentage so that a fault alert message is sent when the set percentage of users or distribution lists is exceeded. See ["Sync Notify Settings" on page 55](#) for more information.

If you are using several Exchange servers and Email Continuity controllers, you can configure SyncManager to specify which Exchange servers are synched by which Email Continuity controller. This is called *distributed synchronization*.

To configure distributed synchronization with SyncManager:

- 1 On the server that is your primary controller, open SyncManager. From the **Start** menu, select **Programs > MessageLabs > SyncManager**.
- 2 Click the **Configure** button. The **Edit Sync Properties** window appears.
- 3 Click the **Distributed** tab.
- 4 Use the **Add** and **Remove** buttons to move Exchange servers from the **Server List** to the **Included Servers** list. Servers in the Included Servers list will be synchronized by this controller.
- 5 Click **Save**.
- 6 Repeat this process for the secondary controllers in your configuration.

4 Administration

This chapter covers the following topics:

- ["Logging Into the Administration Console" on page 21](#)
- ["Administration Console Home" on page 22](#)
- ["User Administration" on page 24](#)
- ["Enabling BlackBerry Forwarding" on page 42](#)
- ["Mailboxes and Aliases" on page 44](#)
- ["Mailing Lists" on page 45](#)
- ["Notification" on page 45](#)
- ["Viewing Audit Reports" on page 52](#)
- ["Modifying System Settings" on page 53](#)
- ["Changing Your Account Settings" on page 58](#)
- ["Testing Email Continuity" on page 59](#)

Logging Into the Administration Console

The Administration Console is available through a web-based application. The web address (URL) for the Administration Console is provided to you by Support. You can log into the Administration Console with the following types of Email Continuity privileges:

- **Email Continuity Service Root**—There is only one service root account. The user name and password for this account are provided to you by Support.
- **Super Administrator**—Users with service root permissions or super administrator permissions can create super administrator accounts. Users with super administrator permissions can perform the same Email Continuity functions as the service root account. See ["Assigning Super Administrator Privileges" on page 33](#).
- **Email Continuity Administrator**—Users with service root permissions or super administrator permissions can create Email Continuity administrator accounts. Email Continuity administrators can perform all of the functions in the Administration Console except those reserved for super administrators and the service root account. See ["Assigning Email Continuity Administrator Privileges" on page 35](#).

CAUTION Protect the Service Root Account

The Administration Console keeps detailed log entries that record the usernames of individuals who initiate critical activities. For this reason, Support strongly recommends that you use the Administration Console to grant Super Administrator privileges and Email Continuity Administrator privileges to appropriate accounts rather than sharing the service root account.

To log into the Administration Console:

- 1 Launch a supported web browser and go to the URL provided by Support. The **Log In** page displays.
- 2 Enter the Email Continuity account **Username**.
- 3 Enter the Email Continuity account **Password**.
- 4 Click **Login**.

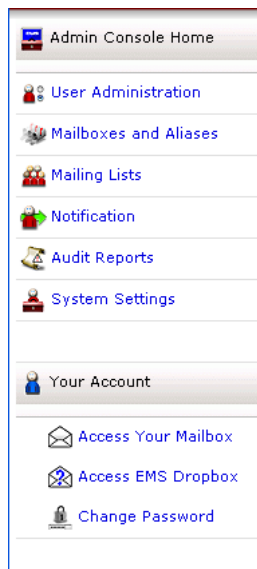
NOTE Some Described Features May Not Appear

Email Security Services configurations vary widely. Depending on the features selected by your organization, some of the functionality described in this chapter may not be visible to you. For more information about obtaining a documented feature, contact Support or your account representative.

Administration Console Home

The Administration Console provides status and readiness information about the environment, enables activation in the event of an outage or for testing purposes, and provides for creation of an email archive to restore email after failback to the primary mail system.

The left column of the Administration Console contains a navigation menu, from which you access all the administrative features of the service.



The buttons in the navigation menu vary according to which products and features your organization has selected and according to the level of access your user account is granted. Some features described in this manual may not appear.

The Administration Console home page displays the sections described in [Table 4-1](#).

Table 4-1 Administration Console Home Page Sections

| Section Name | Description |
|-----------------|--|
| Readiness Check | The service monitors the operational readiness of critical components and automatically sends notifications to designated administrators if their components are not working properly. This section includes a detailed status list for critical components. |
| User Statistics | This section provides data on the number of mailboxes and contacts discovered by SyncManager, and provides statistics on the number of users that have been welcomed. |
| Current State | This section contains controls that activate and recover Email Continuity. When the service is active, this section displays the status of affected users, servers, or both users and servers. |
| Current Tests | This section contains controls that initiate and complete tests of Email Continuity. When a test is active, it displays the status of affected users, servers, or both users and servers. |
| Activity Log | This section displays the status of tasks that are currently running, as well as tasks that completed within the last 24-hour period. Examples include sending notification messages, updating mail routing configuration, or purging old messages from the webmail system after a completed recovery process. |

Readiness Checks

TIP Readiness Check Information Display

If all entries in the readiness checklist are positive, the list automatically collapses. However, if any element requires attention, it automatically expands. Click **Show** to expand the list or **Hide** to collapse the list.

Email Security Services readiness tests monitor the system at all times. When any of the readiness checks marked with an asterisk (*) fails, an email is automatically sent to all email addresses listed in the fault notifications list. (See ["Managing Fault Alerts" on page 50](#) for information on fault notifications.) Readiness checks are described in the following table.

Table 4-2 Readiness Checks

| Readiness Check | Descriptions |
|-------------------------------------|---|
| *Default contacts synchronization | Reports the last time a Contacts synchronization completed successfully. If a scheduled synchronization is more than 12 hours overdue, or if a synchronization reported as failed, this status check fails. The <code>SyncManagerService.log</code> file on the server running the SyncManager in your environment may contain information that is useful for debugging failures. |
| *Default directory synchronizations | Reports the last time a Directory synchronization completed successfully. If a scheduled synchronization is more than 12 hours overdue, or if a synchronization reported as failed, this check fails. The <code>SyncManagerService.log</code> file on the server running the SyncManager in your environment may contain information that is useful for debugging failures. |
| *MX Record (per domain) | If you have chosen to have Email Continuity mail transfer agents (MTAs) listed as an MX record in your public DNS, this readiness check verifies the appropriate DNS entries exist for each domain. If this check fails, verify the appropriate DNS entries exist on all public DNS servers for the domain(s). |

User Administration

Email Continuity users are created by importing existing company information into the system (most commonly with SyncManager) or by manually creating Email Continuity mailboxes. This section describes the functions available to Administrators using the Administrator Console for users that have already been added to the system through one of these methods.

Searching User Information

Search for specific user accounts by using a whole or partial name or email address. In the search results, the **Status** column indicates the user's readiness for activation. The **Action** column provides access to the user's account details and allows you to change the user's password or contact information.

To search user information:

- 1 From the Administration Console, click **User Administration**.
- 2 Click **User Information**. The **User Account Information** screen appears.
- 3 In the **Search Users** field, enter the name or email address; you can use % as a wildcard.
- 4 Click the radio button to select search **By Name** or **By Email address**.

TIP User Search

Below the search box, you can choose to search **By Email address** or **By Name**. Often, full names are not represented in the SMTP email address, making searching By Name more useful. For example, to find Amy Andrews' email address (aandrews@organization.com), using amy as the search string for a **By Email** search would not locate the correct account.

In any search box, you can use a part of the search term, with % as a wildcard.

- 5 Click **Search**. Results appear in the section below the search field.

User Account Information

Search for users by name or email address in order to view activation state, change passwords, or update contact and notification information.

[Reset password for multiple users...](#)

Reset the password for multiple users. Performing this operation represents a security risk as users targeted by this operation will get new passwords which are easily guessed. This operation should not be used on users configured for Windows authentication.

Search Users:

☒ By Email ☐ By Name

| Name | Email Address | State | Action |
|--------------|---|--------|--|
| Beverly Palm | bpalm@docs.devlab.austin.messageone.com | Active | Details Change Password Edit |

- The **State** column indicates the user's readiness for activation.
- The **Action** column provides access to the user's account details and allows you to change the user's password or update contact information.
- To view a user's account information, click **Details**. User account information includes the server on which the account resides, the mailbox store, readiness state, and the user's last login date.

Resetting User Passwords

Email Continuity automatically generates initial passwords for users when you send the Welcome message. There are three methods for resetting a user's password, each covered in its own section:

- ["Resetting an Individual User's Password" on page 26](#)
- ["Resetting Multiple Passwords By Template" on page 26](#)
- ["Resetting Multiple Passwords by CSV Import" on page 28](#)

Resetting an Individual User's Password

To reset a user's password:

- 1 From the **User Information** screen, search for the appropriate user account and locate it in the search results list. On the same line as the user account listing, click **Change Password**.
- 2 The **Change Password** page displays.
- 3 In the **New Password** box, type a new password.
- 4 In the **Confirm Password** box, retype the new password.
- 5 Click **Submit**.

Resetting Multiple Passwords By Template

If enabled by Support, Email Continuity allows you to change passwords for many users at once using a password template based on the users' first and last names or any custom text you provide.

WARNING Potential Security Risk

The multiple password reset feature uses passwords that may be easily guessed.

To change multiple users' passwords:

- 1 From the Administration Console, click **User Administration**.
- 2 Click **User Information**. The **User Account Information** screen appears.
- 3 Click **Bulk update passwords**. The **Select Users** page appears.
- 4 Identify users who need new passwords.
 - a. Use the **User Sets**, **Mailing Lists**, **Servers**, and or **Users** tabs to select users.
 - b. When you find a user or user set, click the check box to select the user or group and click **Add**. The selected user or group moves to the list of users who will get new passwords.

- 5 Click **Next**. The **Enter Password Pattern** page appears.
- 6 Choose the password template pattern to apply for all selected users. This pattern determines what the new password will be for each user.
 - a. To use the recommended pattern, choose **Recommended**. This resets the passwords for all selected users to the following form:
`!Emailaddress_Mmm-YYYY%`
where `emailaddress` is the portion of the user's email address that precedes the `@` sign (first letter capitalized and the rest in lower case), `Mmm` is the 3-digit abbreviation for the current month (first letter capitalized and the rest in lower case), and `YYYY` is the 4-digit year. For example:
 - If you applied this pattern in July 2009 for user `John_Doe@genericorp.com`, the resulting new password would be `!John_doe_Jul-2009%`.
 - If you applied this pattern in August 2010 for user `lilajones@genericorp.com`, the resulting new password would be `!Lilajones_Aug-2010%`.
 - If you applied this pattern in November 2009 for user `samuels.JK@genericorp.com`, the resulting new password would be `!Samuels.jk_Nov-2009%`.
 - b. Choose **Email Username** to reset the passwords for all selected users to the portion of the user's email address that precedes the `@` sign (all lower case). For example:
 - If you applied this pattern for user `John_Doe@genericorp.com`, the resulting new password would be `john_doe`.
 - If you applied this pattern for user `lilajones@genericorp.com`, the resulting new password would be `lilajones`.
 - If you applied this pattern for user `samuels.JK@genericorp.com`, the resulting new password would be `samuels.jk`.
 - c. Choose **Username** to reset the passwords for all selected users to each user's ESS user name.

When you choose this option, the **Default Password** field appears. You must enter a default password that can be used for any users that do not have user name for ESS that differs from their primary email address.
 - d. Choose **Specify Password** to reset the passwords for all selected users to the value you provide.

When you choose this option, the **Password** field appears. You must enter the password to be used for all selected users.

- e. Choose **Custom** to enter a custom password template. Follow the instructions provided in the **Example Template** section that appears. Use the **See Attribute Reference** and **See Transformation Reference** links for additional information.
- 7 After you choose the password pattern, click **Next**. The **Edit Notification Message** page appears.
- 8 Choose either:
 - **Send notification message to the selected users** and compose a message in the field provided.
 - **Don't send a notification message.**
- 9 Click **Next**. The **Confirm** page appears.
 - a. You can click **Show Affected Users** to view a list of users whose passwords will be reset.
 - b. You can click the **Download New Passwords** link to download a CSV file containing the email address and new password for each user whose password will be reset.
- 10 Click **OK** to reset the passwords for the selected users.

Resetting Multiple Passwords by CSV Import

You can use the Administration Console to import passwords in bulk using a CSV (comma separated values) file. This feature works only for users already in the system. You cannot create users using this import file.

To create a password import CSV file:

Two reference files are provided for you to help create your CSV file. To locate them:

- 1 From the Administration Console, click **User Administration**.
- 2 From the **User Account Information** page, click **Upload passwords**.
- 3 To view a help page that describes how to create the file, click **File Format Reference**.
- 4 To download a CSV template file that you can use to start your own CSV file, click **Download Template**.

Table 4-3 Example Password Import CSV File

| | A | B | C | D |
|---|-------------------|----------------|----------|-----------------|
| 1 | Primary Email | Password | Welcomed | Notification |
| 2 | user1@example.com | user1-p4ssw0rd | Y | |
| 3 | user2@example.com | user2-p4ssw0rd | N | user2@other.com |

Table 4-3 Example Password Import CSV File

| | A | B | C | D |
|---|-------------------|----------------|---|-----------------|
| 4 | user3@example.com | user3-p4ssw0rd | | user3@other.com |
| 5 | user4@example.com | user4-p4ssw0rd | Y | |

The CSV import file must contain the following:

- 1 The first row must contain the import file header typed exactly as it appears below:
 - Cell A1: Primary Email
 - Cell B1: Password
 - Cell C1: Welcomed
 - Cell D1: Notification
- 2 Each additional row must contain the following information for exactly one user:
 - **Primary Email**—This address must match the user's existing email address in the system. You cannot create new users or addresses using this file. If your file contains an unrecognized email address, the validation step will inform you that the user is invalid.
 - **Password**—The password to import for the user. During the import step, you can choose to enforce your organization's password policy when importing these passwords or to ignore it. To leave a user's existing password as it is, leave this column blank.
 - **Welcomed** flag—A flag indicating whether the user has already been welcomed to the system.
 - To indicate that the user has already been welcomed, set to Y.
 - To indicate that the user must be welcomed the next time they log in, set to N.
 - To leave the user's existing flag as it is, leave this column blank.
 - **Notification** address—An optional notification address for the user.
 - To set the notification address to the same value as the user's primary address, set this column to Y.
 - To set an alternate address, type the email address in this column.
 - To leave the user's existing notification address, leave this field blank.

Save your import file as a CSV file.

To import passwords by CSV file:

- 1 From the Administration Console, click **User Administration**.
- 2 From the **User Account Information** page, click **Upload passwords**.
- 3 On the **Import Passwords** page, click **Browse** to locate the CSV file you want to import. Locate the file, then click **Open**.

NOTE About the CSV Import File

The CSV file you import must be correctly formatted. Refer to ["To create a password import CSV file:" on page 28](#).

The CSV file must be located on your local machine or in a network-accessible location.

- 4 Under the **Import Options** section, select the options to apply to this import:
 - **Overwrite permanent passwords**—Check this box to overwrite any existing permanent passwords with those in the upload file. Leave this box blank (unchecked) to leave any existing permanent passwords alone. A *permanent* password is one that the user is not required to change upon logging in. A *temporary* password must be changed the next time the user logs in.
 - **Validate passwords**—Check this box to validate the passwords you are uploading against the criteria listed. If this box is checked, all passwords in the file must meet the listed criteria, or the import will fail. Uncheck this box to upload all passwords in the file without applying any validation criteria. This box appears only when your organization has an available password policy.
 - **Require users to change password at next login**—Check this box to upload the passwords as *temporary* passwords that users must change immediately when they next log in. Uncheck this box to upload the passwords as *permanent* passwords that can be used until they meet any expiration criteria defined by your organization.
- 5 Click **Next**. The **Validation Results** page displays the total number of users found in the file, the number of users that will be imported or skipped, and any other important information. From this page, you can:
 - Download the validation results file. Click **Download Validation Results** to download a CSV file that shows any users that are skipped or whose information contains errors. You can use the information in this file to revise your import file, if necessary. Commented (informational) rows in the file begin with the # character. To find users whose information contains errors, look for rows that do not begin with the # character.
 - Go back to the previous page to choose another import file or change import options. Click **Back**.
 - Cancel the import and start over. Click **Cancel**.

- 6 To continue with the import, click **Submit**. The Import Results page appears. You can click **Download Validation Results** to view or save a CSV file containing the results of the import.

Changing Status for Multiple Users

The system tracks several types of user status by setting and clearing indicator flags that reflect a user's condition. You can change the status of multiple users at once by setting or clearing these flags. The following types of status settings can be changed in this way:

- Users who have been sent a welcome message. *Welcomed* users have been sent a welcome message or have been assigned a permanent password. Setting this flag indicates the users have been welcomed. Clearing this flag adds them to the list of users who have not been welcomed, and allows them to receive welcome messages.
- Users who have been excluded from the system. See ["Excluded Users" on page 40](#). Excluded users do not appear in any welcome or login reports, and cannot be sent messages. Setting the flag excludes the users. Clearing the flag includes (reinstates) the users.
- Users who have opted out of providing notification data. Users who have opted out chose not to provide notification data in the Welcome Wizard. They cannot be notified during an activation. Setting this flag changes the users' status to *Opted out*, but does not remove any notification information already in the system. Clearing the flag changes the users' status to *has not responded* to the welcome message.

To change status flags for users:

- 1 From the Administration Console, click **User Administration**.
- 2 Click **User Information**. The **User Account Information** screen appears.
- 3 Click **Bulk Reset Flags**. The **Select Users** screen appears.
- 4 Click the appropriate tab to identify the users to change status for. You can select by:
 - **Predefined User Sets:**
 - All Users
 - Users who have never logged in
 - Users not yet welcomed
 - Users who have been sent a welcome message
 - Excluded users
 - Users who have opted out of providing notification dataClick the button next to the appropriate set.
 - **Mailing Lists**—Search by Email or by Name, using % as a wildcard.

- **Servers**—Click the check box by the appropriate server.
 - Individual **Users**—Search by Email or by Name, using % as a wildcard.
- 5 Click the check box to select a user or group from the left list.
 - 6 Click **Add**. The selected users move to the **Change status of these users** list.
 - 7 Click **Next**.
 - 8 For each of the status settings, select one:
 - **Do not change** (Default)
 - **Set flag**
 - **Clear flag**
 - 9 Click **Next**.
 - 10 To see a list of all users affected by the change, click **Show Affected Users**. If the list is incomplete, or you want to make other changes, click **Back**. If you are satisfied with the list of users, click **Submit**.

Updating a User's Contact Information

Normally, each user enters personal emergency contact information after receiving the initial Welcome message and logging in to Email Continuity. However, a user with appropriate administrative privileges can edit this information when needed.

To edit a user's contact information:

- 1 From the **User Information** screen, search for the appropriate user account and locate it in the search results list. On the same line as the user account listing, click **Edit**. The **Edit User Contact** page displays.
- 2 Update any information as necessary. When finished, click **Submit**.

Defining User Sets

Administrators can define groups of mailboxes called *user sets*. User sets allow you to send notification messages, activate Email Continuity, or apply other features to a designated group of users. For example, if you anticipate certain groups of users are likely to be activated separately (such as system administrators for tests), you can define a user set for them. Defining user sets specifically for testing allows for performance of regular system tests without activating all users and without taking down primary services.

To create a user set:

- 1 From the Administration Console, click **User Administration**.
- 2 Click **User Sets**. The **User Sets** page displays.

- 3 Click **Create User Set**. The **User Set Details** screen appears.
- 4 In the **Name** box, type the name for the user set.
- 5 To build the user set manually, click the appropriate tab to select users for inclusion in the set by Servers, Mailing List, or individually by User.
 - If you select the **Mailing List** or **User** tab, in the **Search** box type an email address or name and search for the results. Then click the listed mailing list or user to select.
 - If you select the **Server** tab, click a server to select it.
 - Repeat until all desired servers, mailing lists, or users display in the **Users in the Set** listing.
- 6 To upload a CSV file containing user sets, click the **Upload** tab, browse to the file location, select the upload file, and click **Open**.

The CSV import file must contain the following:

Table 4-4 Example User Set Upload CSV File

| A | B |
|---|-------------------|
| 1 | Email Address |
| 2 | user1@example.com |
| 3 | user2@example.com |
| 4 | user3@example.com |
| 5 | user4@example.com |

- a. The first row must contain the import file header `Email Address`.
 - b. Each additional row must contain the email address for exactly one user.
- 7 When all the users are selected or the upload file is listed, click **Add**.
 - 8 Click **Submit**.

Assigning Super Administrator Privileges

A *super administrator* is a user account that is given the Super Administrator role within Email Continuity. User accounts with Super Administrator permissions can perform the same Administrator Console functions as the *service root account*. Creating Super Administrator accounts helps you track actions taken in the system.

Email Continuity Super Administrators can perform more actions than regular Email Continuity Administrators. The table below summarizes functions available to Super Administrators and the service root account that are not available to regular Email Continuity Administrators.

Table 4-5 Features Limited to Super Administrators or Service Root Account

| Feature | See Also |
|---|--|
| Creating Super Administrators | This section |
| Creating Email Continuity Administrators | "Assigning Email Continuity Administrator Privileges" on page 35 |
| Creating Help Desk Users | "Assigning Help Desk Privileges" on page 36 |
| Configuring email routing | "Configuring Email Routing" on page 53 |
| Modifying the organization's email disclaimer | "Changing the Email Disclaimer" on page 55 |
| Setting user deletion notification thresholds for SyncManager | "Sync Notify Settings" on page 55 |
| Customizing the Home Page | "Customizing the Home Page" on page 56 |
| Customizing the Welcome Wizard | "Customizing the Welcome Process" on page 57 |
| Changing the root account password | "Changing Your Password" on page 58 |

To create a super administrator:

- 1 Log into the Administration Console using an existing *super administrator* account or the *service root account* provided by Support. See ["Logging Into the Administration Console" on page 21](#) for more information.

NOTE Log in Using a Super Admin or Service Root Account

You can only access the Super Admin features by logging into the Administration Console with the service root account or another super administrator account.

- 2 From the Administration Console, click **User Administration**.
- 3 Under the **User Administration** menu, click **Super Admins**.
- 4 In the lower part of the page, search for the user account to which you want to assign the Super Admin role. You can assign this role to any existing Email Continuity account. If you need to create a new account, see ["Adding Mailboxes \(Users\) Manually" on page 44](#) or contact Support.
 - a. In the **Search** field, enter the user name or email address. You can use % as a wildcard.
 - b. Click the radio button to indicate a search **By Name** or **By Email Address**.
 - c. Click **Search**. A list of users matching your search parameters appears.

- 5 To give a user super administrator privileges, check the check box for that user under the **Add** column, then click **Add**. The user is added to the list of super administrators at the top section of the page.

To remove super administrator privileges:

- 1 Log into the Administration Console using an existing *super administrator* account or the *service root account* provided by Support. See ["Logging Into the Administration Console" on page 21](#) for more information.

NOTE Log in Using a Super Admin or Service Root Account

You can only access the Super Admin features by logging into the Administration Console with the service root account or another super administrator account.

- 2 From the Administration Console, click **User Administration**.
- 3 Under the **User Administration** menu, click **Super Admins**.
- 4 In the upper part of the page, locate the user account from which you want to remove super administrator privileges.
- 5 Check the check box for that user under the **Remove** column, then click **Remove**. The user is removed from the list of super administrators at the top section of the page. The user account remains in the system, but has only basic Email Continuity user privileges.

Assigning Email Continuity Administrator Privileges

Email Continuity Administrators can use all the features of the Administration Console except those explicitly limited to Super Administrators and the service root account. (These exceptions are listed under ["Assigning Super Administrator Privileges" on page 33](#).) Creating Email Continuity administrators helps you track actions taken in the system more accurately.

To assign administrative privileges to an account:

- 1 Log into the Administration Console using an existing *super administrator* account or the *service root account* provided by Support. See ["Logging Into the Administration Console" on page 21](#) for more information.
- 2 From the Administration Console, click **User Administration**.
- 3 Click **Administrators**. The **Administrators** page displays.
- 4 In the **Search** box, type the email address or name of the appropriate user. Click **Search**.
- 5 In the search results, locate the appropriate user and click the check box next to the name. Click **Add**.
- 6 The **Administrators** page refreshes and the name of the new administrator displays near the top of the page.

To remove administrative privileges from an account:

- 1 Log into the Administration Console using an existing *super administrator* account or the *service root account* provided by Support. See ["Logging Into the Administration Console" on page 21](#) for more information.
- 2 Click **Administrators**. The **Administrators** page displays.
- 3 Click the **Remove** check box next to the appropriate administrator's name.
- 4 Click **Remove**.

NOTE Super Administrators Can Demote Their Own Accounts

Super administrators can remove the super administrator privileges from their own accounts. Upon their next login, these administrators will no longer have super administrator rights.

Assigning Help Desk Privileges

Help Desk users are user accounts with a limited set of administrator privileges. Help Desk users can view user information and reset users' passwords, but they cannot activate Email Continuity or perform any other administrator tasks.

Help Desk privileges can be assigned to existing Email Continuity users by Super Administrators or by the service root account. Email Continuity Administrators can view the list of Help Desk users, but cannot grant or remove Help Desk privileges.

To grant a user Help Desk privileges:

- 1 Log into the Administration Console using an existing *super administrator* account or the *service root account* provided by Support. See ["Logging Into the Administration Console" on page 21](#) for more information.
- 2 Click **User Administration**.
- 3 Click **Help Desk Users**. The **Help Desk Users** page displays.
- 4 In the **Search** box, type the email address or name of the appropriate user. Click **Search**.
- 5 In the search results, locate the appropriate user and click the check box next to the name. Click **Add**.
- 6 The **Help Desk Users** page refreshes and the name of the new help desk user displays near the top of the page. When the Help Desk user logs in to the service during an activation, a help desk icon displays along with a link to the **User Information** screen in the Administration Console. From the **User Information** screen, the Help Desk user can reset users' passwords.

To remove Help Desk privileges from an account:

- 1 Log into the Administration Console using an existing *super administrator* account or the *service root account* provided by Support. See ["Logging Into the Administration Console" on page 21](#) for more information.
- 2 Click **Help Desk Users**. The **Help Desk Users** page displays.
- 3 Locate the appropriate user and click the **Remove** check box next to the name. Click **Remove**.

Reviewing Login Status

The **Login Status** screen provides quick access to login history. It also provides current activation status, and logon history from past activations.

To review login status:

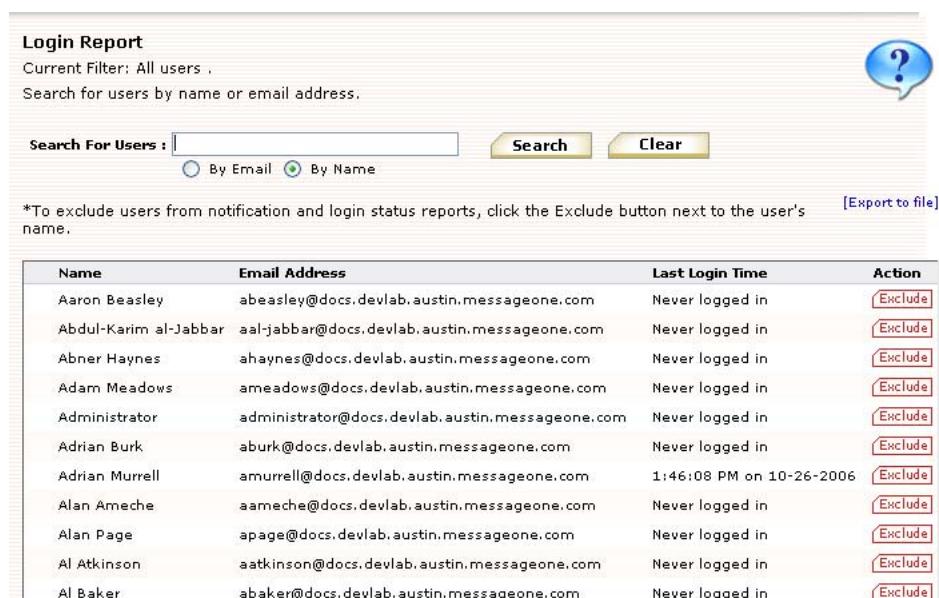
- 1 From the Administration Console, click **User Administration**.
- 2 Click **Login Status**. The **Login Status** screen appears.



The screenshot shows the 'Login Status' screen. At the top, it says 'Login Status' and 'View reports on login activity. Please note that excluded users are not included in the summary counts or in the report views.' There is a help icon (question mark in a blue circle) to the right. Below this, there are three main sections: 'Login History', 'Active Users', and 'Previous Activations'. The 'Login History' section shows '1096 users are in the system. Show last login ...' and '1089 users have never logged in. Show users who have never logged in ...'. There is a green arrow icon and a link 'Remind users who have never logged in ...'. The 'Active Users' section shows '1096 users are in the active state. 3 users have logged in since activation and 1093 users have not logged in since activation. Show last login for users in the active state ...'. There is a green arrow icon and a link 'Remind users in the active state who have not logged in, but have notification options ...'. The 'Previous Activations' section says 'Select a previous activation to view login status during that time frame.' Below this, there is a dropdown menu labeled 'Previous Activations:' with the selected option 'Activation starting on 2:51:08 PM on 10-13-2006'. To the right of the dropdown is a link 'Show last login ...'.

The **Login History** section shows how many users are in the system.

- 3 To see the login status for a user, click **Show last login**. The **Login Report** screen appears.



Login Report

Current Filter: All users .

Search for users by name or email address.

Search For Users :

☐ By Email ☒ By Name

*To exclude users from notification and login status reports, click the Exclude button next to the user's name. [\[Export to file\]](#)

| Name | Email Address | Last Login Time | Action |
|-----------------------|---|--------------------------|--|
| Aaron Beasley | abeasley@docs.devlab.austin.messageone.com | Never logged in | <input type="button" value="Exclude"/> |
| Abdul-Karim al-Jabbar | aal-jabbar@docs.devlab.austin.messageone.com | Never logged in | <input type="button" value="Exclude"/> |
| Abner Haynes | ahaynes@docs.devlab.austin.messageone.com | Never logged in | <input type="button" value="Exclude"/> |
| Adam Meadows | ameadows@docs.devlab.austin.messageone.com | Never logged in | <input type="button" value="Exclude"/> |
| Administrator | administrator@docs.devlab.austin.messageone.com | Never logged in | <input type="button" value="Exclude"/> |
| Adrian Burk | aburk@docs.devlab.austin.messageone.com | Never logged in | <input type="button" value="Exclude"/> |
| Adrian Murrell | amurrell@docs.devlab.austin.messageone.com | 1:46:08 PM on 10-26-2006 | <input type="button" value="Exclude"/> |
| Alan Ameche | aameche@docs.devlab.austin.messageone.com | Never logged in | <input type="button" value="Exclude"/> |
| Alan Page | apage@docs.devlab.austin.messageone.com | Never logged in | <input type="button" value="Exclude"/> |
| Al Atkinson | aatkinson@docs.devlab.austin.messageone.com | Never logged in | <input type="button" value="Exclude"/> |
| Al Baker | abaker@docs.devlab.austin.messageone.com | Never logged in | <input type="button" value="Exclude"/> |

- 4 To find the most recent login for a particular user:
- In the **Search for Users** field, type the name or email address (or part of it with the % wildcard).
 - Click **Search**. Results appear in the window below.
- 5 To export a CSV file of the login report data, click **Export to file**.
- 6 To exclude a user from the system, click the **Exclude** button.
- 7 From the **Login Report** screen, use your browser's **Back** button to return to the **Login Status** screen.
- 8 To find the most recent login for active users, in the **Login Status** screen, click **Show last login for users in the active state**. The **Login Report** screen appears showing only active users.
- 9 To see login information from a past activation:
- In the **Login Status** screen **Previous Activations** section, select a past activation from the drop-down list.
 - Click **Show last login**. The **Login Report** screen appears, from which you can search an individual user's login information during the activation.

The **Login Status** screen also provides links to reminder functionality. By clicking the links, you can:

- Remind users who have never logged in.
- Remind users in the active state who have not logged in, but who have notification options.

Exporting Users' Contact Information

Data maintained by the service can be exported to a CSV file. If present in the system, export files contain data described in [Table 4-6, "Exported User Data"](#).

Table 4-6 Exported User Data

| Category | Data |
|------------------------------|-------------------------------------|
| User Account | Primary Email |
| | Display Name |
| | System ID |
| | Last Login |
| | Welcome Message Sent status |
| | Excluded (status) |
| | Has permanent password (status) |
| | Opted Out of Notifications (status) |
| Contact Information | Street Line 1 |
| | Street Line 2 |
| | City |
| | State/Province |
| | Zip/Postal Code |
| | Country |
| | Home Number |
| | Work Number |
| Notification Email Addresses | Cell Number |
| | Wireless Forwarding Address |
| | Email Address 1 |
| | Email Address 2 |
| | Email Address 3 |

Table 4-6 Exported User Data (Continued)

| Category | Data |
|--------------------|-----------------|
| Emergency Contacts | Full Name 1 |
| | Relationship 1 |
| | Email Address 1 |
| | Phone Number 1 |
| | Full Name 2 |
| | Relationship 2 |
| | Email Address 2 |
| | Phone Number 2 |
| | Full Name 3 |
| | Relationship 3 |
| | Email Address 3 |
| | Phone Number 3 |

To generate a CSV spreadsheet of emergency contact data for all users:

- 1 From the Administration Console, click **User Administration**.
- 2 Click **Export**. The **Export User Information** screen appears.
- 3 Click **Export** to download a CSV file containing the current data for all users.

Excluded Users

You can exclude from Email Continuity mailboxes that are not associated with users, such as resource mailboxes. Excluded users are not included in notification reports or login status reports. You can exclude users by user sets, mailing lists, servers, and individual users.

NOTE Resetting Excluded Status for Multiple Users

In addition to the procedures provided below, you can also use the Reset status feature to change the Excluded status for many users at once. See ["Changing Status for Multiple Users" on page 31](#).

To exclude a user:

- 1 From the Administration Console, click **User Administration**.
- 2 Click **Excluded Users**. The **Excluded Users** screen appears.
- 3 Click **Exclude users**.

- 4 Identify users (mailboxes) to exclude. Click the appropriate tab to identify users by Server, Mailing List, or individually by User.
 - a. If you select the **Mailing List** or **User** tab, in the **Search** box type an email address or name and search for the results. Then click the listed mailing list or user to select.
 - b. If you select the **Server** tab, click a server to select it.
- 5 Click **Add**. Repeat until all users to be excluded appear in the right list.
- 6 Click **Next**. The **Confirm** screen appears. To see the list of excluded users, click **Show Affected Users**.
- 7 Click **Submit**.

To remove individual users from the Excluded list (reinstate them in the system):

- 1 From the Administration Console, click **User Administration**.
- 2 Click **Excluded Users**. The **Excluded Users** screen appears.
- 3 In the **Search for Users** field, type the name (or partial name using % as a wildcard) and click **Search**. The results appear in the table below.
- 4 Click the **Remove** button next to the user's name.

To remove multiple users from the Excluded list (reinstate them in the system):

- 1 From the Administration Console, click **User Administration**.
- 2 Click **Excluded Users**. The **Excluded Users** screen appears.
- 3 Click **Remove Users from the excluded list**. Identify users (mailboxes) to exclude. Click the appropriate tab to identify users by Server, Mailing List, or individually by User.
 - a. If you select the **Mailing List** or **User** tab, in the **Search** box type an email address or name and search for the results. Then click the listed mailing list or user to select.
 - b. If you select the **Server** tab, click a server to select it.
- 4 Click **Add**. Repeat until all are listed in the right list.
- 5 Click **Next**. The **Confirm** screen appears. To see the list of reinstated users, click **Show Affected Users**.
- 6 Click **Submit**.

Enabling BlackBerry Forwarding

If configured to do so by Support, Email Continuity can forward mail to users' BlackBerry devices during an activation. RIM allows BlackBerry device owners to enable a capability on the device called the BlackBerry Internet Service (BIS). BIS includes a carrier BlackBerry Access Plan. If your organization is currently using BlackBerry Enterprise Server capability, you have a BlackBerry Access Plan.

NOTE BlackBerry Forwarding vs. Wireless Continuity for BlackBerry

The BlackBerry Forwarding option, described here, can be turned on for Email Continuity customers by Support. Wireless Continuity for BlackBerry is a separate product. For information on Wireless Continuity for BlackBerry, contact your account manager.

In the event the BES is unavailable, Email Continuity uses the BIS as an alternate path to route messages directly to the BlackBerry device. The software routes inbound messages to the alternate address of the BlackBerry device and forwards messages by way of SMTP to the RIM Hosted Server. The RIM Hosted Server then delivers the messages through the carrier's wireless gateways and on to your wireless device.

Messages that are received while active on Email Continuity are forwarded from Email Continuity to the BlackBerry device; those messages will be recovered automatically during the recovery process. The messages that are sent from the BlackBerry device while active on Email Continuity and using the BlackBerry Internet Service are not automatically recovered during the recovery process. If it is important for these messages to be recovered to the primary system after an activation, the user can configure the Auto BCC function (described below) to send a copy of each sent message back to the account.

After the user's BlackBerry is configured to use the BIS, the user doesn't need to do anything else to receive messages on it during an activation. However, in order to send messages from a BlackBerry, the user must switch message services, as described below.

Configuring a BlackBerry for Use with BlackBerry Forwarding

Before you can enable forwarding for a BlackBerry device, you need three pieces of information.

- The name of the wireless carrier (for example, Cingular, Verizon, T-Mobile, Nextel, Sprint.)
- The PIN number for the BlackBerry device. (For most devices, this is located beneath the battery. If not, consult the manual that came with the device.)
- The IMEI or ESN number for the BlackBerry device. (For most devices, this is located beneath the battery. If not, consult the manual that came with the device.)

To set up a BlackBerry device:

- 1 Follow the account setup process for your carrier.
 - a. Log in to www.blackberry.com, and click **Support**.
 - b. Select **Product Support > BlackBerry Internet Service**. Scroll to the bottom of the support page.
 - c. Select your carrier from the list, and follow the login process. During the process, you are provided with a new email address for your device. Write this address down.
- 2 When you have accessed your account, you must make two changes to the account data:
 - a. In the **Reply-to address** field, enter your complete business email address. This ensures that messages you send from your BlackBerry during an activation are sent by Email Continuity.
 - b. In the **Auto BCC** field, enter your complete email address. This ensures that messages you send from your BlackBerry during an activation are recovered by Email Continuity.
 - c. Save the changes.
- 3 Set up your Email Continuity account to forward messages to your BlackBerry device's new wireless, backup email address.
 - a. Log in to your webmail account.
 - b. Click the **Notification Options** icon.
 - c. Under the **Personal Email** section, add the new email address you obtained during the setup process for your carrier. Click **Add**, then click **Submit**.
 - d. Return to the Email Continuity page and enter this email address in the **Email address** box of the **Email Forwarding** section.

NOTE No Email Forwarding Section

If the Notification Options page of your account does not include an Email Forwarding section, contact Support to make sure Forwarding is enabled.

- 4 During an activation, you must change Message Services to be able to send email from your BlackBerry. To change message services:
 - a. From the device, select **Options > Message Service > Change Option**.
 - b. Change from the Desktop Service to the BIS Account Service configured above.
 - c. When the primary email system is restored, return the Message Service to the Desktop Service option.

NOTE Using the Reply To: Function During an Activation

You cannot use the Reply To: function on messages that were received prior to the activation. If you try to reply to a message received before the activation, the BlackBerry attempts to use the Desktop service book, which relies on the BES, and it will fail. You can use the Reply To: function on messages received after the activation.

Mailboxes and Aliases

The SyncManager automatically creates an account for each mailbox in the primary mail system, whether the mailbox is associated with an individual person (end user) or is a collection box for certain types of email (such as status notices that are sent to a designated address). Administrators can manually create new mailboxes to add other users, and create aliases that map incoming email messages to existing mailboxes.

Adding Mailboxes (Users) Manually

To add a mailbox (user) to Email Continuity:

- 1 From the Administration Console, click **Mailboxes and Aliases**. The **Additional Mailboxes and Aliases** screen appears.
- 2 Click **Create Mailbox**. The **Create Mailbox** screen displays
- 3 In the **Display Name** field, type a name.
- 4 In the **Email Address** field, type an email address.
- 5 Click **OK** to create, or **Cancel** to cancel.

Predefined distribution lists synced from the primary mail system can be used for quick communication with specific groups of users.

Creating Aliases

To create an alias:

- 1 From the Administration Console, click **Mailboxes and Aliases**. The **Additional Mailboxes and Aliases** screen appears.
- 2 Click **Create Alias**. The **Create Alias** screen appears.
- 3 In the **Destination Address** field, type the destination address (the preexisting address that will gain a second name).
- 4 In the **Alias** field, type an alias (the new email address).
- 5 Click **OK** to create or **Cancel** to cancel.

Mailing Lists

Email Continuity synchronizes your existing mailing lists from the primary mail system so that, in the event of a disruption, users can continue to send email to and receive email messages from their usual mailing lists. You can also use mailing lists as activation or recovery units. For example, it might be best to activate the members of a building-specific mailing list or to recover a small set of users before a full-scale recovery.

Mailing lists can contain both internal email addresses (users with Email Continuity accounts) and external email addresses.

To view mailing lists and members of each list:

- 1 In the Administration Console, click **Mailing Lists**.
- 2 To locate a specific mailing list, in the **Search** box type the email address or name and click **Search**.
- 3 To view the individual members of a mailing list, in the **List Name** column click the name of the list. The listing expands to include all members. Account members display with full names; external members display with only email addresses.

Notification

The **Notification** screens in Email Continuity allow you to introduce the service to users through the welcome process, send reminders about the service, send custom messages, and manage fault and transition alerts.

Welcoming New Users

Though it is possible to implement and activate Email Continuity without introducing it to users through the welcome process, welcoming users is strongly encouraged because:

- Introducing users to the service before an emergency helps them understand that system usage is a shared responsibility. It can also be reassuring for users to know that safeguards are in place for them should they ever be needed.
- Capturing notification information prior to Email Continuity activation allows the system to handle notification of users automatically. This is especially beneficial during a disaster because it frees the IT staff to recover the primary mail system. Similarly, the information captured by the service is often needed by Human Resources during an emergency, and, depending on the type of disaster, it may not be readily available.

- Manually setting users' passwords is tedious work. The Welcome Wizard provides temporary passwords automatically so that at the time of activation the IT staff can focus on recovery of the primary mail system. Note that separate Email Continuity passwords are not required if the Windows Authentication feature is enabled.
- Capturing notification information prior to activation allows the system to handle notification of users automatically when the primary mail system has been recovered. Even if they have not used the webmail system, the automatic notification alerts them to the fact that their primary system is again available.
- Providing a notification address during the registration process allows users to take advantage of the forgot password link if they ever need it.

The welcome message:

- Informs users about Email Continuity.
- Provides users with their username and a temporary password.
- Includes a link that, if so configured, starts a welcome wizard that can be configured to collect notification options, home address, and emergency contact information from the user.

To configure which user information is collected using the welcome wizard, see ["Customizing the Welcome Process" on page 57](#).

- Can be sent automatically once a week to any users who have not yet been sent one.

The service tracks different categories of users so that you can send the welcome message to users who:

- Have not yet been sent a welcome message.
- Have been welcomed, but did not respond to the message. A user has *responded* when he has logged in to the service and either provided notification data or stated he has no alternate means of communication (opted out).
- Do not yet have a permanent password for the service. These users either have not been sent a welcome message, or have not yet changed the temporary password provided in the welcome message.
- Have responded, but did not provide notification data (have opted out).

NOTE Status for Users Can Be Reset

If you need to reset the status for multiple users in the system, use the **Reset flags for multiple users** feature. See ["Changing Status for Multiple Users" on page 31](#).

The service provides default text for the welcome message. As you customize the message, note that it uses variables that are filled in when the message is sent:

- `%__username%` — the recipient's Email Continuity username
- `%__tempPassword%` — temporary password generated by Email Continuity for the recipient
- `%__autologinUrl%` — the URL to access Email Continuity (with the username and password embedded)

TIP Best Practices for Welcoming Users

- Plan to welcome users in stages, rather than welcoming the entire organization at one time. Particularly if your organization has several thousand mailboxes, welcome users in groups of 500 or fewer to minimize impact on your incoming gateway.
 - A day or two before sending a welcome message, send an explanatory memo to the users introducing Email Continuity and urging them to respond promptly when they receive the welcome message.
 - A couple of days after sending the welcome message, send a reminder to users who have been welcomed, but who have not responded. By this time, an average user response is about 50%; a good goal is 80%.
 - Continue to send reminders until the target response goal is reached. If you are having difficulty getting users to respond, you may want to change the From address in the message to a department leader, or change the subject line of the message to *Action required* or *Second Notice*.
-

To send a welcome message to one or more users:

- 1 In the Administration Console, click **Notification**.
- 2 Click **Welcome New Users**.

Welcome New Users
Use the welcome process to introduce users (mailboxes) to the service and collect their notification information.

All welcome messages contain the individual's username, temporary password, and URL to access the service.

Users have "responded" to the welcome message when they have logged in and either provided notification information, or stated they had no alternate means of notification.

Users who have not changed their temporary passwords, or who have not been sent a welcome message, do not yet have a permanent password.

If a user does not provide notification information, the user cannot be contacted when the service is activated.

Automatically send a welcome message to any new users who have not been sent one. The message is sent once per week. The automatic welcome feature is currently turned off.

3 users have not received an initial welcome message. [Show users ...](#)
[Welcome users who have not been sent an initial welcome message...](#)
[Re-send welcome message to any user\(s\)...](#)

All welcomed users have responded. [Show users ...](#)
[Re-send welcome message to users who have not responded ...](#)

[Send a welcome message to users who do not have a permanent password ...](#)

All users that have completed the Welcome Wizard have configured their notification information. [Show users ...](#)
[Automatically welcome new users...](#)

- 3 Click **Welcome users who have not received an initial welcome message**. The **Edit Message** screen appears.
- 4 In the **From** box, type an email address, being sure you enter an alias within your organization so that any users who reply with questions are directed to an administrator or Help Desk user.
- 5 In the **Subject** box, make any necessary changes to the default text.

- 6 In the **Text** box, make any necessary changes to the default text.
- 7 Click **Next**. The **Select Recipient** screen appears.
- 8 Click the appropriate tab to identify recipients by User Set, Server, Mailing List, or individually by User.
 - a. If you select the **Mailing List** or **User** tab, in the **Search** box type an email address or name (or part using the % as a wildcard) and search for the results. Then click the listed mailing list or user to select.
 - b. If you select the **Server** tab, click a server to select it.
- 9 Click **Add**. Repeat until all intended recipients are listed in the right list.
- 10 Click **Next**. The **Confirm** screen appears.
- 11 To see a list of recipients, click **Show Affected Users**. Review the message text.
- 12 Click **Send**.

To automatically send welcome messages to new users:

- 1 In the Administration Console, click **Notification**.
- 2 Click **Welcome New Users**.
- 3 Click **Automatically welcome new users**.
- 4 Click **Enable automated welcome message**.
- 5 Click **Submit**.

When the majority of your users have responded to the welcome message, you may need to review the lists of users who have not responded, do not yet have a permanent password, or who have opted out (have not provided contact information). (Note that the data provided about users' responses is an estimate in some cases; these are marked with an asterisk [*].) The service lets you send welcome messages to these categories of users; click the link and follow the process described for welcoming new users, except that the recipient list is already created for you.

In some cases, you may need to exclude certain users/mailboxes from which you don't expect a response. The **Show Users** links in the **Welcome New Users** screen display lists of users in these categories and a button to Exclude individual mailboxes.

Sending Reminders

The **Reminders** screen allows you to send reminders to different categories of users:

- Those who have not responded to the welcome message.
- Those who have responded, but have indicated they have no alternate notification options (they have opted out).

- Those who have responded and provided information, but need to be reminded to keep the information current.

By default, reminders contain a link to the service website, the recipient's username, and a link to the forgot password feature. (The Reminders message does not contain the temporary password or login URLs. If you need to assign a temporary password, or provide the login URL, send a Welcome Message instead.) You can customize any portion of the reminder message.

To send a reminder:

- 1 In the Administration Console, click **Notification**.
- 2 Click **Reminders**. The **Reminders** screen appears.



- 3 Select the reminder to send by clicking one of the following:
 - **Send a reminder to welcomed users who have not responded**,
 - **Send a reminder to users who chose not to provide notification options**, or
 - **Send a reminder to users to keep notification information current**.

The **Edit Message** screen appears.

- 4 In the **From** box, type an email address, being sure you enter an alias within your organization so that any users who reply with questions are directed to an administrator or Help Desk user.
- 5 In the **Subject** box, make any necessary changes to the default text.
- 6 In the **Text** box, make any necessary changes to the default text.
- 7 Click **Next**. The **Select Recipient** screen appears. Note that for each type of reminder, an appropriate user set appears in the **User Sets** tab.
- 8 Either:
 - Click the radio button for the particular user set, or
 - Click the appropriate tab to identify recipients by Server, Mailing List, or individually by User.

- If you select the **Mailing List** or **User** tab, in the **Search** box type an email address or name and search for the results. Then click the listed mailing list or user to select.
 - If you select the **Server** tab, click a server to select it.
- 9 Click **Add**. Repeat until all recipients are listed in the right list.
 - 10 Click **Next**. The **Confirm** screen appears.
 - 11 To see a list of recipients, click **Show Affected Users**. Review the message text.
 - 12 Click **Send**.

Managing Fault Alerts

The fault alerts list includes users who should receive notifications of problems identified by the system. Fault alerts are emailed to these users when:

- Certain data center readiness checks fail (See ["Readiness Checks" on page 24](#));
- The percentage of users or mailing list members exceeds the configured threshold. (See ["Sync Notify Settings" on page 55](#))

To add a user to the fault alerts list:

- 1 In the Administration Console, click **Notification**.
- 2 Click **Fault Alerts**. The **Fault Notification** page displays.
- 3 In the **Search** box, type the email address or name of the user. Click **Search**.
- 4 In the search results, locate the listing for the user. Select the check box next to the name.
- 5 Click **Add**. The **Fault Notification** page refreshes and the newly added user listing displays near the top of the page.

To remove a user from the fault alerts list:

- 1 In the Administration Console, click **Notification**.
- 2 Click **Fault Alerts**. The **Fault Notification** page displays.
- 3 Locate the listing for the appropriate user and select the **Remove** check box next to the name.
- 4 Click **Remove**.

Managing Transition Alerts

The transition alert list identifies users who should automatically receive notifications whenever Email Continuity changes state— that is, whenever it is activated, put into test mode, or returned to READY state. You can use this

function to inform appropriate users when there is an activation of Email Continuity for an actual outage or a test. To see reports on state transitions, see ["Viewing Audit Reports" on page 52](#).

To add users to the transition alerts list:

- 1 In the Administration Console, click **Notification**.
- 2 Click **Transition Alerts**. The **Transition Notification** page displays.
- 3 In the **Search** box, type the email address or name of the user. Click **Search**.
- 4 In the search results, locate the listing for the user. Select the check box next to the name.
- 5 Click **Add**. The **Transition Notification** page refreshes and the newly added user listing displays near the top of the page.

To remove a user from the transition alerts list:

- 1 In the Administration Console, click **Notification**.
- 2 Click **Transition Alerts**. The **Transition Notification** page displays.
- 3 Locate the listing for the appropriate user and select the **Remove** check box next to the name.
- 4 Click **Remove**.

Sending Custom Notifications

Administrators can use the service to send email messages to users even when Email Continuity has not been activated. You can send custom notifications to both primary email addresses and/or alternate email addresses.

To send a custom message:

- 1 In the Administration Console, click **Notification**.
- 2 Click **Custom Notification**.
- 3 Click **Send a custom message**. The **Edit Message** page displays.
- 4 In the **From** box, type an email address, being sure you enter an alias within your organization so that any users who reply with questions are directed to an administrator or Help Desk user.
- 5 In the **Subject** box, type a subject for the message.
- 6 In the **Text** box, type the body of the message.
- 7 Click **Next**. The **Select Recipients** screen appears.

- 8 Click the appropriate tab to identify recipients by Server, Mailing List, or individually by User.
 - a. If you select the **Mailing List** or **User** tab, in the **Search** box type an email address or name and search for the results. Then click the listed mailing list or user to select.
 - b. If you select the **Server** tab, click a server to select it.
- 9 Click **Add**. Repeat until all recipients are listed in the right list.
- 10 Click **Next**. The **Select Recipient Options** screen appears.
- 11 Select the addresses to use for the custom notification:
 - **Primary addresses in your mail environment**
 - **Notification addresses** (addresses users have provided as alternate contact information)
 - **Both Primary and notification addresses**Click **Next**.
- 12 To see a list of recipients, click **Show Affected Users**. Review the message text.
- 13 Click **Send**.

Viewing Audit Reports

The service provides an audit trail of actions taken within the system. You can review six months' history for activations and tests. All audit reports can be exported to a CSV file. The user initiating each state transition is provided along with the time and date of the transition. Users' logon status during an activation is also collected. If a recovery archive has been generated, the name and size of the archive are displayed. See the following sections for more information:

- ["Activation Reports" on page 52](#)
- ["Test Reports" on page 53](#)

Activation Reports

TIP Activation History Records

For an easy way to provide disaster recovery/business continuity auditors with data proving that your organization conducts regular tests, use the Tests page in the Activation History section for a concise record of Email Continuity tests over the last six months.

To view an Activation report:

- 1 From the Administration Console, click **Audit Reports**.
- 2 Click **Activations**. The **Activation History** report appears.
- 3 From this screen, you can:
 - Click the **State Transitions** arrow for an activation to display the date, time, and responsible party.
 - Click **View logon records during this activation** to see active users, and identify who has logged in to the service. (See also ["Reviewing Login Status" on page 37.](#))
 - Click **Export** to obtain a copy of the report in CSV format.

Test Reports

To view a Test report:

- 1 From the Administration Console, click **Audit Reports**.
- 2 Click **Tests**. The **Test History** report appears.
- 3 From this screen, you can:
 - Click the **State Transitions** arrow for an activation to display the date, time, and responsible party.
 - Click **Export** to obtain a copy of the report in CSV format.

Modifying System Settings

NOTE System Settings Are Only Available to the Root Administrator Account

The System Settings menu and its options are only available to administrators logged in using the root account.

Configuring Email Routing

The system allows you to designate a series of next hops for inbound (forwarded) mail destined for your organization's mail system, and outbound email during an activation of Email Continuity. Before changing these settings, see the sections ["Mail Routing Inbound—Store and Forward" on page 7](#), and ["Mail Routing—Outbound During Activation" on page 8](#). Note that an audit trail is provided for all changes made to email routing, including event, actor and day/time information.

The default behavior is to use MX records for these functions. If you decide to provide a list of alternate hosts, the system uses them in the order you provide them. If your organization uses a third-party vendor to handle incoming mail, you

must identify a list of hosts using the Administration Console. In order to prevent mail looping, mail for the organization will be queued by Email Continuity until the hosts are specified.

NOTE Allow Time for Changes to Take Effect

When you configure the system to use hostnames instead of MX records, it can take up to 10 minutes for the changes to take effect.

TIP Use Hostnames instead of IP Addresses for Alternative Routing

Though the routing features accept both IP addresses and hostnames, hostnames provide greater flexibility and are preferred.

CAUTION Testing Recommended

After making changes to routing for inbound or outbound mail routing or delivery, verify the changes by performing a test activation. Incorrect or invalid settings can result in delayed, bounced or lost messages.

Routing for Forwarded Mail

To configure the path for forwarded mail:

- 1 From the Administration Console, click **System Settings**.
- 2 Click **Email Routing**. The Email Routing Rules page appears. The **Forwarding of Inbound Email to Your Mail System** section displays the current forwarding setting.
- 3 To change the routing:
 - a. Click **Edit**.
 - b. In the **Routing Rules** section, enter the host name in the field and click **Add**. The hostname appears in the **Hosts in priority order** field above. Repeat to add all required hostnames.
 - c. Click **Submit**. The new setting appears in the **Forwarding of Inbound Email to Your Mail System** section.

Routing for Outbound Mail During an Activation

To configure the path for outbound mail during an activation:

- 1 From the Administration Console, click **System Settings**.
- 2 Click **Email Routing**. The **Sending Outbound Email to External Recipients During an Activation** section displays the current setting.
- 3 To change the routing:
 - a. Click **Edit**.
 - b. In the **Routing Rules** section, select either:

- **According to MX records** (default) or
 - **Send via specific hosts**. A dialog box appears.
- c. If you selected specific hosts, enter the host name in the field and click **Add**. The hostname appears in the **Hosts in priority order** field above. Repeat to add all required hostnames.
 - d. Click **Submit**. The new setting appears in the **Outbound Email to External Recipients During an Activation** section.

Changing the Email Disclaimer

Only administrators logged in using the root account can change the email disclaimer.

To add disclaimer text to the end of each message sent by the service:

- 1 From the Administration Console, click **System Settings**.
- 2 Click **Email Disclaimer**. The **Email Disclaimer** screen appears.
- 3 In the **Disclaimer Text** field, type the organization's disclaimer.
- 4 Click **OK**.

Sync Notify Settings

During a Directory Sync, user and mailing list information is transferred to the data center. Users and mailing lists are deleted from the system if their information is not provided during the sync. This feature sends an email warning to Fault Alert list members if the percentage of users or lists deleted during a sync exceeds the threshold amount. See also ["Managing Fault Alerts" on page 50](#).

To configure the user/mailing list deletion percentage at which a warning message is sent:

- 1 From the Administration Console, click **System Settings**.
- 2 Click **Sync Notify Settings**.
- 3 In the **Sync Notification Settings** section, **Deletion Threshold** field, enter the percentage of deleted users or distribution lists above which you the system should send a warning email.
- 4 Click **Submit**.

Customizing the Home Page

The system allows you to control the information that appears to end users on the Email Security Services home page.

You can select which links appear in the **Preferences** section at the bottom of the home page, or hide the Preferences section entirely. Information about the link settings is provided in [Table 4-7](#).

Table 4-7 Home Page Preferences Links

| Link Name (Administration Console) | Link Name (displayed on Home Page) | Function |
|------------------------------------|------------------------------------|--|
| Notification Options | Notification Options | Collects basic contact information about users, such as alternate email accounts or cell phone numbers. |
| Home Address | Home Address | Collects end user home address information. |
| Contacts | Emergency Contacts | Collects emergency contact information from end users. |
| Change Password | Change Password | Allows end users to change their service password. Not available for organizations using Windows Authentication. |
| Help | Help | Displays online help for end users. |
| Wireless Settings | Enabling Wireless Forwarding | Allows end users to provide information used by the BlackBerry Forwarding service. |

To hide the Preferences section of the Home page:

- 1 In the Administration Console, click **System Settings**.
- 2 Click **Home Page Settings**.
- 3 In the **Preferences Section Settings** section, deselect the **Enable user preference** check box.
- 4 Click the **Submit** button at the bottom of the page.

To enable individual links in the Preferences section of the Home page:

- 1 In the Administration Console, click **System Settings**.
- 2 Click **Home Page Settings**.
- 3 In the **Preferences Section Settings** section, click the check box next to each item you want to display to end users. Depending on which services your organization uses, all items in the list may not apply.
- 4 Click the Submit button at the bottom of the page.

If Email Continuity is enabled for your organization, you can modify the message displayed to users when they log in during each of the Email Continuity states. (For information about Email Continuity states, see ["About Email Continuity" on page 1.](#))

If you want to include images or links in your message, you can do so using Bulletin Board (BB) code. For example, to add an image, include a link to the image between [IMG]link to image[/IMG]. To add a link, include the link between [URL]link[/URL].

To change the text displayed to end users in each state of Email Continuity:

- 1 In the Administration Console, click **System Settings**.
- 2 Click **Home Page Settings**.
- 3 In the **Custom Text Settings Active state text** section enter appropriate text for your organization when Email Continuity is in an active state.
- 4 Click the **Preview** button beneath the section to see how the text would appear to end users.
- 5 Repeat for the Ready and Recovery states.
- 6 Click the **Submit** button at the bottom of the page.

Customizing the Welcome Process

The welcome wizard leads new users through a series of pages that collect information your organization may need. You can choose which pages of the welcome wizard are included:

- Notification Options page
- Home Address page
- Emergency Contacts page

For more information on the welcome process and sending a welcome message to new users, see ["Welcoming New Users" on page 45.](#)

To select pages to include in the welcome wizard:

- 1 In the Administration Console, click **System Settings**.
- 2 Click **Welcome Settings**. The Welcome Process Settings page appears.
- 3 In the **Welcome Process Page Settings** section, click the check box next to each welcome wizard page you want to include.
- 4 Click **Submit**.

Changing Your Account Settings

Accessing Your Mailbox

When Email Continuity is active, you can access your webmail account directly from the Administration Console. Note that if you're logged in using the root account, the email account for emsroot is accessed. If you're logged in as an administrator with a personal Email Continuity account, your personal account is displayed.

To access your webmail account during an activation:

- 1 From the Administration Console Home, click **Your Account**.
- 2 Click **Access Your Mailbox**. The webmail account appears.

Viewing Undeliverable Mail in the Dropbox

If configured to do so, during an activation, Email Continuity places mail it cannot deliver (because it cannot resolve an address, or for some other reason) into a dropbox, where it is held until recovery. Administrators logged in using the root account can view undeliverable messages from the Administration Console.

To view undeliverable mail during an activation:

- 1 From the Administration Console Home, click **Your Account**.
- 2 Click **Access Email Continuity Dropbox**. The webmail inbox for the Dropbox appears.

Changing Your Password

You can change your password directly from the Administration Console. If you are logged in as an administrator, this feature allows you to change your personal administrator password. If you are logged in as a root administrator, this feature changes the root-level password.

CAUTION Changing Root Account Password

If you are logged in using the root account, you are changing the root password, which may be used by other people in your organization. Make sure you communicate changes to the root account password to others who must use it.

To change your password:

- 1 From the Administration Console Home, click **Your Account**.
- 2 Click **Change Password**. The **Change Password** screen appears.
- 3 In the **New Password** field, type the new password.
- 4 In the **Confirm Password** field, retype the new password.

- 5 Click **OK**.

Testing Email Continuity

To prepare for Email Continuity testing, determine an appropriate procedure for your organization. A Test Wizard walks you through the standard process.

To start a test of Email Continuity:

- 1 In the Administration Console **Current Tests** section, click **Start Test** to launch the test wizard.
- 2 Identify the mailboxes to include in the test.
 - a. Select the tab that indicates how you will identify mailboxes: **User Sets**, **Mailing Lists**, **Servers**, or **Users**.
 - b. If you select either the **Mailing Lists** or **Users** tab, search, locate, and select appropriate listings. If you select the **User Sets** or **Servers**, select the appropriate user sets or servers.
 - c. Click **Add**. Repeat until all appropriate selections display in the **Start test for these users** list box.
- 3 Click **Next**.

TIP User Sets Make Testing Easier and More Reliable

The easiest and most repeatable process includes maintenance of lists of users in testing User Sets. Select a test group from the **Saved User Sets** tab and click **Add the group to the Start Test list**. Click **Next**. Support recommends that you run tests with different groups of users.

When testing the service, you can edit the notification message to indicate that the activation is a test (recommended), use the default notification message, or bypass the notification message entirely.

- 4 Click **Next**. The message composition page containing the default message displays. Either:
 - Edit the Subject or Text of the message as needed, or
 - To bypass the notification message and continue with the test process, select **Don't send a notification message**.
- 5 Click **Next**. The **Confirmation** page provides information on the actions to be performed in the test.
- 6 Carefully review the contents of the **Confirmation** page and verify that these are the test parameters you want.
- 7 Click **Start Test**.

Upon activation, the service sends any requested notification message to the addresses you selected. (See ["Managing Transition Alerts" on page 50.](#)) During the test, Email Continuity activates all mailboxes for users you identified, allowing them to log in using the webmail interface.

When the test is underway, a **Current Tests** section displays in the Administration Console. Mail sent to users included in the test goes to their Email Continuity mailboxes.

In the list of users, those you included in the test display as In Test and those receiving email through the primary mail system display as Ready.

During the test, all affected users should log in to the webmail interface and use as many features as possible. When ready, the administrator can end the test and start the recovery process.

To start recovery from a test:

- 1 In the **Current Tests** section of the Administration Console, click **Start Recovery**.
- 2 Select the recovery type and click **Next**. A notification message composition page displays. As with the activation notification message, you can edit the message, use the default message, or bypass the message.
- 3 In the **Archive Name** box, type a name for the archive. This name displays when you use the RecoveryManager to restore messages to the primary mail system.
- 4 Click **Next**.
- 5 Click **Start Recovery**.

TIP Partial Activation Test Workaround

If the partial activation option is unavailable (Exchange 5.5 and Lotus platforms) a simple addressing standard has been implemented to facilitate the sending and receiving of email by users included in a test and using the webmail interface.

To use this standard, append a suffix available from Support (for example, emrs.company.com) to the ordinary email address. This forces the message to route to Email Continuity. For example, a test user with the email address aandrews@genericorp.com could receive email through the webmail interface through the email address aandrews@genericorp.com.emrs.company.com.

5 Activation

When your primary mail system experiences a disruption of service, you can activate Email Continuity and allow end users to access their email through the webmail interface.

Once the regular email system is functional, follow the recovery process to restore users' email data to the primary mail system.

Activating Email Continuity

When preparing for an activation, ensure that none of the internet gateway mail servers has a higher priority than the MTA hostname for Email Continuity (see the network settings document provided by Support). When the service is given highest priority, mail destined for the domain is routed to the Email Continuity MX record and users receive email via the service.

To activate Email Continuity:

- 1 Log in to the Administration Console (you must use an administrator account or the root account).
- 2 Ensure that all components are functioning properly; that is, that a green check mark precedes all items in the **Readiness Check** panel. If there are problems, contact Support for assistance.
- 3 In the Current ESS State panel, click **Activate**.

A rectangular button with a red border and a light gray background, containing the word "Activate" in bold black text.

NOTE Deleted Users In the Ready State Are Not Activated

Users that are deleted but in the Ready state will not transition to Active during an activation. Deleted users in the Active or Recovery states will transition during an activation or recovery like all other users. This may cause user statistics to appear out of sync in the SyncManager summary.

Notify users that Email Continuity is being activated. Notification messages are sent to the contact addresses listed in Email Continuity user profiles. When users receive this notification message, they can log in to the webmail interface to send and receive email.

- 4 Click **Next**. The message composition page containing the default message displays. Either:
 - Edit the **Subject** or **Text** of the message as needed, or
 - Select `Don't send a notification message`.

TIP Inform Users About Webmail Limitations

In your notification message, you should inform users that from within the webmail interface, they can:

- Send and receive email, attaching up to 12MB of data files to each message.
- View calendar information but not edit it.

Setting clear expectations for the webmail interface will help limit the number of calls made to the Help Desk during an activation

5 Click **Next**. The **Confirmation** page displays

6 Review the summary of the activation steps, then click **Activate**.

Note that the Administration Console now shows the state of the service as active. In the ACTIVE state, the service functions as the mail system for your environment. This state continues until your primary mail servers are back online and you choose to move to the RECOVERY state.

6 Recovery

The recovery process reintegrates archived messages into your primary email system.

Recovery Archives can contain:

- Messages sent or received by active users during an activation of Email Continuity. You can use Recovery Manager to bring these messages into your primary email system after the activation has ended.
- Messages sent or received during the time leading up to an activation of Email Continuity. You can use Recovery Manager to patch a data loss window between your last good backup and a failure of your email server.

See the following sections for procedures relevant to Recovery Archives:

- ["Starting Recovery from an Activation" on page 63](#)
- ["Restoring Mail to Users' Mailboxes" on page 64](#)
- ["Completing Recovery from an Activation" on page 72](#)

Starting Recovery from an Activation

The recovery process typically begins after restoration and testing of the primary mail system. The recovery process allows you to migrate users from Email Continuity back to the primary mail system.

To initiate recovery:

- 1 Log in to the Administration Console.
- 2 In the **Current ESS State** panel, click **Start Recovery**.

A rectangular button with a yellow-to-orange gradient background and a thin black border. The text "Start Recovery" is centered in a bold, black, sans-serif font.

Notify users entering the recovery process that the service is no longer active—they can resume using the primary mail system, and that the email data they sent and received during the activation period will be restored to their primary email. Notification messages are sent upon deactivation of a user's Email Continuity mailbox.

TIP **Remind Users to Run Custom Rules on Restored Mail**

After Recovery, users must manually run any custom rules that they have for filtering mail; you may want to remind them in the notification message.

- 3 Click **Next**. The message composition page containing the default message displays.
- 4 Edit the **Subject** or **Text** of the message as needed.
- 5 Click **Next**. The **Confirmation** page displays.
- 6 Click **Next**.

The RecoveryManager uses the recovery archive to deliver to end users' mailboxes the email data sent or received during the activation period. Give the archive any name that helps you identify it.

- 7 In the **Archive Name** box, type a name for the archive file (for example, Archive_10_12_06).
- 8 Click **Next**. The Administration Console displays a summary of all recovery steps to be taken.
- 9 Review the recovery steps summary.
- 10 Click **Start Recovery**. The recovery process begins.

The Administration Console displays status information on the recovery process. How long the recovery process takes depends on the quantity and size of email data sent and received during the activation period.

Restoring Mail to Users' Mailboxes

Use the RecoveryManager to restore email that was sent and received during the activation to end users' mailboxes. Whether you are recovering from a regular activation or a test, make sure you have created a recovery archive (during the initial recovery process) before launching the RecoveryManager.

NOTE Recovery and Blackberry Devices

If you subscribe to the Wireless Continuity for BlackBerry service, messages sent during an activation are accessible by Blackberry devices as well as the Email Continuity web interface (webmail). During recovery, those messages are recovered back into users' mailboxes from the Email Continuity service. Because those messages were also delivered to Blackberry devices during the activation, users can continue accessing them on Blackberry devices after recovery.

If you do not subscribe to the Wireless Continuity for BlackBerry service, messages sent during an activation are available only through the Email Continuity web interface (webmail). During recovery, those messages are recovered back into users' mailboxes from the Email Continuity service. Because the messages were never accessible to Blackberry devices during the activation, they are not accessible on Blackberry devices after recovery.

To restore email after an activation:

- 1 On the ESS server, from the Start menu, select **Programs > MessageLabs > RecoveryManager**.
- 2 Log into the RecoveryManager.
- 3 Click **Start Recovery**.

Select an EC Recovery Archive that contains mailboxes to import into your primary mail system and click Continue. EC RecoveryManager will automatically download archive data from the MessageLabs EC data center.

You also need to select a directory that EC RecoveryManager will use for downloaded archive data and during the recovery process.

Working directory: [Browse ...](#)

| Name | Mailboxes | Messages |
|------------------------|-----------|----------|
| Server_Crash_24_5_2008 | 2 | 2 |
| Open local archive ... | | |

[Refresh List](#) [Continue](#)

- 4 Select a working directory for RecoveryManager to use as a temporary data store during the import process. You can either:
 - Use the default directory
 - Click **Browse** and locate and select any directory with plenty of space, or
 - Type the path into the **Working Directory** field.

- 5 Select the appropriate archive from the list and click **Continue**.

This downloads metadata about the archive into the working directory. Actual mail data is downloaded for each user later in the process.

The screenshot shows the 'RECOVERY MANAGER Email Continuity' configuration window. At the top, it says 'Enter information about your mail system.' and 'EC RecoveryManager will use directory data to match existing users with their EC mailboxes. The mailbox access settings will be used to import mail into users' mailboxes.'

Platform: Lotus Notes (selected in a dropdown menu)

Directory Settings

In order to access user directory EC needs to know the full name of a Domino server and the password of the user on the local client.

Domino Server: HQMAIL01
Password: [masked]

Mailbox Access Settings

In order to access contacts EC needs the full name of a Domino server and the password of the user on the local client.

☒ Use same settings as Directory sync

Domino Server: HQMAIL01
Password: [masked]

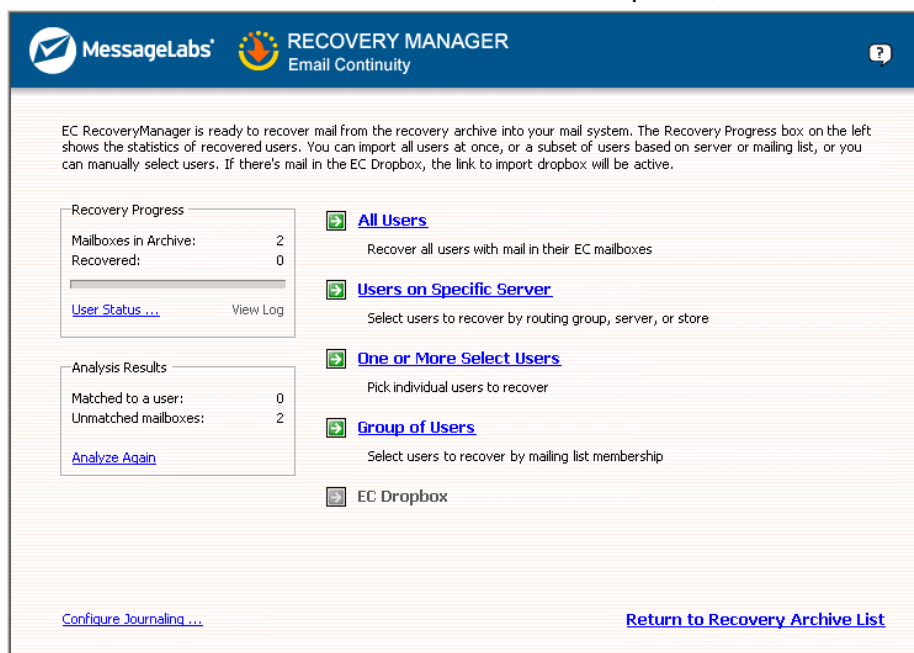
☐ Skip detailed analysis
The RecoveryManager relies on data from the last directory sync or recovery rather than a detailed comparison of your mail system directory to the recovery archive.

Back Continue

- 6 Configure mail settings. From the drop-down list, select Lotus Notes.
- 7 In the **Directory Settings Domino Server** box, enter the name of the Domino server to which the SyncManager should connect.
- 8 In the **Password** box, enter the password for the user with permissions on the Domino server.
- 9 In the **Mailbox Access Settings** pane, click the **Use same settings at Directory Sync** to select the Domino server and password identified in the fields beneath.
- 10 Typically, during a recovery, directory information is compiled as part of the process. In large environments, this step can be time-consuming. If SyncManager is installed, and if the most recent Directory sync was successful, RecoveryManager can use the cached results from the Directory sync for the recovery process. To use this cached data, select the **Skip detailed analysis** check box.

11 Click **Continue**.

Email Continuity analyzes the recovery archive to match up mailboxes in the archive to users' mailboxes in the primary mail system. This process can take several minutes. When it completes, click **Continue**.

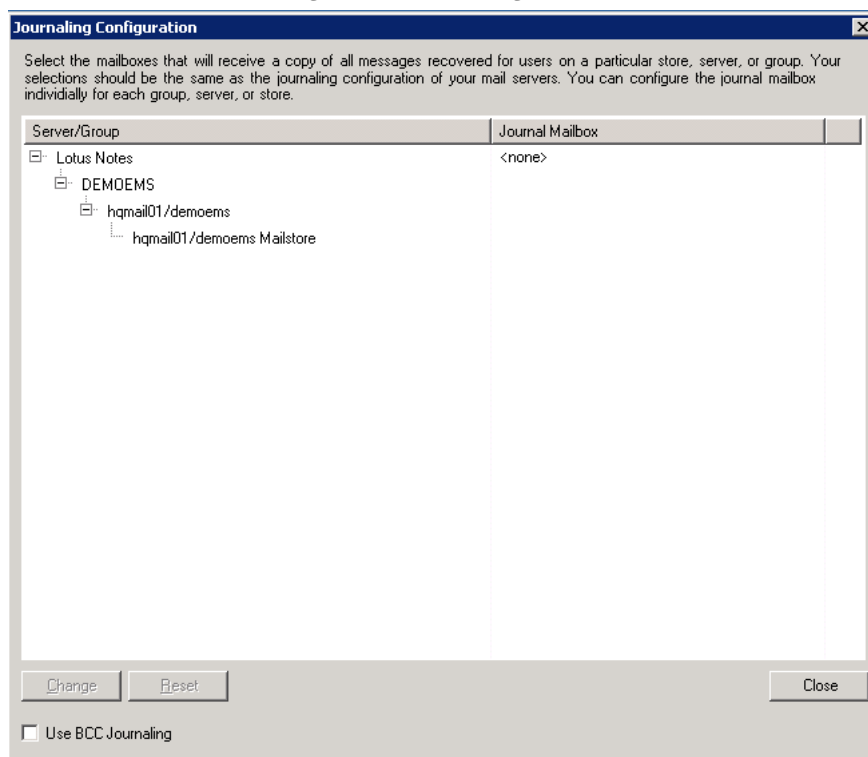


The Select Users page controls the scope of the user set. Status indicators display in the left column of the page.

- **Recovery Progress**—Displays the total number of mailboxes and the number recovered.
- **User Status**—Displays the status of each individual user. The display includes user names per server, user accounts with email data for recovery, and user accounts that cannot be matched to an account on the primary mail system.
- **Analysis results**—Displays how many user accounts can and cannot be matched to an account on the primary mail system. This also provides an option for reanalysis of the archive.

- 12** If your organization uses a third-party journaling product, you can configure RecoveryManager to place copies of recovered email into a mailbox for the journaling product. To do this:

a. Click **Configure Journaling**.



- b.** Usually, the identity of the recipient of a BCC email is not exposed when mail is recovered to a journaling mailbox. You can configure the service to append the recipient's email address to the BCC field in BCC mail recovered to the journaling product. If you're recovering the mail to an alternate mailbox, the alternate mailbox's address will be

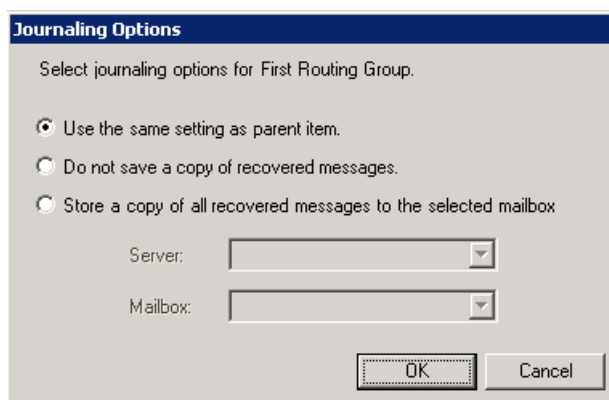
appended as well. To do this, select the **Use BCC Journaling** check box. [Figure 6-1](#) shows the results of recovery with and without the BCC Journaling feature selected.

| Original Mail | |
|---|---|
| To: | |
| BCC: User A, User B | |
| Recovery Without BCC Journaling | Recovery With BCC Journaling |
| User A Mail Recovered to User A Mailbox | User A Mail Recovered to User A Mailbox |
| To: | To: Undisclosed |
| BCC: | BCC: |
| User A Mail Recovered to Journal Mailbox for A | User A Mail Recovered to Journal Mailbox for A |
| To: | To: Undisclosed |
| BCC: | BCC: User A |
| ----- | |
| User A Mail Recovered to Alternate Mailbox X | User A Mail Recovered to Alternate Mailbox X |
| To: | To: Undisclosed |
| BCC: | BCC: |
| User A Mail Recovered to Journal for Alternate Mailbox X | User A Mail Recovered to Journal for Alternate Mailbox X |
| To: | To: Undisclosed |
| BCC: | BCC: User A, User X |
| ----- | |
| User B Mail Recovered to User B Mailbox | User B Mail Recovered to User B Mailbox |
| To: | To: Undisclosed |
| BCC: | BCC: |
| User B Mail Recovered to Journal Mailbox for B | User B Mail Recovered to Journal Mailbox for B |
| To: | To: Undisclosed |
| BCC: | BCC: User B |
| ----- | |
| User B Mail Recovered to Alternate Mailbox X | User B Mail Recovered to Alternate Mailbox X |
| To: | To: Undisclosed |
| BCC: | BCC: |
| User B Mail Recovered to Journal for Alternate Mailbox X | User B Mail Recovered to Journal for Alternate Mailbox X |
| To: | To: Undisclosed |
| BCC: | BCC: User B, User X |

Figure 6-1 BCC Journaling Results

- c. Highlight the group, server or store you want to configure.

d. Click **Change**.

A dialog box titled "Journaling Options" with a blue header bar. Below the title bar, the text "Select journaling options for First Routing Group." is displayed. There are three radio button options: "Use the same setting as parent item." (which is selected), "Do not save a copy of recovered messages.", and "Store a copy of all recovered messages to the selected mailbox". Below these options are two drop-down menus labeled "Server:" and "Mailbox:". At the bottom right of the dialog are "OK" and "Cancel" buttons.

Journaling Options

Select journaling options for First Routing Group.

☒ Use the same setting as parent item.

☐ Do not save a copy of recovered messages.

☐ Store a copy of all recovered messages to the selected mailbox

Server:

Mailbox:

OK Cancel

e. Using the radio buttons, select whether to:

- Use the same setting as parent items
- Do not save a copy of recovered messages, or
- Store a copy of all recovered messages to the selected mailbox, and, using the drop-down lists, select the server and mailbox for the recovered mail.

f. Click **OK**. The RecoveryManager user selection screen reappears.

13 Select the set of users for recovery.

- **All Users**—The All Users option imports email data for all users who were activated during the outage, used the Email Continuity webmail interface, and for which data has not yet been recovered.
- **Users on a Specific Server**—The Users on a Specific Server option recovers email data for users on a selected message store, server, or group of servers. If you select this option, you must also:
 - (1) Check any combination of individual mail stores, servers, or servers for recovery. (Servers without users with recovery data are greyed out.)
 - (2) Click **Continue**.
- **One or More Select Users**—The One or More Select Users option recovers the mailbox of one user or the mailboxes of selected users by name. If you select this option:
 - (1) The page displays a list of the first 300 users, including users with email data for recovery and users who cannot be matched to any account on the primary mail system. If your organization has more than 300 users, search by name to find users not listed.
 - (2) Select the users to recover, then click **Add**.

TIP Viewing User Properties and Overriding User Recovery Destinations

To view information about a specific user, click a user's name and then click **Properties**. Information that displays includes which server hosts the user's mailbox and the number of size of messages in the user's Email Continuity mailbox. The Properties page also allows you to override the destination of the user's restored email data.

- **Group of Users**—The Group of Users option recovers users based on Lotus Notes group membership. When selected, the display lists all distribution lists with members who have email that needs recovery. If you select this option:
 - (1) Click a group to select it, then click **Add**.
 - (2) Click **Continue**.
- **Drop Box**—The Drop Box option provides a repository for email data received by Email Continuity for any recipients in your organization domains that it is unable to resolve. If there is no drop box, this option is unavailable. If you select this option:
 - (1) Select a mailbox to where all drop box content will be imported.
 - (2) In the primary mail system, log in to the selected mailbox, sort through the mail data, and manually forward each item to the appropriate recipient.

The summary screen displays the users identified for recovery.

14 Choose how recovered mail should be restored.

Recovery Options

☒ Recover to alternate folder

☐ Recover all messages to single mailbox

- a. To recover all mail from the activation to a designated folder within users' mailboxes, click the **Recover to alternate folder check box**, and, in the dialog box that appears, type a name for the folder.
- b. To recover all messages from the activation to a single mailbox (such as an administrator mailbox, for troubleshooting purposes), click **Recover all messages to single mailbox** and, in the dialog that appears, select the mailbox.
- c. To recover all messages to a single mailbox, but place them in a designated folder, complete both the **Recover to alternate folder**, and **Recover all messages to single mailbox** options.

- 15 During the recovery process, if RecoveryManager encounters any unmatched mailboxes, you can:
 - a. Click **Prompt to Manually Match a Mailbox** to select the correct server and mailbox for each user's account not automatically matched. If this option is chosen, whenever a mailbox cannot be matched, the following screen appears for you to select a mailbox.
 - b. Click **Skip Users without a mailbox** to reroute unmatched mailboxes later.
- 16 Click **Start Recovery** to begin importing data.
- 17 The RecoveryManager downloads email data from the Email Continuity server and imports it to the appropriate mailbox and mailbox folders. The **Progress** page displays the number of items that successfully imported, failed to import, or were skipped. To see the recovery status for each mailbox, click **View Log**.

NOTE C Cancelling Recovery

If you click **Cancel** to stop the recovery process and a mailbox is being processed, the process completes that mailbox before stopping.

- 18 When the mail for all selected users has completed recovery, click **Continue**.
- 19 If you need to recover additional mail, click **Select another archive to recover** to return to the RecoveryManager main screen. If not, select **Exit ESS RecoveryManager**.

NOTE Email Continuity Does Not Import Mail Twice

Even if users or mailboxes belong to more than one group, their data will only be imported once; the RecoveryManager skips already recovered user accounts, even if they are members of multiple distribution lists or groups.

Completing Recovery from an Activation

After successful restoration of all email data to users' mailboxes, return to the Administration Console and finalize the recovery process. This returns mailboxes to the READY state. Returning mailboxes to the READY state deletes email from the webmail interface.

WARNING Verify Mail Import was Successful Before Ending Recovery.

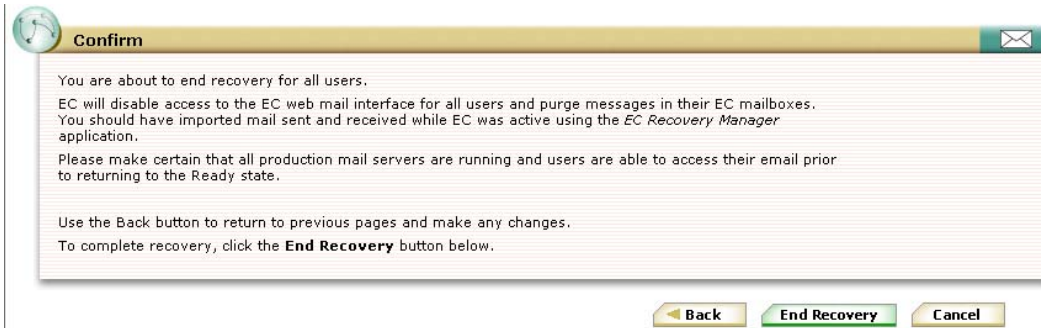
Ending recovery permanently deletes activation email data from the webmail interface. Ensure that all email data is successfully imported into the primary mail system before completing this process. All recovery archives can be downloaded for a period of 30 days after initial creation; however, after you end recovery in the Administration Console, the recovery archive no longer exists.

To complete recovery from an activation:

- 1 In the Administration Console **Current ESS State** panel, click **End Recovery**, which launches the Recovery Wizard.

A green rectangular button with the text "End Recovery" in black.

- 2 On the **Confirmation** page, click **End Recovery**. This purges the email archive from the data center and returns all activated mailboxes to the READY state.



Index

A

- Activation (Email Continuity)
 - defined 1
 - customizing message on log in screen 57
 - overview 61
 - reports 52
 - starting 61
 - starting recovery from 63
- Administration Console 22
- aliases, creating 44
- audit 52
- audit trail
 - for email routing configuration 53
 - viewing 52

B

- BCC Journaling 68
- browsers, supported
 - for administration 5
 - for users 6

D

- DNS 6
- dropbox 58

E

- Email Continuity
 - defined 1
 - activating 61
 - changing message to users during each state 57
 - completing recovery 72
 - starting recovery 63
 - states of 3
 - testing 59
 - welcoming users 45
- excluded users
 - changing status for multiple users 31
 - creating 40

F

- fault alerts
 - adding users to notification list 50
 - for user deletion during sync 55
 - readiness checks that trigger 24
- firewall requirements 6

G

- gateway requirements 6

H

- hardware
 - requirements 8
- help desk users 36
- home page 56
- HTTPS 5

I

- internet browsers. See browsers

L

- logging in
 - to Email Continuity via a welcome message 45
 - to the administration console 21
- login status of users 37
- Lotus Notes
 - account requirements 11
 - server software requirements 10

M

- message transfer agent
 - See MTA
- messages
 - adding disclaimer to 55
 - undeliverable placed in dropbox 58
- Microsoft Internet Connectivity Wizard 5
- Mozilla Firefox
 - See browsers
- MTA 6, 61
- MX Record
 - during activation 61
 - used for forwarding mail 54
 - used for sending outbound mail during activation 54

N

- networking requirements 5
- next hop routing
 - inbound, configuring 53, 54
 - inbound, described 7
 - outbound during activation, configuring 54
 - outbound during activation, described 8

O

- operating systems
 - supported 9

P

passwords
 changing administrator 58
 Email Continuity 26
 resetting multiple users' 26
 root account 13
 permissions
 help desk user 36
 preferences, editing home page 56
 proxy requirements 6

R

readiness checks
 overview 24
 sending fault alerts when failed 50
 Recovery
 defined 1
 completing 72
 starting (from an activation) 63
 RecoveryManager
 defined 1
 installation 13
 See also Recovery
 reminders, sending 48
 reports
 activation 52
 audit 52
 of users in the welcome process 48
 test 53
 requirements
 account 11
 communications 5
 firewall 6
 gateway 6
 hardware 8
 messaging software 9
 networking 5
 operating systems 9
 proxy 6
 server software 10
 service software 9
 root account
 logging in using 22

S

SMTP
 message gateway 6
 store and forward mail routing 7
 SyncManager
 defined 1
 configuring 16
 configuring user deletion to trigger alert 55
 installation 13

port used 5
 setting schedules for 16

T

test
 Email Continuity 59
 reports 53
 transition alerts 50
 transition reports 52

U

undeliverable mail 58
 users
 activating Email Continuity for 61
 adding manually to Email Continuity 44
 changing status in the system 31
 changing status of those who have opted out 31
 creating aliases for 44
 defining sets of 32
 deletion during sync, configuring warnings 55
 excluding from the service 31, 40
 granting administrative privileges to 35
 help desk 36
 login status of 37
 passwords for 26
 restoring mail to after an activation 64
 searching information 25
 sending reminders to 48
 updating contact information 32
 uploading sets of 32
 welcoming to the service 45

W

Warnings, See Fault Alerts
 welcome process
 about 45
 changing status for multiple users 31
 including pages in welcome wizard 57