



MessageLabs[®]
Now part of Symantec

Be certain

Email Security Services Administrator Guide

For Microsoft Exchange[®] 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	vii
About This Book	xi
Intended Audience	xi
Viewing the Document	xi
Conventions	xi
Product Documentation	xii
1 About the Service	1
Software Release Versions Included in this Book	1
About Email Continuity	2
About Windows Authentication	4
About Wireless Continuity for BlackBerry	5
About the Outlook Extension	7
About Historical Mail and Email Archive	9
Interaction of Components	11
2 Preinstallation	13
Communications Requirements	13
Networking Requirements	13
Firewall Requirements	14
Proxy Requirements	14
SMTP Message Gateway Requirements	14
Gateway Requirements	14
Mail Routing Inbound—Store and Forward	15
Mail Routing—Outbound During Activation	16
Historical Mail Routing Requirements	16
SMTP Connector	17
Hardware Requirements	17
Software Requirements	18
Service Software	18
Supported Operating Systems	19
Supported Messaging Software	19
Server Software Requirements	20
Exchange 5.5 Environments	20
Exchange 2000/2003 Environments	20
Exchange 2007 Environments	21
Coexistence Exchange Environments (2000/2003/2007)	22
Account Requirements	23
Exchange 5.5 Account Requirements	23
Exchange 2000/2003 Account Requirements	24
Exchange 2007 Account Requirements	25
Coexistence Environments Account Requirements	26
Virtualization	26
Windows Authentication Requirements	27
Windows Authentication Limitations	28
Wireless Continuity for BlackBerry Requirements	28
Wireless Continuity for BlackBerry Installation Prerequisites	29
Adding the Email Continuity Service Root Account to the Local Administrator Group	30
Enabling TCP and Name Pipes to Access the BES Database	30
Verifying that Mobile Data Services are Installed and Configured	31
Wireless Continuity for BlackBerry Supported Configurations	32
Wireless Continuity for BlackBerry Limitations	32

Outlook® Extension Requirements.....	33
Outlook Extension Limitations.....	34
Planning RedirectorSink/RedirectorController Placement.....	35
RedirectorSink Placement.....	35
RedirectorController Placement.....	36
Historical Mail Requirements.....	39
AlertFind Integration Requirements.....	40
AlertFind Integration Limitations.....	40
3 Installation and Configuration.....	43
Installing Service Software.....	43
Configuring the SyncManager.....	49
Configuring RedirectorManager.....	57
Installing RedirectorManager on a Standalone Server.....	58
Upgrading RedirectorManager.....	59
Installing RedirectorSink on Clustered Exchange Servers.....	59
Installing the RedirectorAgent.....	60
Provisioning Wireless Continuity for BlackBerry.....	62
Synchronizing RIM Data.....	62
Distributing the Client Agent.....	63
Distribution Over-the-Air for BES 4.x.....	64
Distribution Over-the-Air for BES 5.x.....	67
Sending the Agent to Users by Email.....	71
Installing the Outlook® Extension.....	72
Enabling User Authentication Through the Command Line.....	75
Manual Installation.....	76
Installation Using Group Policy.....	77
Installation Using Systems Management Software (SMS).....	79
Troubleshooting Installation of the Outlook Extension.....	82
Installing Custom Forms in Exchange 2000/2003 (Storage Management Only).....	83
Installing Custom Forms in Exchange 2007 (Storage Management Only).....	85
Installing Historical Mail/Email Archive.....	86
Configuring VaultBoxes.....	90
Changing Settings in the VaultBox Console.....	90
Monitoring VaultBoxes.....	92
4 Administration.....	97
Logging Into the Administration Console.....	97
Administration Console Home.....	98
Readiness Checks.....	100
Authentication Manager Status.....	102
RedirectorController/RedirectorSink/RedirectorAgent Status.....	102
Historical Mail Administration.....	103
Retention Policies.....	103
Membership-based (Current Membership) Policies.....	104
Capture-Based Policies.....	104
User Classification Retention Policies.....	105
Retention Policy Best Practices.....	107
Creating Retention Policies.....	108
Using Retention Policies to Implement Legal Holds.....	111
Query-Based Legal Holds.....	112
Storage Management.....	112
Creating Storage Management Policies.....	112
Configuring Scanning and Data Transfer from the VaultBox Console.....	115
Harvester Operation and Data Logging.....	118
Removing (Unstopping) Files for a User.....	120

Storage Reports	121
Reviewer Groups	122
Advanced Reviewer Searches	124
Search Limitations	128
Replication Zones	128
Email Recovery Archives	129
User Administration	131
Searching User Information	131
Resetting User Passwords.....	133
Resetting an Individual User's Password	133
Resetting Multiple Passwords By Template	133
Resetting Multiple Passwords by CSV Import	135
Changing Status for Multiple Users.....	138
Updating a User's Contact Information	139
Defining User Sets	139
Assigning Super Administrator Privileges	141
Assigning Email Continuity Administrator Privileges	143
Assigning Help Desk Privileges	144
Reviewing Login Status.....	145
Exporting Users' Contact Information	147
Excluded Users	149
Resolving User ID Conflicts Manually	150
Enabling BlackBerry Forwarding	152
Configuring a BlackBerry for Use with BlackBerry Forwarding	153
Wireless Continuity for BlackBerry Administration.....	154
Managing Users and Devices	154
Using Device Menu Options in Standard Display Mode	156
Using Device Menu Options in Advanced Display Mode	156
Viewing Device Advanced Display Information	157
Outlook® Extension Administration	157
Mailboxes and Aliases	158
Adding Mailboxes (Users) Manually.....	158
Creating Aliases	159
Mailing Lists	159
Notification	159
Welcoming New Users	160
Sending Reminders.....	163
Managing Fault Alerts	164
Managing Transition Alerts	165
Sending Custom Notifications	166
Viewing Audit Reports	167
Activation Reports	167
Test Reports.....	168
Mail Searches Reports	168
Reviewer Groups Reports	169
User Classification Reports	170
Modifying System Settings	171
Changing User Attributes Imported from Active Directory	172
Displaying Global Address List (GAL) Attributes.....	173
Configuring Email Routing	173
Routing for Forwarded Mail	174
Routing for Outbound Mail During an Activation	174
Changing the Email Disclaimer	175
Resolving User ID Conflicts Automatically	175

Sync Notify Settings	176
Customizing the Home Page	176
Customizing the Welcome Process	178
Changing Your Account Settings.....	178
Accessing Your Mailbox.....	178
Viewing Undeliverable Mail in the Dropbox.....	179
Changing Your Password	179
Testing Email Continuity	180
5 Activation.....	183
Activating Email Continuity	183
6 Recovery.....	187
Starting Recovery from an Activation	187
Restoring Mail to Users' Mailboxes	189
Completing Recovery from an Activation.....	200
Recovering Mail from Discovery Archives	201
Index.....	207

Task Reference

To grant service account permissions for Exchange 5.5:.....	23
To grant Exchange administrator permissions for Exchange 2000/2003:.....	24
To grant Send As and Receive As permissions:.....	25
To add the Email Continuity account to the local administrator group of the BES group:.....	30
To enable TCP and Name Pipes to have access to the BES database:.....	30
To verify that the MDS server is a push server and has an appropriate listening port configured:.....	31
To set IT policies:.....	32
To install service software:.....	43
To launch the SyncManager Setup Wizard manually:.....	50
To configure the SyncManager:.....	50
To configure distributed synchronization with SyncManager:.....	57
To install RedirectorManager:.....	58
To install RedirectorSink on clustered Exchange servers:.....	59
To install the RedirectorAgent:.....	61
To remove the RedirectorAgent:.....	61
To synchronize RIM data:.....	62
To download the client agent:.....	64
To configure the agent:.....	65
To assign software applications to users:.....	66
To remove the Blackberry agent for all users:.....	66
To remove the Blackberry agent for one user:.....	67
To prepare the shared application directory:.....	67
To update your IT policies:.....	69
To download the client agent:.....	69
To add the client application to BAS:.....	69
To create and populate application policies:.....	70
To create and populate the software configuration:.....	70
To create a BlackBerry client user group:.....	71
To assign the software configuration to the BlackBerry client user group:.....	71
To send installation instructions to device users:.....	71
To authenticate users through the command line (prior to Outlook Extension deployment):.....	76
To install the Outlook Extension manually using setup.exe:.....	76
To remove the Outlook Extension manually:.....	77
To install the Outlook Extension using Group Policy:.....	77
To upgrade the Outlook Extension using Group Policy:.....	78
To remove the Outlook Extension using Group Policy:.....	78
To install the Outlook Extension using SMS:.....	79
To upgrade the Outlook Extension using SMS:.....	79
To remove the Outlook Extension using SMS:.....	81
To add a new folder to Exchange Organizational Forms Library in Exchange 200/2003:.....	83
To publish forms to the Exchange Organizational Forms Library:.....	84
To create an organizational forms library in Exchange 2007:.....	85
To publish forms to the Exchange Organizational Forms Library:.....	86
To install the Historical Mail software on a VaultBox system:.....	87
To change data transfer settings:.....	91
To log into the Administration Console:.....	98
To configure Manual Retention (User Classification) Task schedule settings:.....	105
To create a retention policy:.....	109
To add users to a retention policy:.....	110
To prioritize retention policies:.....	111

To remove a Legal Hold from a collection of messages:.....	112
To create a storage management policy:	114
To prioritize storage management policies:	115
To change data transfer settings for Storage Management:	116
To configure Storage Management parameters:	117
To unstub all messages for a user:	120
To view storage reports:	122
To create a reviewer group:.....	123
To build advanced searches:.....	126
To assign servers to replication zones:	129
To create a Time-based Recovery Archive:	130
To create an Activation-based Recovery Archive:.....	131
To search user information:	132
To reset a user's password:	133
To change multiple users' passwords:	134
To create a password import CSV file:	135
To import passwords by CSV file:	137
To change status flags for users:	138
To edit a user's contact information:.....	139
To create a user set:.....	140
To create a super administrator:.....	142
To remove super administrator privileges:	142
To assign administrative privileges to an account:	143
To remove administrative privileges from an account:	143
To grant a user Help Desk privileges:	144
To remove Help Desk privileges from an account:.....	144
To review login status:.....	145
To generate a CSV spreadsheet of emergency contact data for all users:	149
To exclude a user:	149
To remove individual users from the Excluded list (reinstate them in the system):.....	149
To remove multiple users from the Excluded list (reinstate them in the system):	150
To resolve multiple user ID conflicts using CSV upload:	151
To resolve user ID conflicts individually:.....	151
To set up a BlackBerry device:.....	153
To manage BlackBerry user information in the Administration Console:	154
To view information about a device using the interface installed with the device agent:.....	155
To enable or disable the Extension:	158
To export the list of users:	158
To add a mailbox (user) to Email Continuity:.....	158
To create an alias:	159
To view mailing lists and members of each list:	159
To send a welcome message to one or more users:.....	162
To automatically send welcome messages to new users:.....	162
To send a reminder:	163
To add a user to the fault alerts list:	165
To remove a user from the fault alerts list:	165
To add users to the transition alerts list:.....	165
To remove a user from the transition alerts list:	165
To send a custom message:	166
To view an Activation report:	167
To view a Test report:.....	168
To run a Mail Searches report:	168
To run a Reviewer Groups Report:.....	170
To run a User Classification Report:.....	170

To change the attributes imported from Active Directory:	172
To change the attributes displayed in Global Address List:.....	173
To restore an attribute that has been removed:	173
To configure the path for forwarded mail:	174
To configure the path for outbound mail during an activation:.....	174
To add disclaimer text to the end of each message sent by the service:	175
To configure the method by which user ID conflicts are resolved:	175
To configure the user/mailing list deletion percentage at which a warning message is sent:	176
To hide the Preferences section of the Home page:	177
To enable individual links in the Preferences section of the Home page:	177
To change the text displayed to end users in each state of Email Continuity:	177
To select pages to include in the welcome wizard:	178
To access your webmail account during an activation:	178
To view undeliverable mail during an activation:	179
To change your password:	179
To start a test of Email Continuity:.....	180
To start recovery from a test:.....	181
To activate Email Continuity:	183
To initiate recovery:	187
To recover email from an activation or from a recovery archive:.....	189
To complete recovery from an activation:.....	200
To recover a Discovery Archive:.....	201

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 xi.
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> .
	Information that applies only to the Outlook Extension, an optional feature.	
	Information that applies only to Wireless Continuity for BlackBerry, an optional feature.	
	Information that applies only to Historical Mail, an optional feature.	

Product Documentation

The following documentation is available for Email Continuity:

- *Email Security Services Administrator Guide*
This book is a comprehensive document for installing, configuring, and administering the Email Security Services suite of products.
- *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.

The following materials are available for Email Archive:

- *Email Security Services Administrator Guide*

This book is a comprehensive document for installing, configuring, and administering the Email Security Services suite of products.

- *Email Archive User Guide*

This document explains how to use Email Archive, such as how to access and search historical email.

- *User's Guide to Storage Management*

This document describes how the storage management features works, and teaches users how to view stored documents.

- *Email Archive Search Help page*

Accessible from the Archive Search page in the user interface, the Email Archive Search Help page provides guidance on using the simple and advanced search modes.

For the latest version of any document, contact Support.

1 About the Service

The Email Security Services suite of products provides a total solution for email and BlackBerry® continuity, recovery, archiving, and security. Depending on your organization's implementation, some of the features described in this guide may not appear to you.

Software Release Versions Included in this Book

This guide is current up to the following released versions of Email Security Services software. For information on features or limitations described in subsequent releases, refer to the Release Notes or contact Support.

Table 1-1 Software Release Versions

Software	Description	Documented Version	How do I know what version I have?
Data center/ Administration Console	Software installed in the data center. Changes made to this software may be visible in the Administration Console, or may not be visible at all to administrators or end users.	6.5	Administration Console > About
Client-side installed software	SyncManager, RecoveryManager, and other software components installed in your organization's environment.	6.3.5	Start one of the client-side programs (such as Start > Programs > MessageLabs > SyncManager.) The version number appears on the opening screen.
Outlook Extension	Software installed on an end-user's machine to support the multiple features of the Outlook Extension.	6.2	Tools > Options > MessageLabs Email Continuity > About
Wireless Continuity for BlackBerry	Agent software distributed to user's devices.	6.2	Administration Console > Blackberry Administration > Export > Export. Sort by Agent Version to see all software versions.

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.

If the Outlook[®] Extension has been installed on end-user's desktops, they can continue to access their email using Outlook[®] in cached mode.

Email Continuity consists of the following components:

Table 1-2 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, calendar 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.
RedirectorSink™	An SMTP Event Sink that enables dynamic rerouting of messages, allowing some users to remain on the primary mail system while others use Email Continuity—a process called <i>Partial Activation</i> . Also transfers copies of mail to the VaultBox for users of Historical Mail.	Installed on one or more of customer's Exchange servers. Note that RedirectorSinks are the only components supported on Windows 2000 servers.
RedirectorAgent	A custom transport agent that performs functions similar to the RedirectorSinks to support the partial activation feature for Email Continuity in Exchange 2007 environments.	Installed on all customer's Exchange 2007 Hub Transport servers. The RedirectorAgent is not supported on Exchange 2007 Edge servers.
RedirectorController™ (also called the ESS Controller)	Software that communicates to the data center and provides updates to the RedirectorSinks and RedirectorAgents.	Installed in customer's environment.
RedirectorManager™	A centralized console to install, upgrade and maintain RedirectorSinks on standalone Exchange servers.	Installed in customer's environment.

Table 1-2 Components

Component	Description	Location
Authentication Manager	Allows end users to log in to the Email Continuity portal using their Windows user name and password.	Installed in customer's environment. For Windows Authentication only.
RIM Agent	A light-weight, java-based agent.	Installed on each BlackBerry device. For Wireless Continuity for BlackBerry service only.
VaultBox™	Software responsible for accepting mail from customer's Exchange servers, encrypting, compressing, and transferring it to the data center. Used for Historical Mail/ Email Archive.	Installed in customer's environment. Must be installed on a dedicated server; this can be the same server on which the SyncManager and RecoveryManager are installed, or a separate dedicated server.
Outlook® Extension	Software that provides access to certain Email Security Services features through a user's Outlook application.	Installed on end-user desktops.

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

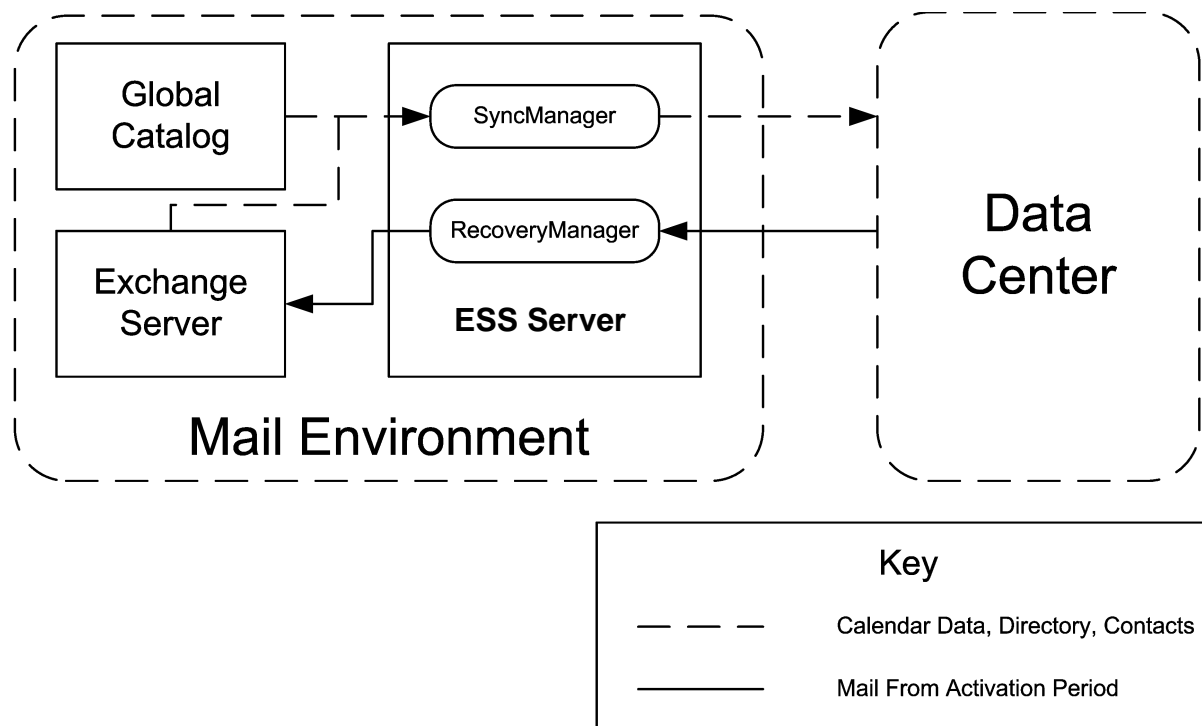


Figure 1-1 Email Continuity Data Transfer

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](#).

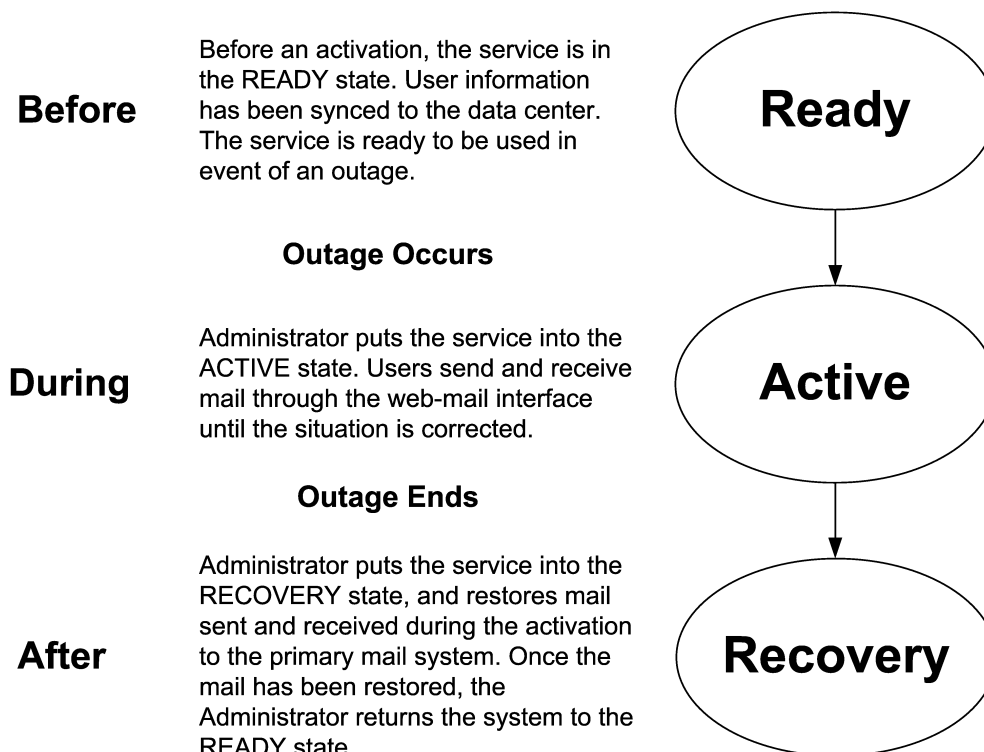


Figure 1-2 Email Continuity States

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 176](#).

About Windows Authentication

The Windows Authentication feature allows your users to log in to the Email Continuity portal using their regular network passwords. To accomplish this, an Authentication Manager installed on a local machine in your environment validates a user's credentials with the local Windows subsystem using New Technology LAN Manager (NTLM). If the user's credentials are correct according to the local Windows subsystem, the Authentication Manager reports this to the data center, and the user is allowed to log in to the Email Continuity portal. MessageLabs does not synchronize users' passwords from Active Directory.

If the Windows subsystem determines the login credentials are invalid, Email Continuity (and Windows, if applicable) increments the failed login count by one, and access to Email Continuity is denied.

If the Windows subsystem cannot determine if the login credentials are valid or invalid, the validation request is passed to a different Authentication Manager. The request is discarded if none of the Windows Subsystems can determine if the credentials are valid or invalid, or if two minutes elapse, whichever comes first.

For more information, see:

- ["Windows Authentication Requirements" on page 27](#)
- ["Windows Authentication Limitations" on page 28](#)
- ["Authentication Manager Status" on page 102](#)

About Wireless Continuity for BlackBerry



The Wireless Continuity for BlackBerry feature ensures messages are delivered to BlackBerry users when Email Continuity is active. BlackBerry agents version 6.2 and higher can also deliver messages to BlackBerry users if the BES fails along with the primary email system.

The SyncManager collects data about the BlackBerry users from the BES, then the RIM Agent installed on each BlackBerry device provides seamless email delivery and retrieval during outages.

- Prior to an activation, SyncManager software collects RIM[®] data, just as it collects other data related to your email system. Using remote calls, it retrieves required information from the database used for BlackBerry Enterprise Server (BES) management. You must have these databases configured prior to installing Wireless Continuity for BlackBerry.
- A MessageLabs agent is installed on each BlackBerry device. This agent can be deployed by way of the policy management features of BES 4.0+ (deployment over-the-air) or can be manually downloaded to the device through a hyperlink sent to the user through the Administration Console.
- The RedirectorController acts as a RIM data relay for posting push messages to the specified BES. The RedirectorController must be able to post HTTP requests to each configured BES, which must have functional

network connectivity to communicate with the BlackBerry handheld device. The Redirector Controller and BES must be online when an agent is first authenticated.

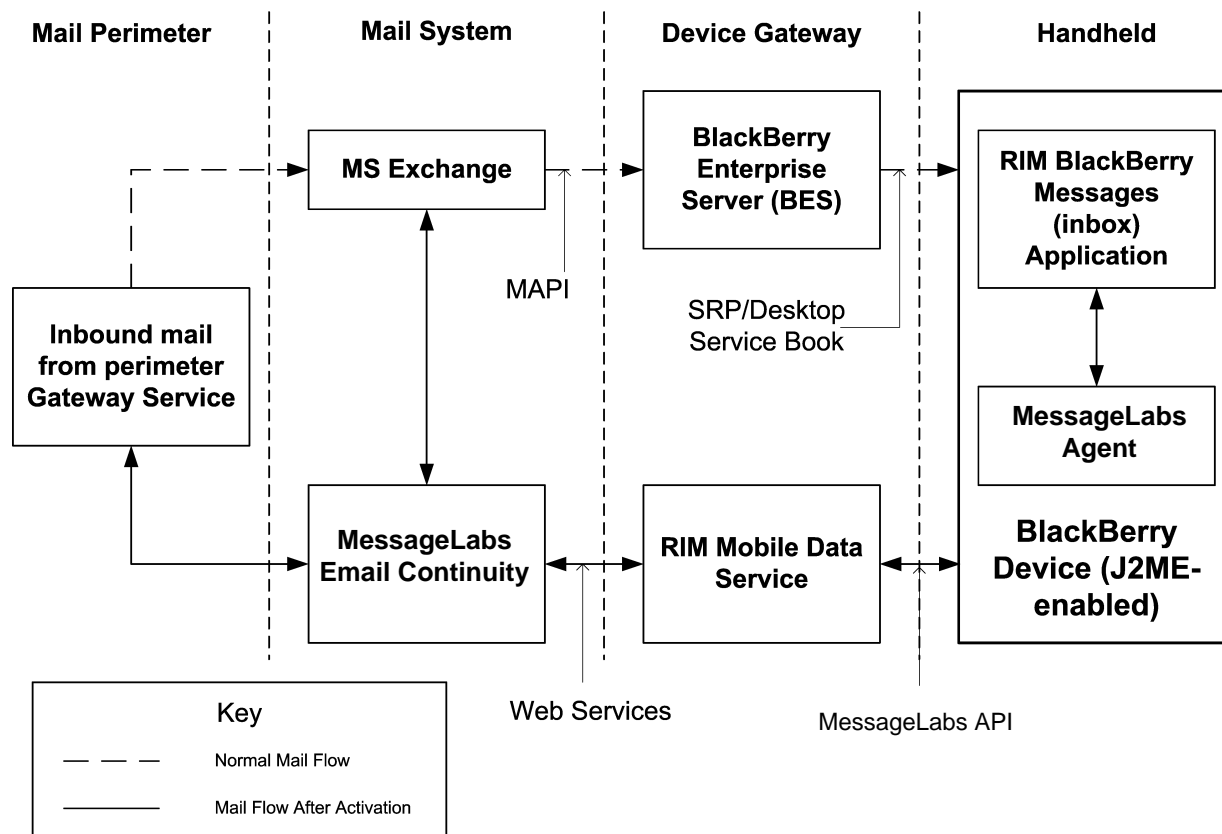


Figure 1-3 Wireless Continuity for BlackBerry Process

NOTE BES-Independent Wireless Continuity for BlackBerry

The ESS version 6.5 data center implements a BES-independent continuity model that allows BlackBerry users to compose, send, and receive email on their BlackBerry devices even if the BES has failed. This BES-independent continuity option works for any user who can establish a secure (HTTPS) internet connection from their BlackBerry device. This feature works only for organizations using the version 6.5 data center and the version 6.2 BlackBerry agent. Organizations using previous versions of the data center or agent software will notice no change to their Wireless Continuity for BlackBerry implementations.

Wireless Continuity for BlackBerry supports:

- Viewing text from Word, PDF, and HTML attachments. Formatting and images are not displayed.

- Viewing messages no larger than 64 KB in size (due to restrictions in the device software). If you receive larger messages, or messages that have attachments, Wireless Continuity for BlackBerry adds information to the end of the message stating that the entire message and/or attachment can be accessed by logging in to your Email Continuity web-mail account.
- Partial activation of Email Continuity, if your organization has purchased that feature.

NOTE BlackBerry Forwarding vs. Wireless Continuity for BlackBerry

The BlackBerry Forwarding option can be turned on for Email Continuity customers by Support. Wireless Continuity for BlackBerry, described here, is a separate product. To prevent receiving duplicate messages on the device during activation, your organization should be provisioned for only one of these services. For information on BlackBerry Forwarding, contact Support.

For more information, see:

- ["Wireless Continuity for BlackBerry Requirements" on page 28](#)
- ["Wireless Continuity for BlackBerry Supported Configurations" on page 32](#)
- ["Wireless Continuity for BlackBerry Limitations" on page 32](#)
- ["Provisioning Wireless Continuity for BlackBerry" on page 62](#)
- ["Wireless Continuity for BlackBerry Administration" on page 154](#)

About the Outlook Extension



When the Outlook Extension is installed on the end user's machine, and the end user has been authenticated (logged in/registered with Email Security Services), the Extension periodically polls the data center to see if Email Continuity has been activated. If so, then Outlook[®] goes into offline mode, and remains offline for the duration of the activation. While the service is active, MessageLabs delivers messages to the user's Outlook Inbox through Email Continuity.

When the activation period is over, messages sent and received during the activation using the Outlook[®] Extension are resynced by Exchange when Outlook[®] returns from offline mode. These messages are included in the Recovery archive, but are not restored during normal Recovery unless you direct the RecoveryManager to do so.

After an activation, Outlook returns to the same state it was before the activation occurred. For example, if Exchange was Offline before the activation, it will appear as Offline after the activation. Users can right-click the **Offline** button and reconnect to Exchange.

NOTE Proxy Servers

If your organization uses proxy servers, the Outlook Extension provides basic proxy authentication. The Outlook Extension provides a dialog box for a user to enter proxy server credentials (user name and password) to gain access to their email during an activation of Email Continuity.

NOTE When Email Continuity is active, only one instance of Outlook with the Extension installed can be open per user mailbox

If Outlook, with the Extension installed, is open on multiple machines pointing to the same mailbox, it is likely that each instance of Outlook will only receive a subset of the messages received during an activation.

Outlook, with the Extension installed, is similar to configuring a POP3 profile and deselecting the option to leave a copy of the message on the server; Each message is downloaded only by the first Outlook Extension instance running that polls for the message.

[Table 1-3](#) compares the features/functionality available to users through Email Continuity web-mail and the Outlook Extension. A ✓ means that the feature or function is available. A dash (—) means the feature or function is not available. To see known limitations for the Outlook Extension, see "[Outlook Extension Limitations](#)" on page 34.

Table 1-3 Outlook Extension/Email Continuity Webmail Feature Comparison

Outlook Functionality	Web-mail	Outlook Extension
Send/receive email	✓	✓
View calendars	✓	✓
Modify calendars	—	✓
View contacts	✓	✓
Modify contacts	—	✓
View Global Address List	✓	✓
View tasks	—	✓
Modify tasks	—	✓
Categories	—	✓
Folder management	Not applicable	✓
Message importance	✓	✓
Message sensitivity	—	✓
Access to PST folders	Not applicable	✓

Table 1-3 Outlook Extension/Email Continuity Webmail Feature Comparison

Outlook Functionality	Web-mail	Outlook Extension
Reminders window	—	✓
Send appointments	—	✓
Receive appointments	✓	✓
Access to free/busy information	—	—
Client-side rules (filters)	—	✓
Server-side rules and Out-of-Office	—	—
Delegate access (view others' mailboxes)	—	—
Delivery options	—	—
Support of HTML mail	✓	✓

For more information, see:

- ["Outlook® Extension Requirements" on page 33](#)
- ["Outlook Extension Limitations" on page 34](#)
- ["Installing the Outlook® Extension" on page 72](#)
- ["Outlook® Extension Administration" on page 157](#)

About Historical Mail and Email Archive



Historical Mail (also called ActiveMailbox) allows users to review designated historical email during an activation of Email Continuity using a searchable, web-based interface.

The maximum message size that can be fully indexed in the data center archive is 50 MB. Message bodies or individual attachments that are larger than 50 MB are partially indexed using their available header fields and metadata.

Historical Mail/Email Archive requires that you install VaultBox software on a dedicated server. This dedicated server can be the same one on which SyncManager, RecoveryManager, and other Email Security Services software is installed. VaultBox software captures, compresses, and transfers historical email to the data center. VaultBox components are described in [Table 1-4](#).

Table 1-4 VaultBox Components

Component	Description
Store Driver	A plug-in for Microsoft's SMTP Service that takes messages received by SMTP, compresses them, and writes them to the Compression Directory on the VaultBox.
Compression Directory	Storage location for all message that are pending transfer to the data center.
Transfer Service	Transfers the mail in the compression directory to the data center through SFTP (SSH) on port 22.
VaultBox Monitor	A service that gathers health information from the other services, reports it to the data center for display in the Administration Console, and logs it locally on the VaultBox. The VaultBox Monitor also restarts the Transfer Service if it has stopped or is unresponsive.
VaultBox Console	A graphical tool that is used to configure and monitor tasks and services on the VaultBox, including the Transfer Service, the MAPI and Exchange configurations, and the VaultBox Monitor.
Storage Management Task (Storage Management only)	A task that finds messages that are candidates for storage management, transfers them to the data center (through the Compression Directory and Transfer Service), and replaces the attachments in those messages with HTML pointers to the data center.
Harvester Service (Storage Management only)	A service that schedules the Storage Management Task. The Storage Management Task runs in a separate process from the service. Note that when using the Harvester Service, you should add the m1harvester service to your list of monitored services.
Import from Exchange command (Storage Management only)	A low level command that uses the Harvester Service to import selected messages from Exchange. This command requires a carefully constructed XML file, and that file can only be built by Support.

Data transfer using the VaultBox is shown in [Figure 1-4](#).

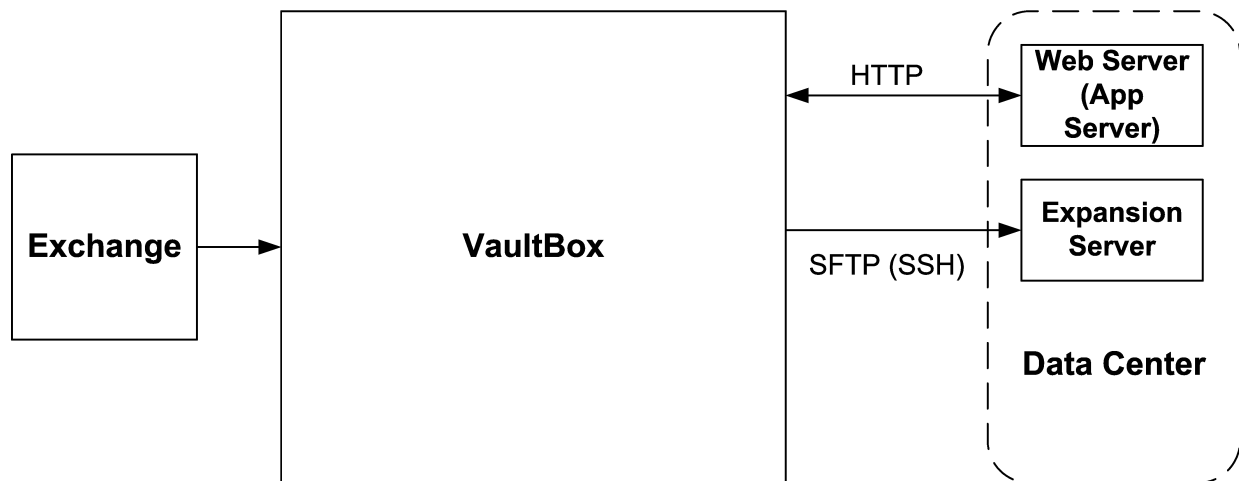


Figure 1-4 Data Transfer for Historical Mail

Interaction of Components

The interaction of components with Exchange 2000/2003 and the data center are shown in [Figure 1-5](#). Port numbers are shown in parentheses.

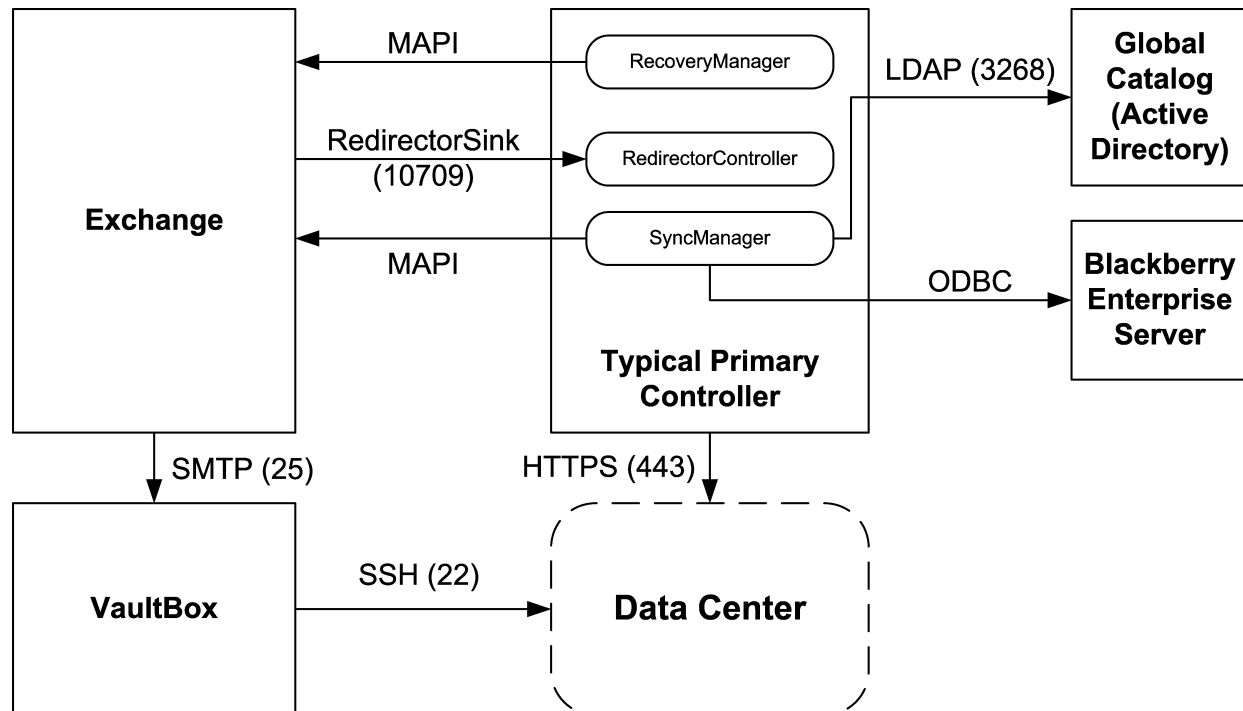


Figure 1-5 Communications Protocols and Port Numbers, Exchange 2000/2003

The interaction of components with Exchange 2007 and the data center are shown in [Figure 1-6](#). Port numbers are shown in parentheses.

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.

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.

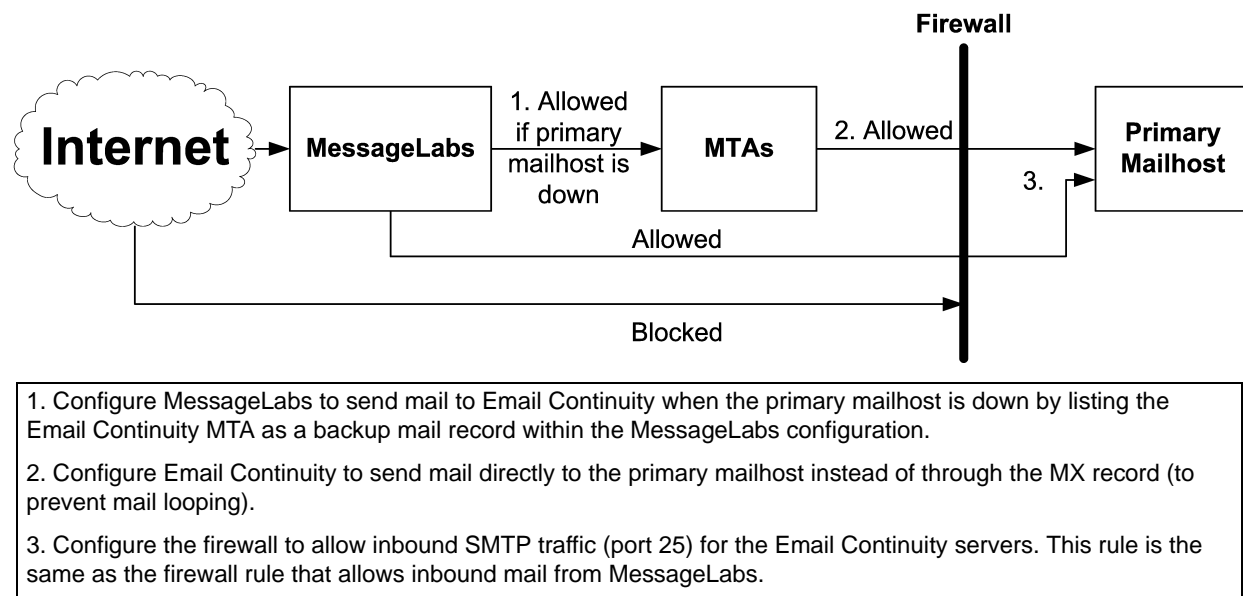
Gateway Requirements

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.

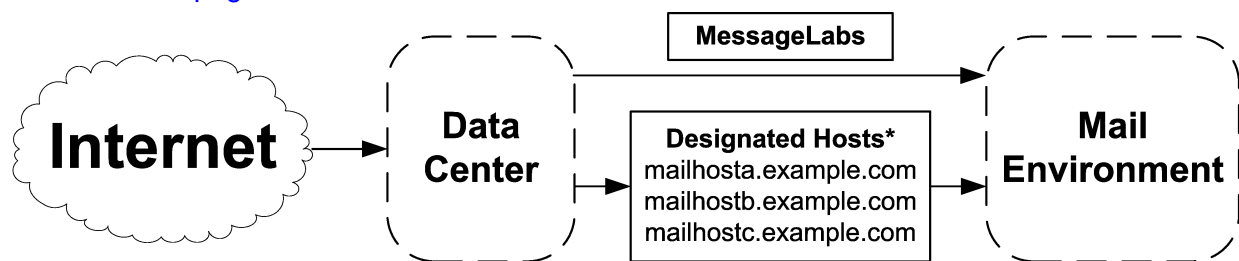
Figure 2-1 Mail Routing with MessageLabs

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.

Similarly, if your organization performs a partial activation, this feature allows you to designate hostnames to use to deliver mail to users who are not active on Email Continuity.

To configure email routing for inbound mail, see ["Routing for Forwarded Mail" on page 174](#)



*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 16](#).

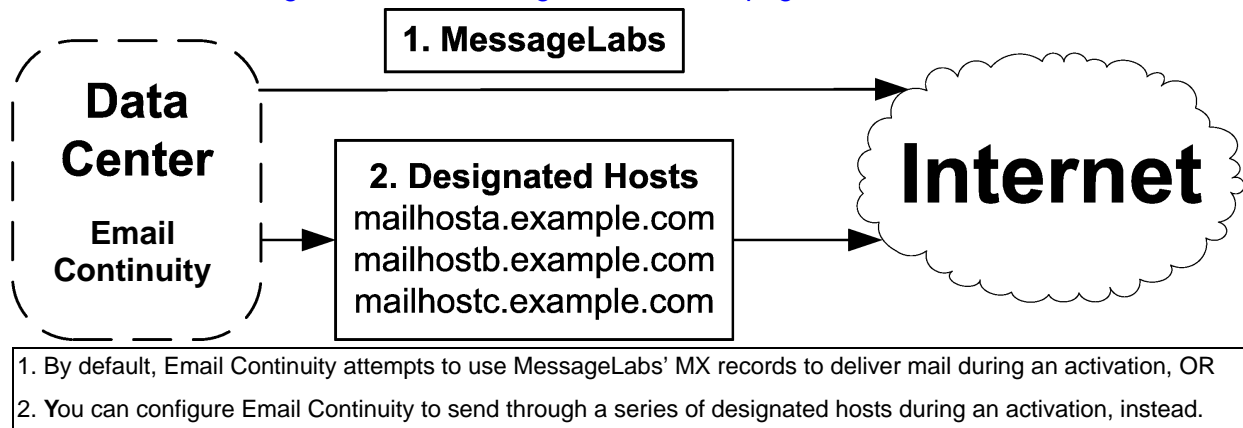


Figure 2-3 Outbound Mail Routing During Activation

Historical Mail Routing Requirements



Work closely with Support to determine the routing requirements for your organization. Because of the number of variables involved and the uniqueness of each network, it is not possible to provide a static requirements list.

Determining the routing requirements for your organization's Historical Mail implementation requires an understanding of your organization's Exchange routing topology and advanced knowledge of Exchange functionality. An analysis of the variables involved leads to the identification of your organization's preferred routing topology, which requires configuration of:

- Historical Mail replication zones, which include the primary and secondary VaultBox systems to which each particular Exchange server routes mail. You must assign Exchange servers to the replication zones.
- DNS zones and zones created in your internal DNS configuration
- Historical Mail MX records created in your internal DNS configuration

Correct implementation of the preferred routing topology not only allows for proper operation of the Historical Mail feature, but it limits the impact of Historical Mail deployment on your organization's environment. Variables considered in making this determination include, but are not limited to:

- General network topology

- Exchange routing groups
- Connections between locations, including bandwidth and latency
- Number of users at each location
- Number of and which users at each location will enable the Historical Mail feature
- Location of internet access points

Smaller organizations may have only one preferred routing topology; large organizations may have one or more per data center.

SMTP Connector



If you use an SMTP connector for sending outbound internet mail, and it is configured to use a smart host and not DNS, then you must create an additional SMTP connector for the Historical Mail address space that uses internal DNS for address resolution.

In this configuration, if the additional SMTP connector is not created for the Historical Mail address space, then the Exchange servers may route the mail that should go to the VaultBox systems out to the internet through the SMTP connector for internet mail.

For additional information on SMTP connector configuration for the Historical Mail feature, contact Support.

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.



If you plan to install Historical Mail, the VaultBox must have a dedicated server. You can use the same server on which SyncManager and RecoveryManager are installed, or you can dedicate a second, separate server to the VaultBox software. If you plan to install the RedirectorController, ensure that its server meets the requirements as well.

The recommended minimum hardware requirements for any machine designated as a VaultBox system are:

Table 2-2 Minimum Hardware Requirements, VaultBox

Component	Minimum Requirement
Processor	2.4 GHz Pentium 4-type
Memory	1 GB RAM
Disk Space	RAID 1, with adequate storage for seven times the estimated mail volume for Historical Mail users. A formula that may help you calculate the recommended storage is: $N = (Tf / 30) * 7$ where N is the RAID size in GB and Tf is 30 days of mail traffic (total internal and external traffic).

If you have questions about whether or not a machine meets VaultBox requirements, contact Support.

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.



For full use of Historical Mail features, your implementation must be running version 6.0 or later of the service software. To see which version you are running of a component, such as the Recovery Manager, select **Start > All Programs > MessageLabs > Recovery Manager**. The software launches, and the version number appears on the opening screen.




For full use of Wireless Continuity for BlackBerry features, your implementation must be running version 5.5 or later of the service software. To see which version you are running of a component, such as the SyncManager, select **Start > All Programs > MessageLabs > SyncManager**. The software launches, and the version number appears on the opening screen.

- 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 2-3](#).

Table 2-3 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
One or more VaultBox systems	Windows Server 2003 SP1/ Windows Server 2008	SP1 is required by Microsoft SQL Server 2005 Express Edition 

Supported Messaging Software

Email Continuity works with the following versions of Microsoft Exchange Server:

- Microsoft Exchange Server 5.5, Service Pack 4 or later
- Microsoft Exchange Server 2000, Service Pack 3 or later
- Microsoft Exchange Server 2003
- Microsoft Exchange Server 2007

Table 2-4 Supported Features/Exchange Configurations

Features	Exchange 5.5	Exchange 2000/2003	Exchange 2007	Coexistence (2000, 2003, 2007)
Email Continuity—full activation	Supported	Supported	Supported ^a	Supported
Email Continuity—partial activation	Not Supported	Supported	Supported	Supported
Historical Mail	Not Supported	Supported	Supported	Supported
Outlook Extension	Not Supported	Supported	Supported	Supported
Windows Authentication	Not Supported	Supported	Supported	Supported
Wireless Continuity for BlackBerry		Supported	Supported	Supported

a. Continuous Cluster Replication is supported for full and partial activations in Exchange 2007.

Exchange 2000/2003: If your organization uses active/active hardware clustering, be aware of the following:

- Email Continuity is supported for global activations.
- Partial activations of Email Continuity are not supported.
- Historical Mail/Email Archive is not supported.

Server Software Requirements

Exchange 5.5 Environments

Table 2-5 Software Requirements for Exchange 5.5



Software	Notes
ESS Server	
.NET Framework v. 2.0	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.
Microsoft Data Access Components (MDAC) 2.7 or later	If not already installed, the service software installation package includes this application. After its installation, you must reboot the computer before you can proceed with the service software installation.
Microsoft Outlook messaging and Collaboration client must NOT be installed.	
MAPI/CDO (Latest version)	Download from Microsoft

Exchange 2000/2003 Environments

Table 2-6 Software Requirements for Exchange 2000/2003 Environments

Software	Notes	
Email Security Services Server		
.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.	
Microsoft Data Access Components (MDAC) 2.7 or later	If not already installed, the service software installation package includes this application. After its installation, you must reboot the computer before you can proceed with the service software installation.	

Table 2-6 Software Requirements for Exchange 2000/2003 Environments (Continued)



Software	Notes	
Exchange System Management	For Exchange 2000, Exchange 2000 System Manager, Service Pack 3 or later	
	For Exchange 2003, Exchange 2003 System Manager	
Microsoft Internet Information Server (IIS) and simple mail transfer protocol (SMTP)	For the RedirectorManager to function properly, you must install, but can then disable, IIS services, including SMTP.	
	To use Historical Mail, you must have IIS services, including SMTP, enabled.	
Microsoft SQL Server 2005 Express	To use Historical Mail, you must have SQL Server 2005 Express. Though it is provided in the service software package, installation of this software can take 30 minutes or more; Support recommends that you install it prior to scheduling your service call.	
Microsoft Outlook messaging and Collaboration client must NOT be installed.		
Exchange 2000/2003 Server		
Microsoft Distributed Component Object Model (DCOM)	To use the RedirectorManager for remote RedirectorSink installation, you must allow communications using DCOM from the ESS Server to the Exchange Servers. If you cannot use DCOM, other installation methods are available; contact Support.	

Exchange 2007 Environments

Table 2-7 Software Requirements for Exchange 2007 Environments

Software	Notes	
Email Security Services Server		
.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.	
Microsoft Data Access Components (MDAC) 2.7 or later	If not already present on the ESS server, the service software installation package includes this application. After its installation, you must reboot the computer before you can proceed with the service software installation.	
MAPI/CDO (Latest version)	Download from Microsoft	

Table 2-7 Software Requirements for Exchange 2007 Environments (Continued)

Software	Notes	
Microsoft Internet Information Server (IIS) and simple mail transfer protocol (SMTP)	For the RedirectorManager to function properly, you must install, but can then disable, IIS services, including SMTP.	
	To use Historical Mail, you must have IIS services, including SMTP, enabled.	
Microsoft SQL Server 2005 Express	To use Historical Mail, you must have SQL Server 2005 Express. Though it is provided in the service software package, installation of this software can take 30 minutes or more; Support recommends that you install it prior to scheduling your service call.	
Microsoft Outlook messaging and Collaboration client must NOT be installed.		
Exchange 2007 Servers		
If the Exchange 2007 server was not installed with support for pre-Outlook 2007 clients, you must create a Public Folder store	<ol style="list-style-type: none"> 1 Launch the Exchange Management Console. 2 Expand the Server Configuration node, and select the Mailbox node and server on which you want to create the Public Folder store. 3 In the Storage Management tab, select the storage group you want to contain the public folder database. 4 In the Actions pane, click New Public Folder database. Name the database, assign a path, then click New. 5 Stop, then restart, the MExchangeIS service. 	
Configure Offline Address Book for Outlook 2003 and earlier clients.		

Coexistence Exchange Environments (2000/2003/2007)

Table 2-8 Software Requirements for Coexistence Environments (2000/2003/2007)

Software	Notes
ESS Server	
.NET Framework v. 2.0	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.

Table 2-8 Software Requirements for Coexistence Environments (2000/2003/2007) (Continued)

Software	Notes
Microsoft Data Access Components (MDAC) 2.7 or later	If not already installed, the service software installation package includes this application. After its installation, you must reboot the computer before you can proceed with the service software installation.
Exchange System Management	Exchange 2000 System Manager, Service Pack 3 or later, 2003 System Manager, MAPI/CDO (Latest version) Download from Microsoft
Microsoft Internet Information Server (IIS) and simple mail transfer protocol (SMTP)	For the RedirectorManager to function properly, you must install, but can then disable, IIS services, including SMTP
Microsoft Distributed Component Object Model (DCOM)	To use the RedirectorManager for remote RedirectorSink installation, you must allow communications using DCOM from the ESS Server to the Exchange Servers. If you cannot use DCOM, other installation methods are available; contact Support.
Microsoft Outlook messaging and Collaboration client must NOT be installed.	

Account Requirements

Exchange 5.5 Account Requirements

Table 2-9 Account Requirements, Exchange 5.5

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.
Service Account Administrator Permissions	Administrator permissions required for the service account on the Organization, Site, and Configuration containers.

To grant service account permissions for Exchange 5.5:

- 1 In the Exchange 5.5 Administration Console, select `Organization` from the top of the left tree.
- 2 From the **File** menu, select `Properties`. The **Properties** dialog displays.

- 3 Select the **Permissions** tab. Then, to select the account for use by the Email Continuity service, click **Add**.
- 4 From the **Roles** drop-down list, select `Service Account Admin`. Click **OK**.
- 5 Repeat for each of the Site and Configuration containers.

Exchange 2000/2003 Account Requirements

Table 2-10 Account Requirements, Exchange 2000/2003

Account	Notes
ESS Server	
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.
Service Account Administrator Permission	ESS requires <code>Exchange Admin</code> permissions at the Organization level, as well as <code>Send As</code> and <code>Receive As</code> permissions on each mailbox store.
Exchange Servers	
Local Administrator Permissions on Exchange Servers	For remote deployment of <code>RedirectorSinks</code> using the <code>RedirectorManager</code> . You could also deploy <code>RedirectorSinks</code> using a different account that has local administrator permissions.

To grant Exchange administrator permissions for Exchange 2000/2003:

- 1 In the Exchange System Manager, right-click the **Organization** name (top level) and, from the pop-up menu, select **Delegate Control**. Click **Next**.
- 2 Click **Add** and then **Browse**. Select the account ESS will use. Then, for **Role** select `Exchange Administrator`.
- 3 Right-click **Administrative Group** and, from the pop-up menu, select **Delegate Control**. Click **Next**.
- 4 Verify that the ESS service account displays as being *inherited*. If, after 15–20 minutes, this is still not displayed, add the ESS account to each administrative group.

To grant Send As and Receive As permissions:

- 1 In the Exchange System Manager, expand the left tree until all expanded storage groups display. For each mailbox store, go to **Properties** and select the **Security** tab.

NOTE Public Folder Stores

You do not need to modify permissions on public folder stores.

- 2 Click **Add**. Select the account that ESS will use. Click **OK**. Verify selection of the account and that **Send As** and **Receive As** permission options show as selected (black check box).
- 3 Repeat for each mailbox store on each Exchange 2000/2003 server.

Exchange 2007 Account Requirements**Table 2-11 Account Requirements, Exchange 2007**

Account	Notes
ESS Server	
ESS Service Account	A <i>service account</i> , under which all service processes run, must be created on the ESS server. This user must be a member of the domain and the local administrator group on the ESS server.
Exchange 2007 Servers	
Send As permissions for the Service Account on 2007 Exchange Servers	Link to instructions Get-Mailboxdatabase Add-ADPermission -User [service account] -ExtendedRight "send as" [service account]=display name Plan at least two hours for permissions to propagate.
Receive As permissions for the Service Account on 2007 Exchange Servers	Link to Instructions Get-Mailboxdatabase Add-ADPermission -User [service account] -ExtendedRight "receive as" [service account]=display name Plan at least two hours for permissions to propagate.

Coexistence Environments Account Requirements

Table 2-12 Account Requirements, Coexistence Environments

Account	Notes
ESS Server	
ESS Service Account	A <i>service account</i> , under which all service processes run, must be created for use on the ESS server. This user must be a member of the domain and the local administrator group on the ESS server.
Service Account Administrator Permission	Email Continuity service requires <code>Exchange Admin</code> permissions at the Organization level, as well as <code>Send As</code> and <code>Receive As</code> permissions on each mailbox store.
Exchange 2000/2003 Servers	
Local Administrator Permissions on Exchange Servers	For remote deployment of <code>RedirectorSinks</code> using the <code>RedirectorManager</code> . You could also deploy <code>RedirectorSinks</code> using a different account that has local administrator permissions.
Exchange 2007 Servers	
Send As permissions for the Service Account on 2007 Exchange Servers	<p>Link to instructions</p> <pre>Get-Mailboxdatabase Add-ADPermission -User [service account] -ExtendedRight "send as"</pre> <p>[service account]=display name</p> <p>Plan at least two hours for permissions to propagate.</p>
Receive As permissions for the Service Account on 2007 Exchange Servers	<p>Link to Instructions</p> <pre>Get-Mailboxdatabase Add-ADPermission -User [service account] -ExtendedRight "receive as"</pre> <p>[service account]=display name</p> <p>Plan at least two hours for permissions to propagate.</p>

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 13](#)
 - ["Hardware Requirements" on page 17](#)

- ["Software Requirements" on page 18](#)
- 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 17](#).

Windows Authentication Requirements

The following are required to use Windows Authentication:

- Exchange 2000 or Exchange 2003. Windows Authentication does not work with Exchange 5.5 or Lotus Notes.
- At least two Authentication Managers must be installed, each in a different geographic region. More Authentication Managers provide redundancy and shorter login times.
- Any machine housing an Authentication Manager must be able to access a Domain Controller capable of authenticating a given user.
- Sites housing Authentication Managers must have dedicated internet connections to provide redundancy in case of a site failure.

When Support configures Windows Authentication in the data center, they set the parameters described in [Table 2-13](#). To change any of the default values, contact Support.

Table 2-13 Windows Authentication Configuration Parameters

Parameter	Description	Default
Cache Windows Password	The number of hours a password is stored to speed subsequent logins	48 hours
Max Password Attempts	The number of failed login attempts after which the user is locked out.	Typically set to one fewer than your organization's network lockout policy, so that a user cannot be locked out of the network because of failed Email Continuity login attempts.
Attempt Count Reset	The number of minutes the system stores a failed attempt and counts it against the number of Max Password Attempts.	30 minutes
Lockout Period	The number of hours an account remains locked	72 hours

Windows Authentication Limitations

The following are known limitations for Windows Authentication:

- Disabled Active Directory accounts cannot log in.
- Windows NT login IDs cannot be used; there is no way to ensure that an NT ID is globally unique. The SMTP address is a unique identifier.
- In multi-domain forests, sufficient trusts must be in place between accessible domain controllers between domains to authenticate users.
- By design, if an Active Directory account is locked, the user's logon will fail for Email Continuity even if they have not exceeded the Max Password Attempts count.
- If a user changes his Active Directory password after having logged in and cached his password in Email Continuity, the cached password remains the Email Continuity password until the Cached Windows Password time-out expires.

Wireless Continuity for BlackBerry Requirements



To use Wireless Continuity for BlackBerry, the following requirements must be met:

- Blackberry device software versions 4.1 or greater must be installed; earlier versions of device software are not supported.
- BES 4.1 and later.
- The MDS service is running on all BES servers.
- The SyncManager software has network access to the BES databases by Window NT authentication.
- If using MSDE, the service account needs read permissions for the directory where the `BESMgmt_data.mdf` and `Besmgmt_log.mdf` reside.
- The RedirectorController software must be able to post HTTP requests to the BES systems that have push capability.
- Each user's display name must match the name on the host where his BlackBerry device is cradled. If a user's name changes, the MAPI profile on the host must be changed as well.
- It is possible to have multiple instances of the MSDE/SQL installed on any one host. However, if your environment includes only one database instance on one host and provides for auto-detection, the installation process auto-detects the correct instance. If your environment does not provide for auto-detection, you must set this manually.

Wireless Continuity for BlackBerry Installation Prerequisites

These instructions are based on the following software versions:

- Email Continuity version 6.0.3 and higher
- BES version 4.1.3
- SQL version MSDE

There are several prerequisites you must have in place before accessing the BES database. The list below gives you a quick overview, and the rest of this section explains how to perform these tasks.

- 1 Add the Email Continuity service account to the Local Administrator Group (see ["Adding the Email Continuity Service Root Account to the Local Administrator Group" on page 30](#)).
- 2 Enable TCP and Names Pipes Access to the BES database (see ["Enabling TCP and Name Pipes to Access the BES Database" on page 30](#)).
 - Run SVRNETCN.exe
 - Stop and Restart SQL services
- 3 Verify that Mobile Data Services (MDS) is installed and configured for Wireless Continuity for BlackBerry (see ["Verifying that Mobile Data Services are Installed and Configured" on page 31](#)).
 - Configure MDS to act as a push server
 - Configure MDS to a valid port
 - Stop and Restart the MDS services
- 4 Verify IT Policy settings (see ["Verifying that Mobile Data Services are Installed and Configured" on page 31](#)).
 - Allow third-party application downloads
 - Allow internal connections
 - Allow external connections
- 5 Grant `db_datareader` and `public` access to the BES SQL database.

Adding the Email Continuity Service Root Account to the Local Administrator Group

You must add the service root account (or the valid super administrator account that is running Email Continuity services for your organization) as a local administrator of the BES group.

To add the Email Continuity account to the local administrator group of the BES group:

- 1 Log in using the BES administrator user name and password.
- 2 Right-click **My Computer** on the desktop, and select **Manage** from the drop-down list. The **Computer Management** window appears.
- 3 Open **System Tools**, then open **Local Users and Groups**. In the **Groups** folder, select and right-click **Administrators** in the list. Select **Add to Group**. The **Administrators Properties** pane appears.
- 4 Click **Add**. The **Select Users, Computers, or Groups** pane appears.
- 5 Type the name of your Email Continuity service root or valid super administrator account in the **Enter the object names to select** box. Click **Check Names**. The complete email address appears in the box.
- 6 Click **OK**. The **Administrators Properties** panel appears again, with the Email Continuity administrator user added to the list.

Enabling TCP and Name Pipes to Access the BES Database

NOTE Instructions for BES version 4 and version 5

The following instructions are written for BES version 4. For a BES 5 server, configure TCP using the Microsoft SQL configuration tools, such as **Start > All Programs > Microsoft SQL Server 2005 > Configuration Tools > SQL Server Configuration Manager**.

Set the TCP/IP protocol for BlackBerry to **Enabled**.

Do not enable IP Addresses IP1 or IP2.

Set the TCP Port for IPALL to 1433.

To enable TCP and Name Pipes to have access to the BES database:

- 1 Navigate to the `SVRNETCN.exe` file. This file is typically located in `C:\Program Files\Microsoft SQL Server\80\Tools\Binn.`
- 2 Run `SVRNETCN.exe`. The **SQL Server Network Utility** window appears.
- 3 Under the **General** tab, locate **Disabled protocols**.
- 4 Select **Named Pipes** and click **Enable** to move it to the **Enabled protocols** box. Do the same with TCP/IP.

- 5 Click **OK**. The SQL Server Network Utility displays a message informing you that changes are made when saved, but do not take effect until the SQL Server service is stopped and restarted.
- 6 Click **OK** to save your changes.
- 7 To stop the MSSQLServer, right-click its icon in the notification area. This pops up the MSSQL menu. Select **MSSQL Server Stop**. You are asked to confirm that you want to stop the MSSQLSERVER service on the selected server. Click **Yes** to stop the service.
- 8 Next, restart the service by right-clicking on the icon. Select **MSSQLServer Start**.

Verifying that Mobile Data Services are Installed and Configured

NOTE Instructions for BES version 4 and version 5

The following instructions are written for BES version 4. For a BES 5 server, MDS is a core component and is set to push by default. You can skip this section for a BES 5 server.

Verifying that MDS is installed and configured for Wireless Continuity for BlackBerry is a multi-step procedure. You must verify that the MDS server is a push server and is listening on an available port. You must then set the IT policies.

To verify that the MDS server is a push server and has an appropriate listening port configured:

- 1 From the **Start** button, select **BlackBerry Enterprise Server**, then **BlackBerry Manager**. The BlackBerry Manager splash screen appears.
- 2 After the BlackBerry Manager has started up, click the **Global** tab.
- 3 Expand **BlackBerry Domain** so that **Servers** is displayed. Expand **Servers** to display a list of servers. Select the server for which you want to verify settings.
- 4 When you select a server, settings for that server appear in the **Connection Service** panel.
- 5 MDS must be a push server. To set it as such, locate **Tasks** on the right side of the panel. Click **Set as Push Server**. The page refreshes and **Is push server:** is now set to `True`.
- 6 Click **Edit Properties** above **Tasks**.
- 7 The **BlackBerry MDS Connection Service** panel appears. Verify that the Web Service Listen Port is an available port (usually 8080).
- 8 Stop and restart the service using the buttons in the **Task** panel.

To set IT policies:

- 1 From the BlackBerry Manager main page, click the **Global** tab.
- 2 Click the ellipsis (...) in the right side of the IT Policies field. The **Global Properties** panel appears.
- 3 In the **Global Properties** panel, locate **IT Policies** and select it. The **IT Policy Administration** panel appears.
- 4 Double-click **IT Policies**. The **IT Policies** panel appears with one default policy. Select this policy. When you select the policy, new options appear. Select **Properties**. The list of properties associated with this policy appears.
- 5 Locate **Security Policy Group** and select it. The bullet beside **Locate Security Policy Group** becomes an arrow.
- 6 Locate **Disallow Third Party Application Download**. Use the drop-down list to set this to **False**.
- 7 Locate **Allow Internal Connections**. Use the drop-down list to set this to **True**.
- 8 Locate **Allow External Connections**. Use the drop-down list to set this to **True**.
- 9 When you have made these changes, click **Apply**, then click **OK**. The **IT Policy Administration** panel appears again. Click **OK** on this panel. The BlackBerry Manager main page appears.

Wireless Continuity for BlackBerry Supported Configurations

The service supports:

- All configurations of 4.1 BES and later supported by RIM.
- All devices later than 4.1, as long as they are supported by the installed BES. The device.xml file must have an updated list of all devices when using the over-the-air deployment method.

Wireless Continuity for BlackBerry Limitations

Limitations for Wireless Continuity for BlackBerry are described below.

- On some platforms and with some carriers, the unread device message counter does not increment correctly when Email Continuity is active. The counter increments twice for each received mail, but decrements only once when a message is read. This is a known RIM issue. To reset the counter, from the **Agent** menu, select **Reset Unread Msg Counter**. When asked **Allow device to restart?**, select **YES**.
- The BES-independent model that allows BlackBerry users to compose, send, and receive email on their BlackBerry devices even if the BES has failed works only for organizations using the version 6.5 (or later) data

center and the version 6.2 (or later) BlackBerry agent. Organizations using previous versions of the data center or agent software will notice no change to their Wireless Continuity for BlackBerry implementations.

- Messages received during an activation cannot be forwarded or replied to after the activation is complete (that is, when EMS has been returned to the READY state). Users should send the message, receive the error message, then resend the message. The initial message failure allows the device to obtain the message body from Exchange through the BES.
- While Email Continuity is active, users cannot send attachments with messages composed on their BlackBerry devices. They can attach files, but message recipients will only receive the body of the message.
- Forwarded messages and replies do not include original attachments, but do provide a text rendering of them up to the device limit (32Kb).

Outlook® Extension Requirements



The following are required to use the Outlook® Extension:

- Windows XP or Windows Vista
- Outlook® 2003 SP 2, or Outlook 2007 SP 1 (when available). Outlook must be in cached mode to use Email Continuity features.

NOTE Required Microsoft Hotfix for Email Continuity Features

The following hotfix is required in order for recurring appointments to perform correctly when using the Outlook Extension.

Outlook 2003: KB # 935411

If you do not install this hotfix, then users will experience problems when responding to recurring calendar requests. The reply to the sender does not indicate that the meeting was declined, and Outlook does not update the tracking status of the invitation.

NOTE Required Microsoft Hotfix for Email Archive Features

Outlook 2007: KB 941275

If you do not install this hotfix, the storage management icons will not perform correctly; the purple paper clip icon does not display.

Cached mode is not required to use Email Archive features, but is encouraged for better performance.

- Users must have administrative permissions to install the Extension.
- For the storage management feature of the Extension to work as described, the administrator must publish two forms to a Library in Exchange, and the end-user's account must have access to the forms on

Exchange. See "[Installing Custom Forms in Exchange 2000/2003 \(Storage Management Only\)](#)" on page 83, or "[Installing Custom Forms in Exchange 2007 \(Storage Management Only\)](#)" on page 85.

Outlook Extension Limitations

[Table 2-14](#) describes known limitations with the Outlook Extension. To compare Outlook Extension features with those of Email Continuity web-mail, see "[About the Outlook Extension](#)" on page 7.

Table 2-14 Outlook Extension Limitations

Limitation	Status
During an activation, read/delivery receipts do not function typically.	During an activation, read receipts are generated and sent when the user clicks the Send/Receive button. If the user does not click Send/Receive, the receipts are delivered after recovery.
During an activation, the New Mail icon does not display in the task bar.	Under investigation for future release
Because of the way Microsoft encodes new lines in the Description field, meetings created using the Extension sometimes display <i>n</i> characters in the text when they are restored by the RecoveryManager. For example, instead of "Meeting Request for Monday 4/23 - 11:00 -11:30", the invitation reads "\nMeeting Request for Monday 4/23 - 11:00 - 11:30\n".	Under investigation for future release
When creating meeting invitations, you can choose conference rooms as recipients (required or optional) but cannot assign them as resources until Outlook is back online.	Outlook cannot process resource requests while offline.
The data center validates email addresses when attempting to send a message. If the address is invalid per RFC-822 specifications, the data center fails to send the message, and it remains in the Outlook outbox during an activation. Exchange would attempt to send the message even if the address did not conform to RFC-822.	Expected difference in behavior between the Extension and Exchange, based on data center processes.
If a client-side rule is based on an Exchange address (such as, "move a message from a user on Exchange to a folder") the rule may not be processed consistently. Rules based on SMTP addresses and other conditions behave as expected.	Under investigation for future release
To address performance issues in earlier versions, Outlook Extension no longer supports context menu functionality in Outlook 2003. Features previously accessible through the context menu are available through the ESS drop-down menu on the toolbar.	Use the ESS drop-down menu on the toolbar for these features.

Planning RedirectorSink/RedirectorController Placement

RedirectorSinks are required to use the partial activation feature in Exchange 2000/2003 environments. Installed on Exchange servers, RedirectorSinks are SMTP event sinks that redirect messages in your Exchange environment for active Email Continuity users to the data center. RedirectorSinks receive this routing information from the RedirectorControllers.

NOTE Partial Activation in Exchange 2007 Environments

The partial activation feature is supported for Exchange 2007. Instead of using RedirectorSinks, the service uses a custom Transport Agent installed on the Hub Transport Server. For more information, see ["Installing the RedirectorAgent" on page 60](#).

RedirectorSink Placement

An Exchange server without RedirectorSinks and RedirectorControllers cannot redirect mail for active Email Continuity users. For this reason, Support recommends that you install a RedirectorSink on all Microsoft Exchange 2000/2003 servers in your environment.

This configuration allows for the greatest level of flexibility and coverage in the event of an outage. By deploying the RedirectorSinks to all Exchange servers in the environment, not only can the servers redirect messages at the first possible hop, but redirection is possible for partial server outages.

When planning for RedirectorSinks, consider the following:

- Bridgehead and SMTP gateway servers—Installation on bridgehead and SMTP gateway servers is critical for redirection. By installing RedirectorSinks on SMTP gateway servers, inbound SMTP mail for active users is redirected at the first hop, minimizing network traffic and providing maximum flexibility in the event of an outage.

Bridgehead servers act as concentrators for message traffic. Even if no mailboxes are on the bridgehead servers themselves, because messages in transit to an active recipient may pass through these, it is important that they include installed RedirectorSinks.

- Mailbox servers—Installation of a RedirectorSink on each mailbox server in your environment allows for redirection of mail between routing group peers, as well as redirection of intraserver message traffic. This protects against failure of a single server in a routing group, as well as in the event of a single database or storage group failure.
- Public folder servers—Typically, dedicated public folder servers do not have messages destined for mailbox recipients transiting them. So, while deploying a RedirectorSink on this type of server may not be essential, it is still considered a best practice.

RedirectorController Placement

Proper placement of RedirectorController instances (controllers) in your messaging environment is essential for high-availability failover. Much like the domain name service (DNS), the controllers provide routing information to the Exchange servers for active users. Without access to RedirectorControllers, the RedirectorSinks cannot redirect messages for active users. Similarly, without access to the data center, RedirectorControllers cannot obtain updated routing information for transmission to the RedirectorSinks.

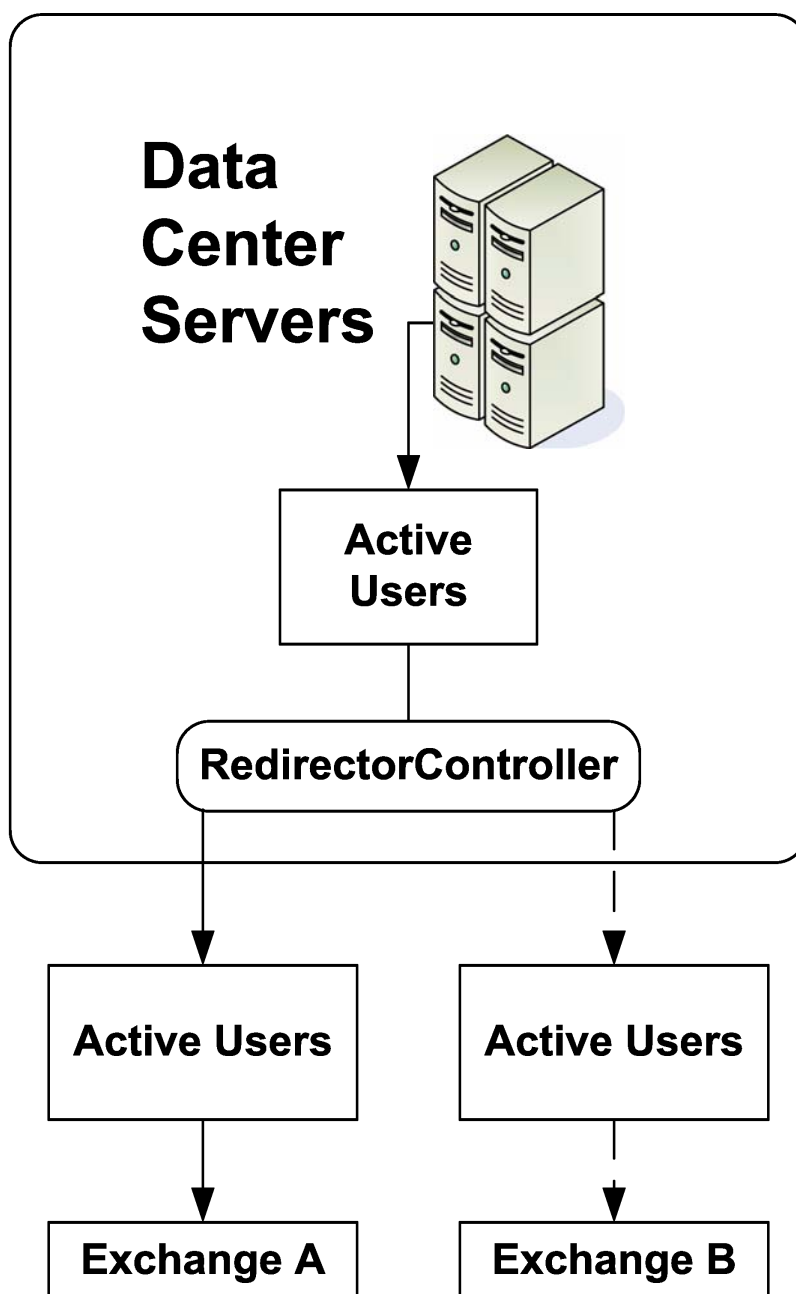


Figure 2-4 RedirectorController

As part of your installation, Support helps you install a single RedirectorController in your environment. You can install additional controllers by running setup and choosing the **secondary controller** option.

When planning for secondary controllers, consider the following:

Geographic diversity—If Exchange servers are available in multiple locations, placing controllers in multiple locations helps protect against catastrophic failure or power outage in a single location.

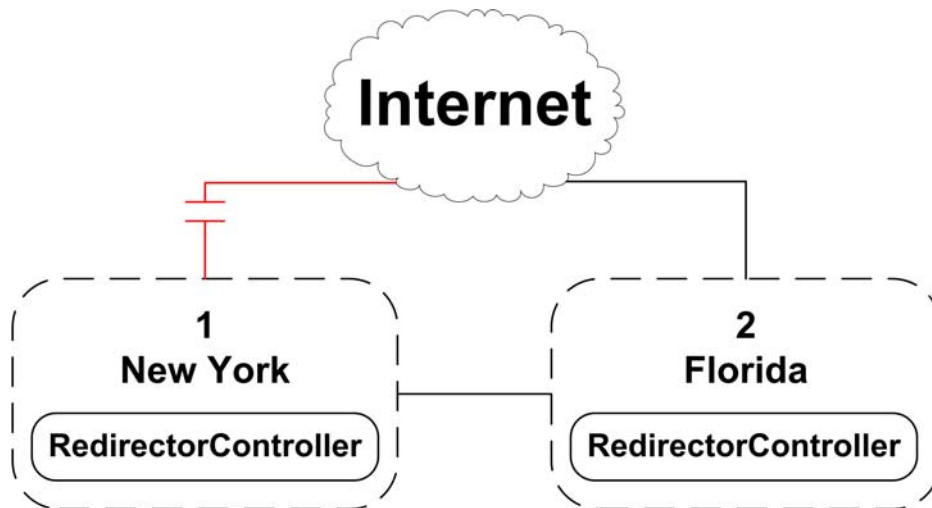


Figure 2-5 RedirectorControllers in Multiple Locations

WAN topology—Where loss of wide-area network (WAN) links, firewalls, or dial-on-demand links may isolate servers from available controllers, strategic placement of secondary controllers allows RedirectorSinks to obtain updated routing information.

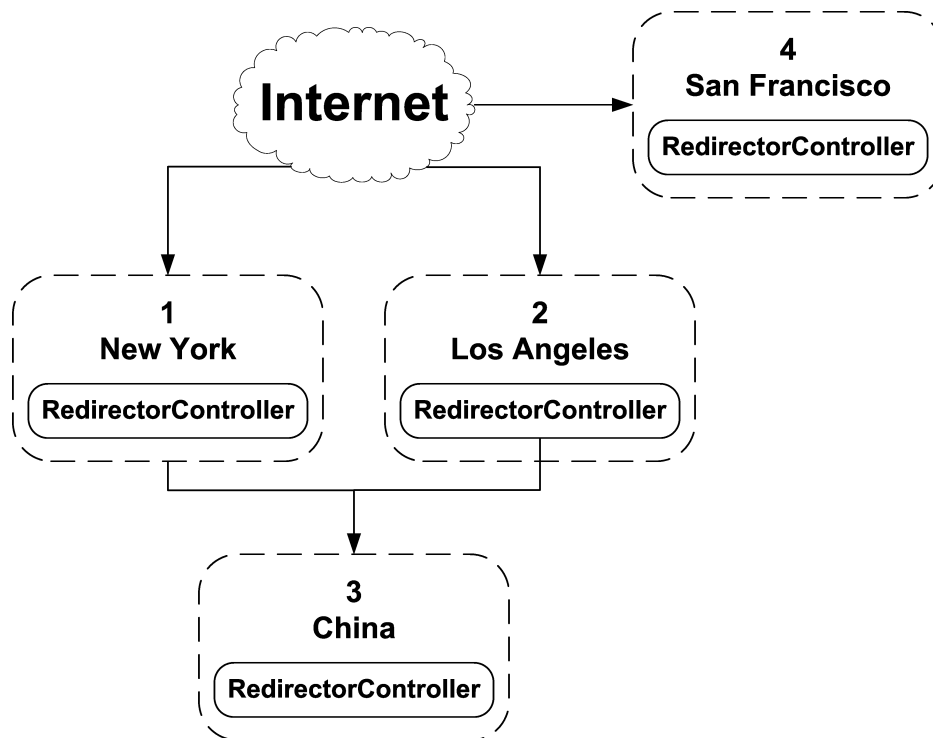


Figure 2-6 RedirectorControllers in WAN

Geographic redundancy—If your environment includes multiple servers located in a single data center, this magnifies the risks associated with a single controller failure. Consider placing multiple controllers in a single data center.

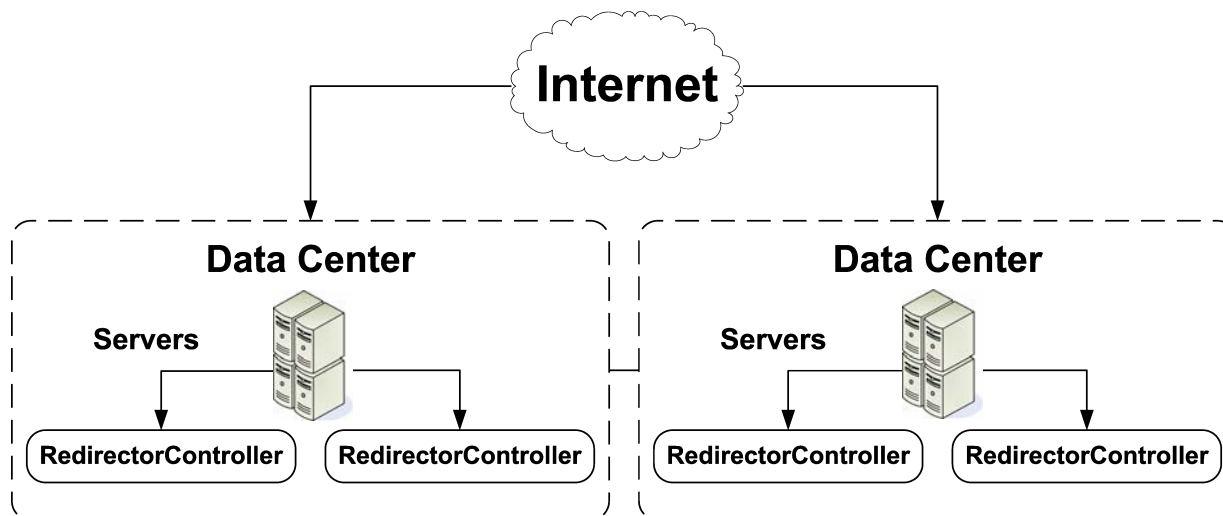


Figure 2-7 Redundant RedirectorControllers

In the event of an outage where normally functioning Exchange servers are unable to communicate with a controller (or the controller is unable to communicate with the data center), you may need to activate the service for users on these functioning servers in order to communicate with users affected by the outage. As a result, Support strongly encourages that you critically evaluate the placement of controllers and WAN/internet connectivity and, where appropriate, add additional controllers, network links, or both to provide the highest possible levels of redundancy.

Historical Mail Requirements

CAUTION Read Before Installing!

Before you begin Historical Mail implementation, be familiar with all requirements and work with your Support representative to identify your organization's preferred routing topology.



Before you can install software for any VaultBox implementations and enable the Historical Mail feature, you must do the following:

- 1 Allow port 22 (TCP) as outbound for SSH through the firewall from all VaultBox machines. See the network settings document provided by Support for specific address information.
- 2 Ensure that all Exchange servers that use SMTP can communicate with any identified VaultBox systems using port 25 (TCP).
- 3 In Exchange, increase the maximum recipients limit to a number at least as large as [the number of recipients on your largest mailing list * 2] + 1. For example, if your largest mailing list has 2000 users, increase the maximum recipients limit to at least 4001 ([2000 * 2] + 1).
- 4 Identify routing requirements for use with the Historical Mail feature and, in the DNS zones file, create additional zones (at least one per preferred routing topology, with a maximum of eight) named consecutively (for actual names of the DNS zones for your Historical Mail implementation, see the network settings document provided by Support).
- 5 Assign MX records for VaultBox systems. Contact Support for specific instructions on how to do this for your organization.
- 6 Gather the following information for each machine that will be used as a VaultBox system:
 - Its name
 - The drive on which you will install the software
 - The location of the cache directory where email messages arrive by SMTP before transmission to the data center

CAUTION Required Drive Space

Be sure you identify a drive with enough space for seven times the expected volume of daily mail. If you fail to install the Historical Mail software on a drive with enough space, the feature will not work properly.

AlertFind Integration Requirements

The following are required to support AlertFind Integration:

- One-to-one mailbox-to-user correspondence between products.
This feature is available only to customers whose Email Continuity and AlertFind products are exactly matched; that is, all of the mailboxes in Email Continuity are also users in AlertFind. This feature does not work for customers who have all of their users in Email Continuity and a subset of users in AlertFind, or the reverse. There must be a one-to-one correlation between users in AlertFind and Email Continuity.
- Active Directory data must be formatted correctly for the AlertFind import to function. For example:
 - Only one phone number per device field is allowed.
 - North American phone numbers must contain 10 digits, beginning with the area code. Do not include text.
 - International phone numbers must begin with the country code, then provide the area/city code and phone number. Do not use in-country long distance numbers. For example, a number in the UK must be formatted 44 20 7333 4444, instead of 44 (0) 20 7333 4444.
 - Email address entries must have a valid alias (must contain an @ symbol) and can contain only one address. Two addresses separated by a semi-colon, for example, is not acceptable.

AlertFind Integration Limitations

The following are known limitations of AlertFind integration with Email Security Services.

- Although you can synchronize custom data fields from Active Directory, and use them as AlertFind groups, PINs and Time Zone data are not mapped to AlertFind. Users can create their own PINS and set time zone data through the AlertFind user interface.
- Custom data fields collected from Active Directory and synced to AlertFind are not available for use in other features of Email Security Services.

- When users are disabled or deleted from Email Continuity they are also deleted from AlertFind. Any data provided by these end users is also removed.
- There is currently no mechanism to automatically use AlertFind to notify users of an activation of Email Continuity.

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, RedirectorController, RedirectorManager, and the Directory Configuration wizard. This *Primary Controller* default install package is applicable to Windows 2000/2003/2007.
- Windows Authentication, if enabled

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 Select Features window, choose the component you want to install.

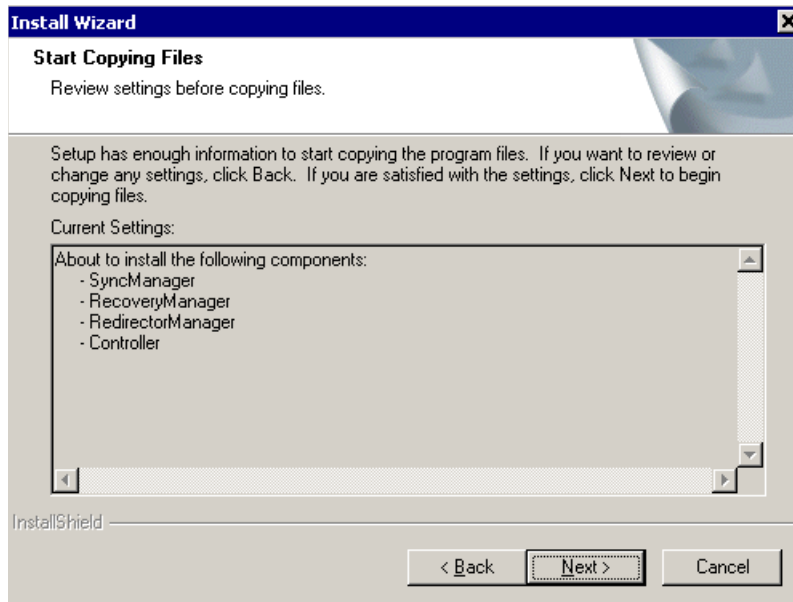
- a. For a typical installation, click **Primary Controller**. This installs the SyncManager, RecoveryManager, RedirectorController, and RedirectorManager.
- b. For installation of only a secondary RedirectorController, click **Secondary Controller**.
- c. To install only the RecoveryManager, click **Recovery Tools**.

- d. To customize your selection of components, click **Custom** (advanced users only). For custom installations, an additional window displays in which you identify which of the available components you want to install. Click **Next**.
- 7 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:

The screenshot shows a dialog box titled "Install Wizard" with a close button in the top right corner. The dialog box has a header section with a decorative background and the text "Service Credentials". Below the header, there is a text prompt: "Please enter the domain, username and password that the services will run as." There are three input fields: "Domain" (empty), "Username" (containing the text "administrator"), and "Password" (empty). At the bottom left of the dialog box, the text "InstallShield" is visible. At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

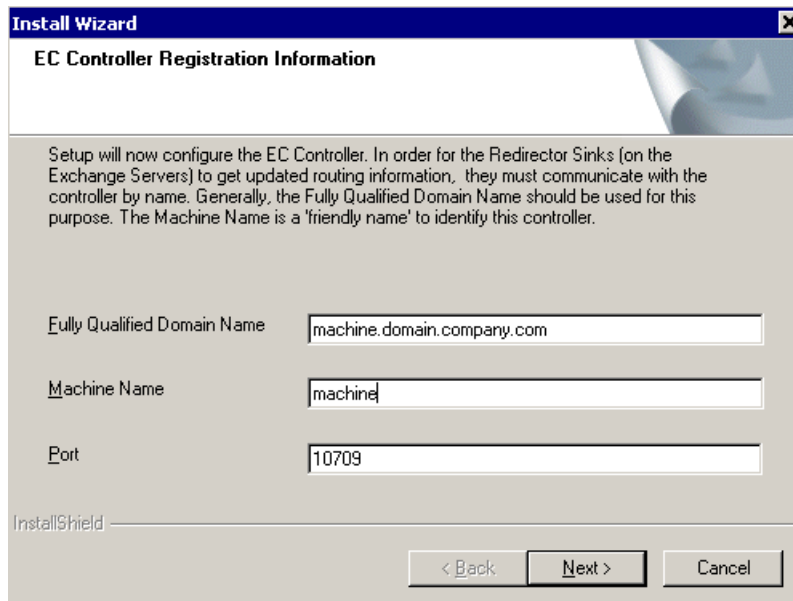
- a. Verify the information in the **Domain** box or, to log in under a different account, enter the appropriate domain information. MessageLabs strongly recommends that you do not use a different account.
 - b. Verify the information in the **Username** box or, if needed, change it to correspond with the information in the **Domain** box.
 - c. In the **Password** box, enter the password for the account.
 - d. Click **Next**.
- 8 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.

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



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

10 Provide RedirectorController registration information.



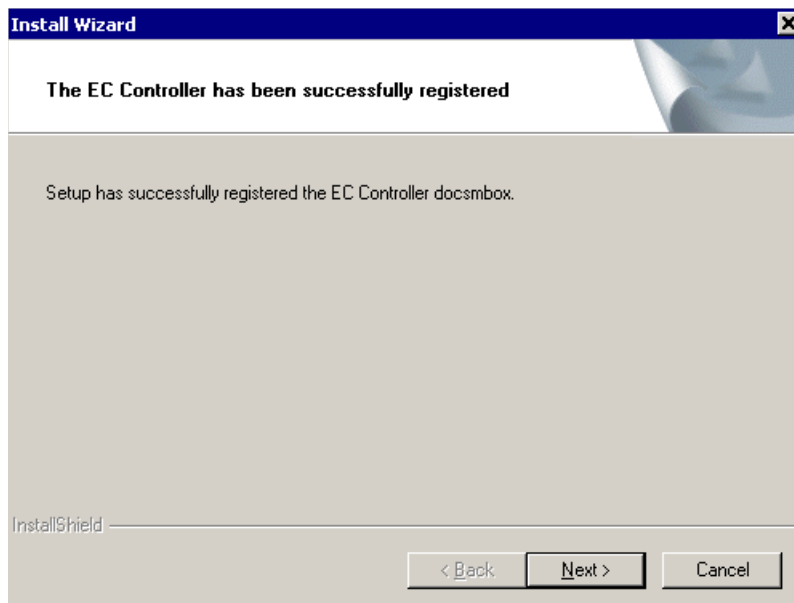
To configure the RedirectorController, the software must register the component so that it can communicate with the Exchange server or servers by name for transmission of RedirectorSink objects. To register the RedirectorController:

- a. Provide the Fully Qualified Domain Name for the RedirectorController.

NOTE Fully Qualified Domain Name

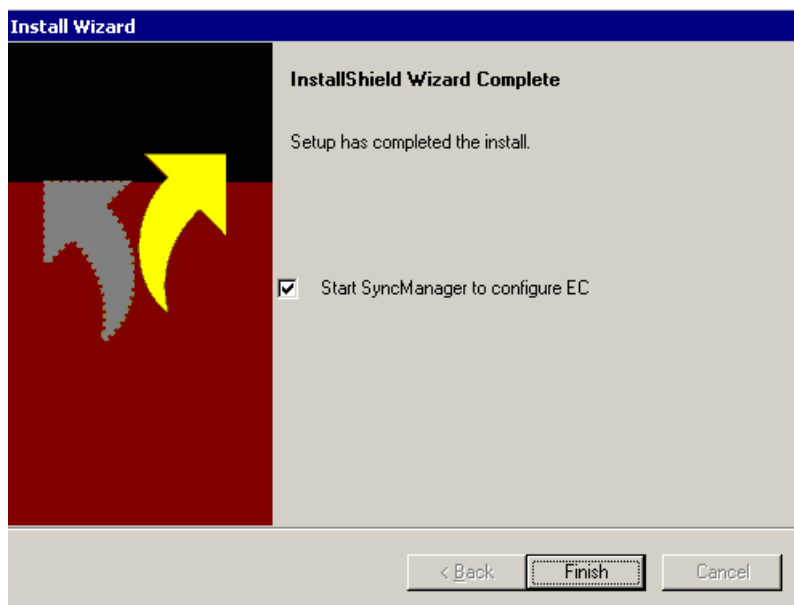
The Fully Qualified Domain name does not need to resolve externally.

- b. Provide the Machine Name of the machine on which you want the RedirectorController installed.
- c. Retain the default Port number (10709) or, if necessary, enter a new port number. If you enter a new port number, be sure you identify a port not used by any other application.
- d. Click **Next**. A window displays confirming registration of the RedirectorController.
- e. Click **Next**.



NOTE Terminal Services and Controller Registration

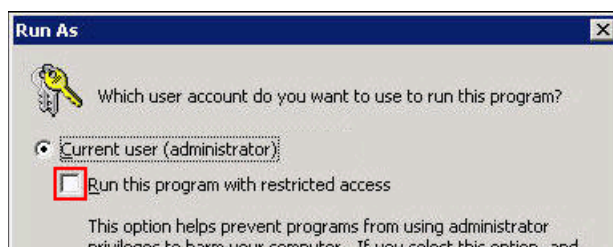
If you are installing using terminal services, after you click Next in the Controller Registration Information window, the process may appear to stall. If a processing icon (such as an hour-glass icon) continues to display for more than a minute or two, click once on the desktop and then click the window again. The process should continue without further delay.



- 11 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.



- 12 If the SyncManager has never been run before, a prompt appears requesting your approval to continue. Click **OK**.
- 13 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 50.

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 and Calendar data if it is stored on the email server. For calendar data, all activities scheduled for the future are synchronized (including future instances of recurring meetings), as well as any activities that occurred during the past seven days. If you need to have a longer period of historical calendar data synchronized, the number of days is configurable. Also, personal distribution lists can be synchronized, if the system has been enabled to do so. Contact Support for more information.

NOTE Personal Distribution Lists

If a Personal Distribution list is created or edited in Outlook, the contents can be synced to the data center if this feature has been enabled by Support. If a Personal Distribution List is created or edited using Outlook Web Access (OWA), the contents are not synced.

While performing a sync, the system also checks for ID conflicts based on a user's primary email address. If more than one instance of an email address is detected, a conflict is reported. (Note that the system does not use other criteria for detecting conflicts, such as aliases or X400 or X500 addresses.) The system provides means to resolve conflicts automatically or manually; see ["Resolving User ID Conflicts Automatically" on page 175](#) and ["Resolving User ID Conflicts Manually" on page 150](#).

Q Why is conflict detection necessary?

A Email Security Services uses the Exchange LegacyDN as a unique identifier when storing mail for a user. When the user changes Administrative Groups or Exchange Organizations, the LegacyDN value changes, the old mailbox is deleted, and a new one is created. To make sure that all mail collected for a user under the old LegacyDN is subsequently associated for the user under the new LegacyDN, SyncManager detects potential conflicts and allows administrators to resolve them by indicating that the two users are the same person.

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**.

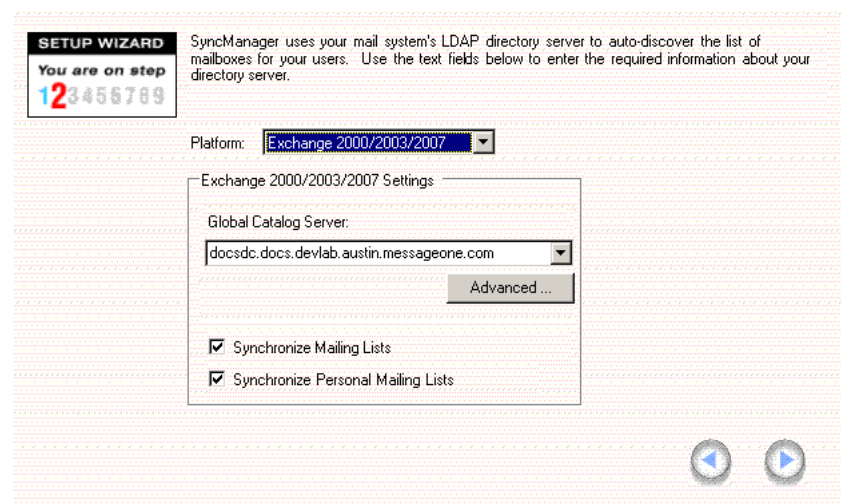
To configure the SyncManager:

- 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.



The screenshot shows the 'SETUP WIZARD' interface. A progress indicator shows 'You are on step 1' out of 9 steps. The main text reads: 'Welcome to the MessageLabs EC SyncManager Console. Since this is your first time using SyncManager, it is necessary to verify your identity. Please enter the user name and password that your Global Client Support Center representative gave you. When done, click Next.' Below this is a 'Login Information' section with two input fields: 'User Name' containing 'emsroot@domain.company.com' and an empty 'Password' field. Navigation arrows are visible at the bottom right.

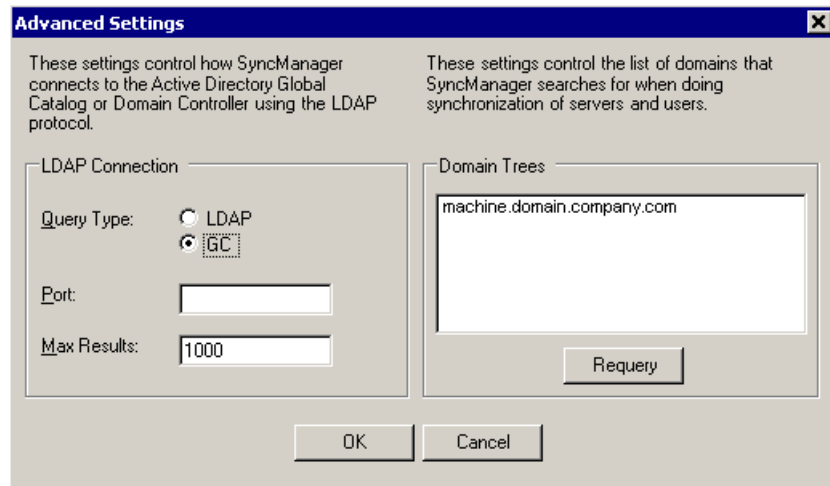
- 2 Identify your version of Microsoft Exchange software.



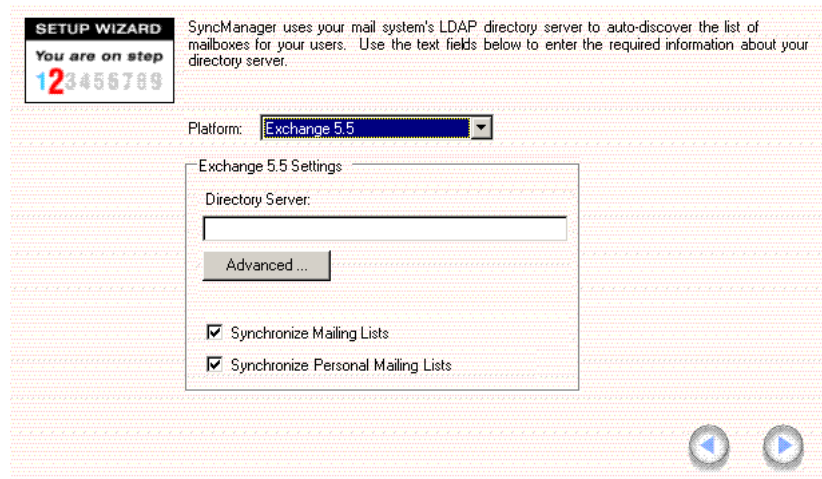
The screenshot shows the 'SETUP WIZARD' interface at step 2. The main text reads: 'SyncManager uses your mail system's LDAP directory server to auto-discover the list of mailboxes for your users. Use the text fields below to enter the required information about your directory server.' Below this is a 'Platform:' dropdown menu set to 'Exchange 2000/2003/2007'. Underneath is an 'Exchange 2000/2003/2007 Settings' section with a 'Global Catalog Server:' dropdown menu set to 'docsdc.docs.devlab.austin.messageone.com'. There is an 'Advanced ...' button. At the bottom, there are two checked checkboxes: 'Synchronize Mailing Lists' and 'Synchronize Personal Mailing Lists'. Navigation arrows are visible at the bottom right.

- a. Select the appropriate email **Platform** and complete the information in the **Settings** portion of the window.
 - If you use Exchange 2000/2003/2007, the wizard automatically detects the Active Directory global catalog or catalogs available for use. From the Server list, select the global catalog server that is physically closest to the machine on which you installed the SyncManager.

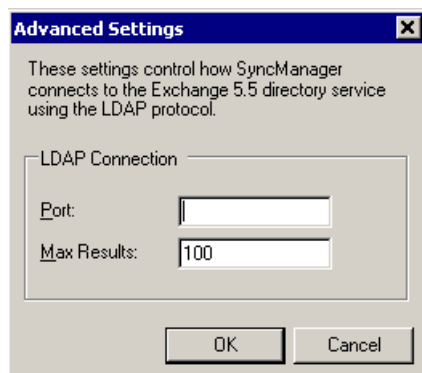
Click the **Advanced** button to see Advanced settings for the Global Catalog Server.



- If you use Exchange 5.5, type the name of the appropriate Exchange server in the **Directory Server** box.

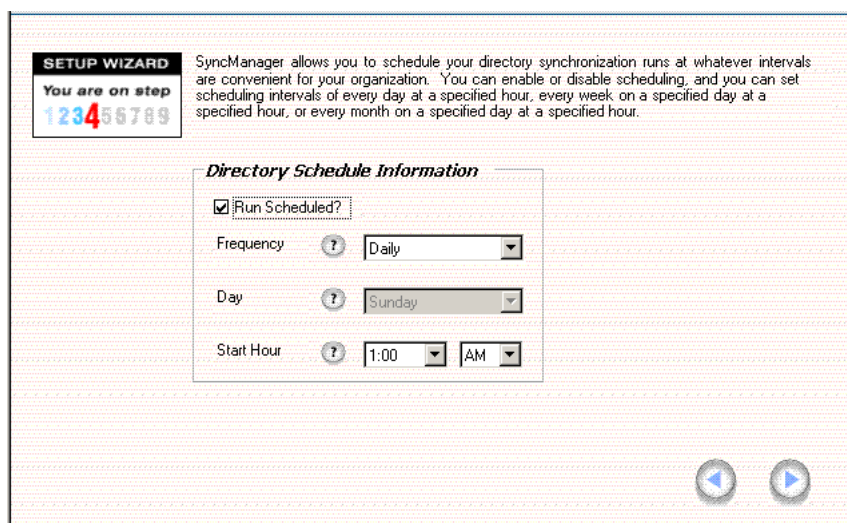


If this Exchange server is also a Windows 2000 domain controller server, click **Advanced** and, for the **LDAP Connection** information, provide information about the port on which Exchange listens for LDAP transmissions (389 is the default), and click **OK**.



- b. Leave the **Synchronize Mailing Lists** and **Synchronize Personal Mailing Lists** check boxes checked to allow these lists to be synchronized. Uncheck these boxes to turn off synchronization of these lists.
 - 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.



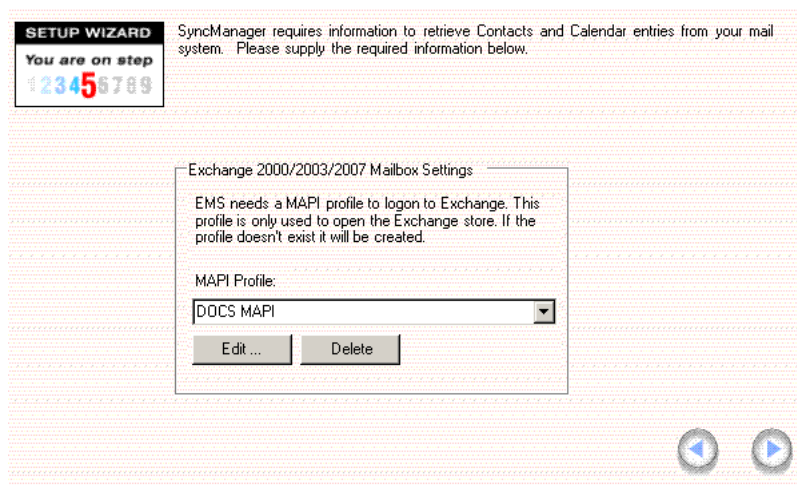
NOTE Actual Synchronization Start Time

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

TIP Imported Active Directory Attributes are Configurable

Email Continuity allows you to identify which user attributes are synched from Active Directory.

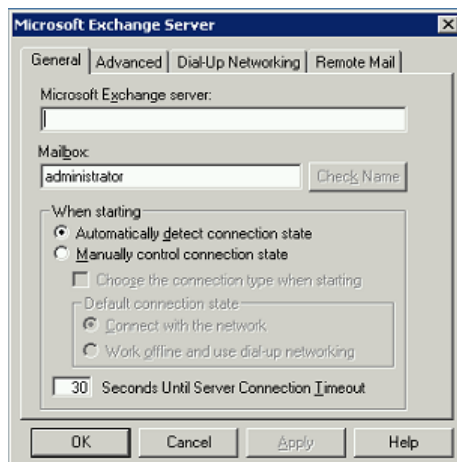
- a. MessageLabs recommends that you run directory syncs on a regularly scheduled basis. If you do not want your selections for the directory sync process to run regularly, clear the **Run Scheduled?** check box.
- b. Select a **Frequency**, including **Day** and **Start Hour**. Indicate whether the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

5 Set a MAPI profile for contact and calendar syncs.

For SyncManager to successfully synchronize data, you must select an appropriate messaging application programming interface (MAPI) profile. The product automatically detects available MAPI profiles. Either:

- Select a **MAPI Profile** from the drop-down list, or

- If an appropriate MAPI profile doesn't exist, the wizard helps you create one. Click **Edit**.

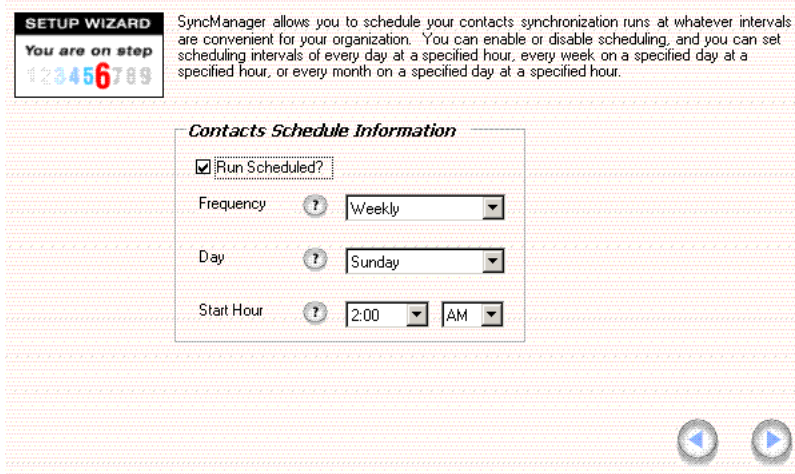


- (1) A MAPI Profile dialog box displays. To create a profile, click **Yes**. If you click **No**, you can provide the appropriate profile name and then click **Yes**.
- (2) A Microsoft Exchange Server dialog box displays. The contents of this dialog reflect the settings for the new MAPI profile. When the process completes, click **OK**.
- (3) Click the **Next** arrow.

NOTE Specific Mailbox Required

The Microsoft Exchange Server dialog box must reflect a specified mailbox that the configuration process can successfully resolve. To ensure this, click **Check Name** in the dialog. If the check fails, you may need to provide a fully qualified domain name for the mail server.

- 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.

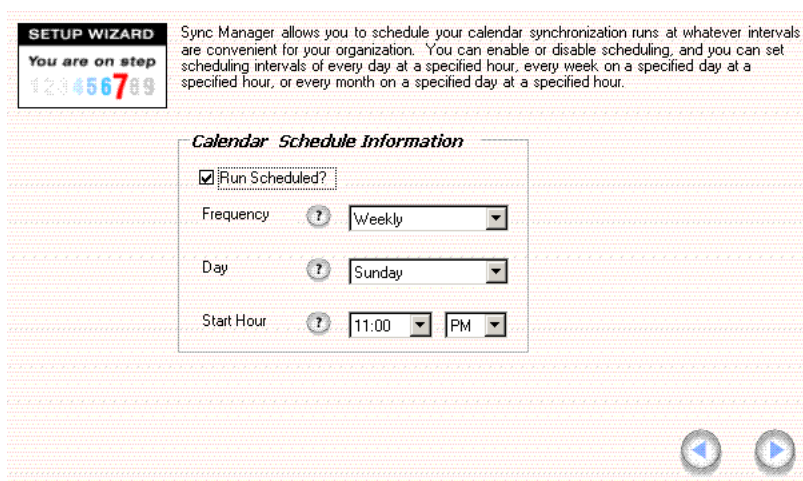


- a. Select a **Frequency**, including **Day** and **Start Hour**. Indicate whether the start hour is AM or PM. (Remember, noon is 12:00 PM and midnight is 12:00 AM.)
- b. Click **Next**.

NOTE Avoid Sync Process Overlap

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

- 7 In the **Calendar Schedule Information** dialog box, schedule the synchronization of users' calendar data. Because this process is more intensive than the directory synchronization process, schedule it for non-peak-load times and, preferably, weekly frequency.



- a. Select a **Frequency**, including **Day** and **Start Hour**. Ensure that you indicate whether the start hour is AM or PM.
 - b. 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 149](#).

Click the **Next** arrow.

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

The screenshot displays the SyncManager summary screen with the following sections:

- Directory Sync:** Last Run Status: **Running**. Last manual run on 11/6/2006 9:56:41 AM. Next run at 11/7/2006 5:37:17 AM. Scheduled daily between 5 AM and 6 AM. Buttons: Sync Now, Sync Test, Edit Schedule ..., Configure ...
- Mailbox Data Sync:**
 - Contacts:** Last Run Status: **Not run**. No run on record. Next run at 11/12/2006 1:11:53 AM. Scheduled Sundays between 1 AM and 2 AM. Buttons: Sync Now, Edit Schedule ...
 - Calendar:** Last Run Status: **Not run**. No run on record. Next run at 11/12/2006 12:39:02 AM. Scheduled Sundays between midnight and 1 AM. Buttons: Sync Now, Edit Schedule ...

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 176 for more information.

If you are using several Exchange servers and Email Continuity controllers, you can configure SyncManager to specify which Exchange servers are synced 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.

Configuring RedirectorManager

The RedirectorManager is a centralized console interface through which administrators install, upgrade, and maintain RedirectorSink objects. In the event of a partial disruption of the primary mail system, the RedirectorSinks route email messages destined for affected users to their Email Continuity mailboxes. The

RedirectorSinks receive configuration and routing updates from RedirectorControllers and perform the required routing changes within minutes. After configuring the RedirectorManager, the partial activation feature is available in the event of a disruption to your primary mail system that affects a single server or a single location.

Installing RedirectorManager on a Standalone Server

Before you can configure the RedirectorManager, you must have administrative privileges on the server that runs the RedirectorManager software, as well as administrative privileges on the Exchange servers.

To install RedirectorManager:

- 1 Log in to the RedirectorManager software (**Start > Programs > MessageLabs > RedirectorManager**). This verifies the email platform and gathers information from each Exchange server. The account you use depends on the synchronization status.
 - a. If data has been synced, you can log in as an administrator.
 - b. If an initial sync has not yet been performed, you must login using the service root account or a valid super administrator account.
- 2 Select servers for RedirectorSink installation.

Along the top of the main RedirectorManager page are buttons for various functions, as well as a list of your environment's Exchange routing group. These are organized by name, with server name listings below. To perform a remote install of RedirectorSinks:

- a. Click **Install**.
 - b. Click **Next**. The installation process begins
 - c. On the **Select Servers for RedirectorSinks** page, select the appropriate routing group or groups, server or servers (left pane).
 - d. Click **Add**. Your selections move to the right pane.
 - e. Verify that your selections are correct. Click **Next**.
- 3 Restart Exchange services and deploy RedirectorSinks.
 - a. Select **Restart Services**.
 - b. Click **Next**.

NOTE **Installing Without Stopping Services**

You can install RedirectorSinks without stopping and restarting Exchange services; however, if you do this, all deployed RedirectorSinks remain inactive.

- 4 Confirm actions.
 - a. Confirm that the action or actions are correct. If so, click **Next**.

This begins the process of copying files, registering the RedirectorSinks with the Exchange environment, setting up registry entries, providing the RedirectorSinks with information about the RedirectorControllers, and stopping and restarting the IIS SMTP service.

NOTE Save the Log

To save the log, click **Save**. The RedirectorManager software queries the Exchange servers and retrieves information regarding their configuration. A RedirectorSink does not initialize after the IIS SMTP restart until it processes the first piece of mail. Therefore, it may take several minutes for the main page to reflect the running version and correct installation status of the event sink.

-
- b. Click **Done**.

TIP Force Load of RedirectorSinks

If the RedirectorManager or Administration Console do not show the RedirectorSinks as installed on a server, send an email message to any user on that server. This causes Exchange to load the RedirectorSink. While not typically an issue on production servers under load, this can occur in test environments.

Upgrading RedirectorManager

The installation process can be used to install an upgrade; however, you must stop and start IIS before the upgrade takes effect. The upgrade installs any new files, but does not change any existing registry entries.

Each time you add a new Exchange server to your environment, or when you reinstall an existing Exchange server, you must repeat the RedirectorSink installation process to install the RedirectorSink on the new or reinstalled server. When reinstallation is necessary, the Administration Console displays an alert message.

Installing RedirectorSink on Clustered Exchange Servers

To install RedirectorSink on clustered Exchange servers:

- 1 Copy the RedirectorSink folder over to the passive node of the Exchange Server.
- 2 Launch `setup.exe`, follow the prompts, and allow the install to complete.
- 3 Restart the SMTP service on the passive node.

- 4 Fail over the active node to the passive node.
- 5 Allow a piece of mail to pass through the server and wait about 90 seconds for the event sync to initialize.
- 6 Verify the RedirectorSink is connected by logging into the web-based Administration console and in the Readiness check section, under Redirector Sinks, click the **Details** link.
- 7 Repeat these steps for each additional node in the cluster.

NOTE RedirectorSinks and SMTP Virtual Servers

The RedirectorSink is designed to bind to only a single SMTP virtual server instance. On a standalone Exchange server, multiple SMTP virtual server instances must be consolidated into a single virtual server instance before installing the RedirectorSink. Multiple SMTP virtual server instances are only supported on Active/Passive or N+1 clusters where the number of virtual servers corresponds to the Exchange nodes present in the cluster. Additional Exchange nodes installed after the RedirectorSink require that you manually register the event sink. Contact Support for assistance.

Installing the RedirectorAgent

To use the partial activation feature of Email Continuity in Exchange 2007 environments, you must install a custom transport agent (the RedirectorAgent) on all Hub Transport servers. The RedirectorAgent is not supported on Edge servers. This agent performs functions similar to the RedirectorSinks used in Exchange 2000/2003 environments. The agent is provided by Support in a ZIP file (RedirectorAgent.zip) in the service software directory. Unzip the file on the Hub Transport server (to C:\RedirectorAgent) and install the agent using Exchange Management Shell. To run the script, you must provide the NetBIOS name and Fully Qualified Domain name of the machine running the RedirectorController.

CAUTION Exchange Transport Service Restart Required

As part of the installation process, the Microsoft Exchange Transport service stops and restarts automatically. Make sure that you install the agent at a time when a stop in this service is not disruptive to your organization.

CAUTION Installation Required on all Hub Transport Servers

To ensure reliable mail delivery during an activation of Email Continuity, the agent must be installed on all Hub Transport servers. Remember to install the agent each time you configure a new Hub Transport server, or modify a server to perform the Hub Transport role.

To install the RedirectorAgent:

- 1 Extract the RedirectorAgent.zip files to C:\RedirectorAgent on the Hub Transport Server.
- 2 Launch Exchange Management Shell.
- 3 Change directory to the one where the script is installed.
- 4 Type:

```
.\ManageRedirector.ps1 install "NetBIOS_name,FQDN"
```

where `NetBIOS_name` and `FQDN` are the Netbios and FQDN of the server running the Email Security Services software. Do not enter the values for your Exchange server.

For example, if the name of the server in your environment running ESS is `Server1`, and your DNS suffix is `company.local`, then this value would be `"server1,server1.company.local"`. The quotes are **required**.

NOTE Providing the ESS Server Name

You can either enter the fully qualified name as a parameter, as shown above, or wait for the install script to prompt you for it. If you enter it initially, you must use quotes around the name. If you wait for the prompt, the quotes are not required.

-
- 5 Exit the Exchange Management Shell to complete the installation.

NOTE Set RedirectorAgent to Lowest Priority

If you are running other transport agents (such as anti-spam or anti-virus agents) on your Exchange servers, you must set the RedirectorAgent to the lowest priority, otherwise you may impede mail flow.

To remove the RedirectorAgent:

- 1 Launch Exchange Management Shell.
- 2 Change directory to the one where the script is installed.
- 3 Type:

```
.\ManageRedirector.ps1 uninstall
```
- 4 Exit Exchange Management Shell. The agent is removed from the server. The log file is retained for analysis purposes.

Provisioning Wireless Continuity for BlackBerry



When Wireless Continuity for BlackBerry is provisioned in the data center, Support sets the following configuration parameters:

- **Device checkin interval**—The amount of time (in minutes) between each attempt a device makes to contact Email Continuity for messages. Contact attempts occur only when the user's Email Continuity account is active. The default setting is 5 minutes; however, the actual interval varies by device according to variables such as battery life and recent activity.
- **Store mail setting**—The number of days Email Continuity retains BlackBerry email it receives but is unable to deliver (for example, when a user's device is turned off or is out of range) after an activation is complete. The default is 10 days.
- **Push timeout interval**—The time (in minutes) that Email Continuity waits before reattempting contact with a device after a previous contact attempt failed. Email Continuity executes as many reattempts as possible until the next device checkin interval. The default is four minutes. This setting applies only to device agent version 6.1 and earlier.

Synchronizing RIM Data

You must have installed the SyncManager and RedirectorController to implement Wireless Continuity for BlackBerry. After you have installed this software, you must synchronize data from your environment to the datacenter.

To synchronize RIM data:

- 1 Launch the SyncManager for Email Continuity. On the Windows desktop, select **Start > Programs > MessageLabs > SyncManager**. The **SyncManager** screen appears.
- 2 In the **BlackBerry Sync** panel, click **Configure**. The **BlackBerry Config** window appears.

NOTE If the BlackBerry Sync Panel Does Not Appear

If Support enabled the Wireless Continuity for BlackBerry feature and the SyncManager interface does not include a BlackBerry Sync panel, exit the SyncManager and relaunch it. If this panel is still not available, contact Support.

- 3 In the **Server Name** field, type the fully qualified server name. (Using the NetBIOS name or IP address is not supported.)
- 4 In most cases, the software auto-detects and fills needed information in the Database Instance Name, and Database Name columns. If it does not, type `Default` in the **Instance Name** field, click the **Database** field and enter the name of the database (for example, `BESMgmt`).

NOTE SQL Security May Prevent Autodetection

If the SyncManager does not detect a database instance automatically, it's likely that the security settings for SQL are preventing the autodetection feature. In this case, type the name of the instance and database instead of selecting them.

- 5 Click **Add**.
 - 6 Repeat the preceding steps for each BES database.
 - 7 After you add all necessary information, click **Verify Configuration**. The software returns information on each entry in the BlackBerry Config window.
 - 8 Based on this information, add items to or remove items from the **Sync Settings** table.
-

NOTE Modifying BlackBerry Configuration Information

You cannot modify entries in the BlackBerry Config window. Instead, you must Remove any incorrect entry and then Add the correct information.

- 9 Click **Save** and close the **BlackBerry Config** window.
- 10 In the **RIM Data Sync** panel of the SyncManager interface, click **Sync Now**. When the RIM data sync completes successfully, you can send users the instructions for Wireless Continuity for BlackBerry feature, and view information about devices using the Wireless Continuity for BlackBerry feature. For information on each of these, see ["Wireless Continuity for BlackBerry Administration" on page 154](#).

Distributing the Client Agent

There are two methods for distributing the client agent. It can be deployed through the policy management features of BES 4.0+ (deployment over-the-air) or can be manually downloaded to the device through a hyperlink sent to the user through the Administration Console.

NOTE Complete All Preliminaries Before Proceeding

Be sure that you have completed all installation preliminaries listed under ["Verifying that Mobile Data Services are Installed and Configured" on page 31](#), especially the steps for setting IT policies. If you have not completed these steps before you distribute the client agent, your deployment will fail.

You can push the Wireless Continuity for BlackBerry client agent software over the air to BlackBerry devices that have never had the agent installed before (new installations, not upgrades). After distribution is performed as described below, the client software is pushed to the device at the next application push default interval. The default interval is four hours.

Distribution Over-the-Air for BES 4.x

The procedures provided in this section are for BlackBerry Enterprise Server version 4.1.3. BlackBerry devices must be version 4.1 or later.

To perform an over-the-air deployment, you must complete the following tasks:

- Download the agent and prepare the shared application directory.
- Index the agent.
- Prepare the software configuration (including creating application policies).
- Assign software applications to users.

To download the client agent:

- 1 Contact Support to obtain the URL from which you can download the agent.
- 2 When prompted to Save or Open the file, select **Save to your desktop**. When you unzip the file, you have three files: EMSBlackBerryClient.alx, EMSBlackBerryClient.cod, and EMSBlackBerryClient.jad.
- 3 Copy these three files.
- 4 Navigate to C:\Program Files\Common Files\Research in Motion. Add a new folder to the Research in Motion folder. Name this folder Shared.
- 5 Create a new folder inside Shared and name it Applications.
- 6 Create a new folder inside Applications and name it MessageLabs.
- 7 Paste the three files you copied earlier into the MessageLabs folder.
- 8 Navigate up the folder tree to the Common Files folder. Right-click the Research in Motion folder. Select **Sharing and Security** from the drop-down list. The **Research in Motion Properties** panel appears.
- 9 On the **Research in Motion Properties** panel click the **Sharing** tab. Then:
 - Select **Share this folder**.
 - Name the Share **Research in Motion**.
 - Set the **User Limit** to **Maximum allowed**.
- 10 Click **Permissions**. The **Permissions for Research in Motion** panel appears. Set permissions for everyone to allow **Read-only**. It is not necessary to check the other boxes. Click **OK** until the **Research in Motion** panel closes.

11 Open a DOS prompt and navigate to this location:

```
C:\Program Files\Common Files\Research in  
Motion\AppLoader
```

Run the following command:

```
loader /reindex
```

This creates two new files in the MessageOne folder you created earlier.

To configure the agent:

- 1** From the BlackBerry agent main page, select the **Software Configurations** tab.
- 2** In the **Tasks** section of the page, click **Add New Configuration**. The **Device Software Configuration** panel appears.
- 3** In the **Configuration Name** field, type `Email Continuity Agent`.
- 4** In the **Configuration Description** field, type `MessageLabs Email Continuity Agent`.
- 5** For the **Device Software Location** field, click **Change**. The **Device Software Share Location** pane appears. Either type the path to the software share location or browse to it, then click **OK**.
- 6** On the **Device Software Configuration** panel, you now have an entry for `Application Software`. Expand this entry. You should see a check box and **Email Continuity Agent**, with a version and delivery method.
- 7** Click the check box beside **Email Continuity Agent**. The **Delivery** field now contains a drop-down list. Select `wireless`.
- 8** Next, click **Policies**. The **Application Control Policies** panel appears.
- 9** Click **New**. The **Application Control Policy** panel appears. You will create two policies: **Global Push** and **Global Remove**.
- 10** To create the **Global Push** policy, complete the following settings:
 - In the **Name** field, type `Global Push`.
 - In the **External Domains** field, type `*.messageone.com`. Click **OK**.
 - Verify that the **Disposition** field is set to `Required`.
 - Verify that **Internal Network Connections** is set to `Allowed`.
 - Verify that **External Network Connections** is set to `Allowed`.
 - Click **Apply**.
- 11** To create the **Global Remove** policy, complete the following settings:
 - In the **Name** field, type `Global Removal`.
 - In the **External Domains** field, type `*.messageone.com`. Click **OK**.
 - Set the **Disposition** field to `Disallowed`.

- Click **Apply**.
- 12 Click **OK**. This returns you to the **Application Control Policies** panel. You should see **Global Push** and **Global Remove** in this list. Click **OK**. You return to the **Device Software Configuration** panel.
 - 13 Verify that Email Continuity Agent is present, that the version number is correct, that delivery is set to **Wireless**, and that policy is set to **Global Push**. If everything is in order, click **OK**.

The **BlackBerry Manager-Security Administrator Authority** page appears. When you click the **Software Configurations** tab, you should see **Email Continuity Agent** with a description and a source path.

To assign software applications to users:

- 1 From the BlackBerry agent main page, select the **All Users** tab. A list of users appears.
- 2 Right-click the name of the user or group of users with which you want to work. From the drop-down list that appears, select **Deploy Application**.
- 3 Click **Edit Properties**. The **Select a software configuration** panel appears.
- 4 Select **Email Continuity Agent** and click **OK**. You are returned to the **BlackBerry Manager-Security Administrator Authority** page, and the user's information is updated. Scroll to the bottom of the user information panel to confirm that the configuration status is ok, the system status is up-to-date, and the application status is up-to-date.

Alternatively, the application poll interval runs at the next BES check-in window. This can take up to four hours, depending on your configuration.

You can also remove the agent from users' handheld devices using the over-the-air method.

To remove the Blackberry agent for all users:

- 1 From the Blackberry Manager main page, select the **Software Configuration** tab.
- 2 Select the **Email Continuity Agent**. The **Device Software Configuration** panel appears.
- 3 In the **Policy** column, use the drop-down list to select **Global Remove**.
- 4 Click **OK**.
- 5 The application poll interval runs at the next BES check-in window. This can be up to four hours, depending on your configuration.

To remove the BlackBerry agent for one user:

- 1 From the BlackBerry Manager main page, select the **All Users** tab.
- 2 Right-click the name of the user for whom you want to disable the BlackBerry agent. Select **Assign Software Configuration**. Change this to None.
- 3 The application poll interval runs at the next BES check-in window. This can be up to four hours, depending on your configuration.

After the application has been removed, the BlackBerry requests that you reset it. After reset is complete, you must delete the application from the BlackBerry.

Distribution Over-the-Air for BES 5.x

The procedures provided in this section are for BlackBerry Administration Service version 5.0. BlackBerry devices must be version 4.1 or later.

To perform an over-the-air deployment for BES 5.x, you must complete the following tasks:

- 1 Prepare the shared application directory. See ["To prepare the shared application directory:" on page 67](#).
- 2 Update your IT policies. See ["To update your IT policies:" on page 69](#).
- 3 Download the client agent. See ["To download the client agent:" on page 69](#).
- 4 Add the client application to the BlackBerry Administration Service. See ["To add the client application to BAS:" on page 69](#).
- 5 Create and populate application policies. See ["To create and populate application policies:" on page 70](#).
- 6 Create and populate the software configuration. See ["To create and populate the software configuration:" on page 70](#).
- 7 Create a user group to hold all users who will receive the BlackBerry client. See ["To create a BlackBerry client user group:" on page 71](#).
- 8 Assign the software configuration to the BlackBerry client user group. See ["To assign the software configuration to the BlackBerry client user group:" on page 71](#).

To prepare the shared application directory:

- 1 On your BES server or network, create a folder to hold the shared application files, for example, C:\rimshare\Shared\Applications.

Important! Do not use the older BES path (C:\Program Files\Common Files\Research In Motion\).

- 2 Set sharing and permissions for the folder you created.
 - a. Right-click the folder you just created and select **Properties**.
 - b. In the **Properties** dialog box, click the **Sharing** tab and check (enable) `Share this folder`.
 - c. Click the **Permissions** button.
 - d. Click the **Add** button and enter the information for the BES Admin service account.
 - e. Grant the BES Admin service account `Full control` over this directory.

NOTE Restrict Modifications to the Shared Application Directory

This shared application directory should be used only by the BlackBerry Administration Service for BES 5. Do not manually place files into this directory or modify any files you find there.

- 3 Log into the BlackBerry Administration Service for BES 5.
- 4 From the BAS navigation menu, under **Servers and components**, choose **BlackBerry Solution topology**. Navigate to the BlackBerry domain in use for the BlackBerry client and choose **Component View**. The **Components** page appears.
- 5 On the **Components** page, click the **BlackBerry Administration Service** link listed under the **Component** column.

BlackBerry Administration Service		
You can use the BlackBerry® Administration Service to manage the entire BlackBerry® Enterprise Solution.		
Name	Component	Installation server
BAS	BlackBerry Administration Service	LAB201BES

The **Components** page for the BAS appears. The breadcrumbs at the top of the page should be in the form: BlackBerry Solution topology > BlackBerry Domain > Component view > View (BlackBerry Administration Service).

- 6 Scroll to the bottom of the **Components** page and click the **Edit component** link. The **Components** page becomes editable, and the breadcrumbs at the top of the page should appear in this form: BlackBerry Solution topology > BlackBerry Domain > Component view > Edit (BlackBerry Administration Service).
- 7 On the **Component Information** tab of the **Components** page, in the **Software management** section, enter the UNC of the shared application directory you created into the **BlackBerry Administration Service application shared network drive** field. For example, if you created the directory `C:\rimshare\Shared\Applications\`, then you would enter `\\machinename\rimshare\Shared\Applications`.

- 8 Scroll to the bottom of the page and click the **Save All** link.

To update your IT policies:

Perform the following updates to all of your existing BES IT policies so that users are not prompted to either configure or confirm their local device firewall settings. If you do not set the following, users will be prompted to configure their own devices.

Note: It is strongly recommended that you notify your users **in advance** that their IT policies will be changing. When you make the changes below, the BES server will send a one-time pop-up notice to all associated BlackBerry devices alerting them that the IT policy has been updated and requiring them to reboot their devices. Inform your users in advance to expect this policy notification and reboot.

- 1 Within the BAS Admin console, click **BlackBerry Solution management > Policy > Manage IT policies > Manage IT policies**.
- 2 One at a time, perform the following steps for each policy currently in use:
 - a. Click **Edit policy**.
 - b. Click the **Security** tab.
 - c. Set **Disallow Third Party Application Downloads** to **No**.
 - d. Set **Allow Internal Connections** to **Yes**.
 - e. Set **Allow External Connections** to **Yes**.
- 3 Repeat these steps for all policies in use.

To download the client agent:

- 1 Contact Support to obtain the URL from which you can download the ZIP file containing the BES 5 client agent files.
- 2 Download and save the ZIP file to a location on your local machine or network.

To add the client application to BAS:

- 1 Log into the BlackBerry Administration Service for BES 5.
- 2 From the BAS navigation menu, under the **BlackBerry solution management** section, click **Software > Applications > Add or update applications**. The **Add or update applications** page appears.
- 3 Browse to the location on your local machine or network drive where you saved the ZIP file containing the client agent files. Click **Next**.
- 4 Choose **Publish application**.

To create and populate application policies:

- 1 From the BAS navigation menu, under the **BlackBerry solution management** section, click **Software > Applications > Manage default application control policies**. The **Manage default application control policies** page appears.
- 2 Click the **Standard Required** application control policy, or the policy in use your BlackBerry client application. On the page that appears, scroll to the bottom and click **Edit application control policy**.
- 3 Click the **Access settings** tab and set the following required settings:
 - **Are internal network connections allowed:** allowed
 - **Are external network connections allowed:** allowed
 - **List of internal domains:** *.messageone.com
 - **List of external domains:** *.messageone.com

The following setting is not required but is recommended unless Support tells you to use alternate settings:

- **Is access to the phone API allowed:** allowed

To create and populate the software configuration:

- 1 From the BAS navigation menu, under the **BlackBerry solution management** section, click **Software > Create a software configuration**. The **Create a software configuration** page appears.
- 2 Enter a **Name** for the BlackBerry client application, such as BBC Agent. All other values can be left at their defaults.
- 3 Scroll to the bottom of the page and click **Save**. You are returned to the **Create a software configuration** page, with the new configuration listed.
- 4 Click the name of the configuration you just created. The **Manage software configurations** page appears.
- 5 Scroll to the bottom of the page and click **Edit software configuration**. The **Manage software configurations** page becomes editable.
- 6 Choose the **Applications** tab. Scroll to the bottom of the page and click the **Add applications to software configuration** link.
- 7 Use the BAS search features to find the BlackBerry client application, usually named `Email Continuity Agent (daemon)`. This application was added when you unzipped the ZIP file containing the application files.
- 8 Click the check box next to `Email Continuity Agent (daemon)`, then scroll to the bottom of the page and click **Add to software configuration**. The application appears on the **Applications** tab of the **Manage software configurations** page.
- 9 Accept all defaults, then scroll to the bottom of the page and click **Save All** to save the configuration.

To create a BlackBerry client user group:

- 1 From the BAS navigation menu, under the **BlackBerry solution management** section, click **Group > Create a group**. The **Create a group** page appears.
- 2 Enter a **Name** for the group, then click **Save**. The new group is listed on the **Create a group** page.
- 3 Click the name of the group. The **Manage groups** page appears.
- 4 Scroll to the bottom of the page and click **Add users to group membership**.
- 5 Use the BAS search features to find all users who will use the BlackBerry client, or import them from a file using the BAS import feature.
- 6 When the user list is complete, click **Add to group membership**.

NOTE Removing the BlackBerry Client for Users

To remove (uninstall) the BlackBerry client for a user, remove those user from the BlackBerry client user group.

To assign the software configuration to the BlackBerry client user group:

- 1 From the BAS navigation menu, under the **BlackBerry solution management** section, click **Group > Manage groups**. The **Manage groups** page appears.
- 2 Click the name of the BlackBerry client user group you created. When the group information appears, click the **Software configuration** tab.
- 3 Scroll to the bottom of the page and click **Edit group**. The available software configurations appear.
- 4 Move the BlackBerry client software configuration you created from the list of **Available software configurations** to the list of **Current software configurations**. Scroll to the bottom of the page and click **Save All**.

Sending the Agent to Users by Email

You can notify device users of the Wireless Continuity for BlackBerry feature and provide instructions on how to use it by email. However, this deployment method is not recommended as it will deploy the basic software with none of the configurations described in the previous sections. As a result, you will have to provide users with the information required to manually configure their local device firewalls and network access in order for the agent to function properly.

To send installation instructions to device users:

- 1 Log in to Email Continuity as an administrator.
- 2 In the navigation menu, click **BlackBerry Administration**. The **BlackBerry Device Information** page appears.

- 3 Click **Send Installation Instructions**. The **Edit Message** page appears.
- 4 Edit the default message as necessary. Note that any message you use must include the variable %__rimAgentUrl%. When the message is distributed to users, the variable inserts the URL from which the client software can be downloaded. When you have finished editing the message, click **Next**. The **Select Recipients** page appears.
- 5 In the pane on the right of the **Select Recipients** page, select the users who should receive the installation instructions.
- 6 Click **Add**. This moves the selections to the **Send notification to these users' devices** list. Repeat this for each tab view, as needed, until your recipient list is complete. For initial implementation purposes, you should select all users.

NOTE Only Users With Devices are Added

As you add recipients, the software expands any category selections you made to list individual users in the selected category and only adds users who have BlackBerry devices; that is, all users are initially added, but the agent is only sent to users who have BlackBerry devices.

-
- 7 When you finish adding all desired recipients, click **Next**. The **Verify Recipients** page appears. The page lists:
 - Current BlackBerry software versions installed by your users.
 - The number of devices for each listed software version.
 - Any warnings associated with use of the listed software versions installed.
 - 8 Select the appropriate BlackBerry software versions and click **Next**. The **Confirm** page appears.
 - 9 Review the message information. If needed, go **Back** to any previous page to make changes.
 - 10 When you complete all selections, click **Send**.

Installing the Outlook® Extension



The Outlook® Extension is provided to you by Support as an MSI file designed to be compatible with standard distribution methods. The Outlook Extension conforms to Microsoft-approved Outlook Integration APIs and uses Extended MAPI and Outlook Object Model to interact with Outlook.

Guidelines for installing the Outlook Extension:

- MessageLabs recommends that Outlook not be running during the installation process.

- You must use the setup.exe for manual installation, and installations when users are logged in to Outlook. Use the MSI for automated installation (such as with GPO or SMS), when users are not logged in to Outlook.
- Select one method of installation (GPO, SMS, or manual), then use it consistently. Do not combine methods of install/uninstall. For example, if a user installs the Outlook Extension through setup.exe, the application cannot be reinstalled or updated through GPO, unless the user first uninstalls the Extension manually. Similarly, if the software has been installed using GPO, it cannot be removed using the Add/Remove Programs function.
- Outlook Extension can support multiple users running on the same machine in an enterprise environment. However, to enable this feature, the installation must be done using local administrator privileges, and the GPO method must be used. See ["Installation Using Group Policy" on page 77](#).
- After the Outlook Extension has been installed, its directory location **can never be changed**. You cannot uninstall the software, then reinstall it in a different location.

The installer follows this process:

- 1 The installer runs the necessary prerequisite checks.
- 2 The installer creates the INSTALL directory.
- 3 The installer copies the following to the INSTALL directory.
 - m1ext.ECF
 - m1ext.dll
 - m1resource.dll
 - m1command.dll
 - m1common.dll
 - Branding.ini
- 4 The installer sets up the registry entries.
- 5 A system search locates the ADDINS in InstallShield.
- 6 The M1EXT.DLL is marked as self-registering. The regsvr32 is called to register and unregister the DLL.
- 7 InstallShield modifies the m1ext.ecf file; the PATH is set to the ADDINS directory cited above.

The Outlook Extension sets the Registry Keys described in [Table 3-1](#).

The installer writes out to HKLM key, which becomes default (read-only values). When Outlook® starts and the Extension runs, it updates the HKCU key (based on HKLM and user preferences).

Table 3-1 Outlook Extension Registry Keys

Location	Key
HKEY_LOCAL_MACHINE\Software\MessageOne\EMS\Install	Working Directory “[INSTALLDIR]”
HKEY_LOCAL_MACHINE\Software\MessageOne\EMS\LogSettings	<ul style="list-style-type: none"> • FlushUpdate • SeverityLevel • LogFilePath • FlushAll • TruncateAfter
HKEY_LOCAL_MACHINE\Software\MessageOne\EMS\WebRequests	<ul style="list-style-type: none"> • HostName • MsgFileSizeKB • EMailDir • authToken • Username
HKEY_LOCAL_MACHINE\Software\MessageOne\EMS\Timers	<ul style="list-style-type: none"> • LoginStatusTimer • InitTimer • EnableControls • CheckStateTimer • PollTimer • RetrieveTimer • SwitchToOfflineTimer • LoginResetTimer • StartSMTimer
HKEY_LOCAL_MACHINE\Software\MessageOne\EMS\Persistent	
HKEY_LOCAL_MACHINE\Software\MessageOne\EMS\Help	

Outlook® Extension uses an authentication token stored at HKEY_CURRENT_USER\Software\MessageOne\EMS\Profile Info\Outlook\AuthToken to allow a user to use the Extension features without having to log in to Email Security Services. The token can be created by a user logging in with a password, or the administrator can run a command line tool to create authentication tokens for one or more users. (See [Enabling User Authentication Through the Command Line](#).) After the authentication token is set the user will not need to log in again during an activation or while using other Extension features.

Enabling User Authentication Through the Command Line

You can use the command line tool **PrepareOutlookAuth** to authenticate (register) users automatically. This allows authenticated (registered) users to use Extension features without providing a password. The tool is installed with the SyncManager on the primary controller. You must complete a directory sync before running this tool. When you run the tool using the **-all** argument, it walks through all user mailboxes and writes an authentication token to a hidden message if a token is not there already. The message is stored in the associated Contents table of the IPM_SUBTREE folder. If you have developer tools such as MFCMapi or Outlook Spy, you can look at the Associated Contents table of the IPM_SUBTREE folder for the message with the subject *Authentication*.

NOTE SyncManager

MessageLabs recommends you upgrade the SyncManager software to version 6.0 or later prior to installing the Extension. If your organization uses distributed SyncManager, the PrepareOutlookAuth tool should only be run on the primary SyncManager server.

TIP Run PrepareOutlookAuth prior to deploying the Outlook Extension

For best results, run this command a day or two before deploying the Outlook Extension, so that the SyncManager has time to complete a sync before the software is installed for users. Otherwise, users must restart Outlook again after the next directory sync.

The following arguments are available. You must use either **-user<mailboxDN>** or **-all**. Other arguments are optional.

Table 3-2 PrepareOutlookAuth Arguments

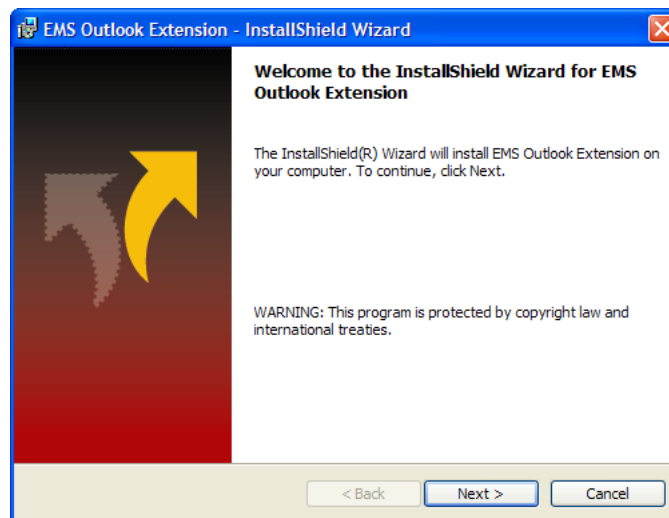
Argument	Definition
-all	Updates authentication for all users
-rewrite	Writes authentication tokens to all mailboxes (even if a token is already present)
-user <mailboxDN>	Writes an authentication token for a specific user only (even if a token is already present). The Mailbox DN value comes from the Active Directory value legacyExchangeDN. Use ADSI Edit to find this value. The value must be entered in lower case, in quotes (for example: "/o=first organization/ou=first administrative group/cn=recipients/cn=testuser")
-verbose	Enables verbose output
-help	Displays usage information

To authenticate users through the command line (prior to Outlook Extension deployment):

- 1 Open a command-line prompt on the server on which SyncManager is installed.
- 2 Go to the following directory: C:\Program Files\MessageLabs\ESS.
- 3 Enter either:
 - `-prepareoutlookauth.exe -user "mailboxdn"`
 - `-prepareoutlookauth.exe -all`
- 4 Wait for the new mailbox properties to take effect, approximately an hour.
- 5 Install Outlook Extension using one of the documented processes. When a user starts Outlook, the Extension toolbar appears, and the user has access to Extension features without entering his password.

Manual Installation**To install the Outlook Extension manually using setup.exe:**

- 1 Exit the Outlook® application, if it is open.
- 2 Double-click the **setup.exe** provided to you by Support to launch the InstallShield Wizard.



- 3 Click **Next**.
- 4 The default installation location is C:\Program Files\MessageLabs\Outlook Extension. To change the location, click **Change**, browse to a new location, and click **OK**. To accept the default location (Recommended), click **Next**.
- 5 Click **Install**. Installation may take a few minutes.
- 6 Click **Finish**.

- 7 Launch Outlook®. The Outlook Extension toolbar displays and the **Tools > Options** screen includes a tab for MessageLabs Email Continuity.

To remove the Outlook Extension manually:

- 1 Exit Outlook, if the application is open.
- 2 Select **Start > Control Panel > Add or Remove Programs**.
- 3 In the **Currently installed programs:** field, scroll to Email Continuity Outlook Extension, and click it.
- 4 Click **Remove**.
- 5 In the confirmation dialog box, click **Yes**.

Installation Using Group Policy

NOTE GPO Administration Experience Required

These instructions presume familiarity with creating and distributing software using GPO. Not all steps in the process are documented here, as each organization's environment is unique, and distribution practices may vary.

The Outlook Extension can be distributed through group policy; this method was tested, and is supported, under the following conditions and using the following process.

- The Group Policy Object Editor provides configuration settings at the Computer and User levels. Outlook Extension packages should be assigned using the Computer Configuration hierarchy.
- The Group Policy Object Editor does not display full version numbers. Consequently, MessageLabs recommends using the complete version number in the package name (for example, Outlook Extension 6-1-0-8015).

WARNING Use the same method for installation and removal of the Extension

If you install the Outlook Extension through Group Policy, you must remove it using Group Policy.

To install the Outlook Extension using Group Policy:

- 1 Create a new GPO package using the Outlook Extension MSI.
- 2 Open the package in the GPO editor.
- 3 Expand **Computer Configuration**.
- 4 Expand **Software Settings**.
- 5 Right-click **Software Installation** and select **New > Package**.
- 6 Browse for the Outlook Extension MSI, select it, and click **Open**.

- 7 In the **Deploy Software** dialog, select **Assigned**, then click **OK**.
- 8 Link the GPO to the Organizational Unit (OU) that contains the target computers.
 - a. Right-click the OU and select **Link an Existing GPO**.
 - b. In the **Group Policy objects:** field, click the GPO.
 - c. Click **OK**.

To upgrade the Outlook Extension using Group Policy:

Add the new Outlook Extension MSI to the existing policy.

- 1 Open the package in the GPO editor.
- 2 Expand **Computer Configuration**.
- 3 Expand **Software Settings**.
- 4 Right-click **Software installation** and select **New > Package**.
- 5 Browse for the Outlook Extension MSI, select it, and click **Open**.
- 6 In the left pane, click **Software Installation**. In the right pane, right-click the Outlook Extension package and select **Properties**.
- 7 Click **Upgrades**. In the **Upgrades** tab, **Add Packages this package will update** field, click **Add**.
- 8 In the **Add Upgrade Package** dialog, click **Current Group Policy**.
- 9 In the **Package to Upgrade** field, select **Uninstall the existing package, then install the upgrade package**. Click **OK**.
- 10 Restart the machines.

To remove the Outlook Extension using Group Policy:

- 1 Edit the Group Policy Object.
- 2 Expand **Computer Configuration**.
- 3 Expand **Software Settings**.
- 4 Click **Software installation**. In the right panel, right-click the package and select **All Tasks > Remove**.
- 5 Select the **immediate removal** method, and click **OK**.

Installation Using Systems Management Software (SMS)

The Outlook Extension MSI can be distributed by SMS; this method was tested, and is supported, using SMS2003 SP2 and the following process.

NOTE SMS Administration Experience Required

These instructions presume familiarity with creating and distributing software using SMS. Not all steps in the process are documented here, as each organization's environment is unique, and distribution practices may vary.

To install the Outlook Extension using SMS:


- 1 Using the SMS Create Package from Definition wizard, build an SMS package using the EMS Outlook Extension MSI.

NOTE Per-system unattended vs. Per-system attended Installation

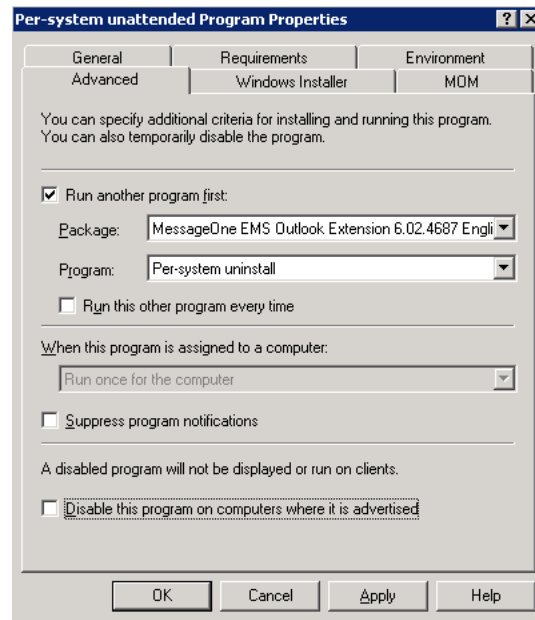
If your users are logged in to Outlook, install the Extension using the EXE and the Per-system attended function. If your users are not logged in to Outlook, use the MSI and the Per-system unattended function. You may want to use the `install only when no user is logged in` option when distributing by MSI.

- 2 In the **Site Database** menu tree, expand **Packages**.
- 3 Expand the Outlook Extension package and click **Programs**.
- 4 In the right pane, right-click **Per-system unattended > All Tasks > Distribute Software**. The Distribute Program Wizard launches.
- 5 Complete the Wizard.
- 6 Advertise the package to the target collection, according to your organization's established process.

To upgrade the Outlook Extension using SMS:

- 1 Verify that the SMS package created with the previous version of the MSI still exists; if not, recreate it.
- 2 Define a Collection of hosts with the prior version of the MSI installed. To do this:
 - a. In the **Site Database** menu tree, select **Collections > New > Collection**.
 - b. In the **Collection Properties** window, **General** tab, name the Collection.
 - c. Click the **Membership Rules** tab.
 - d. Click the **Query Rule Properties** icon. 
 - e. In the **General** tab, name the Query.
 - f. In the **Resource Class** field, select `System Resource`.

- c. In the **Program** drop-down list, select **Per-system uninstall**.



- d. Click **Apply**, then **OK**.

- 8 Use the Distribute Software Wizard to advertise the package.
- In the **Programs:** field, select **Per-system unattended**.
 - In the **Advertisement Target** screen, click the **Advertise this program to an existing collection:** button.
 - Click **Browse**, and select the Collection you defined above. Click **OK**.
 - Complete the Wizard according to your organization's established practices.

To remove the Outlook Extension using SMS:

- In the **Site Database** menu tree, expand **Packages**.
- Expand the package containing the Outlook Extension.
- Click **Programs**.
- In the right pane, right-click **Per system uninstall**, and select **All Tasks > Distribute Software**.
- Complete the Distribute Program Wizard to advertise the package to the target collection, according to your organization's established process.

Troubleshooting Installation of the Outlook Extension

If the Extension toolbar does not appear in the Outlook application:

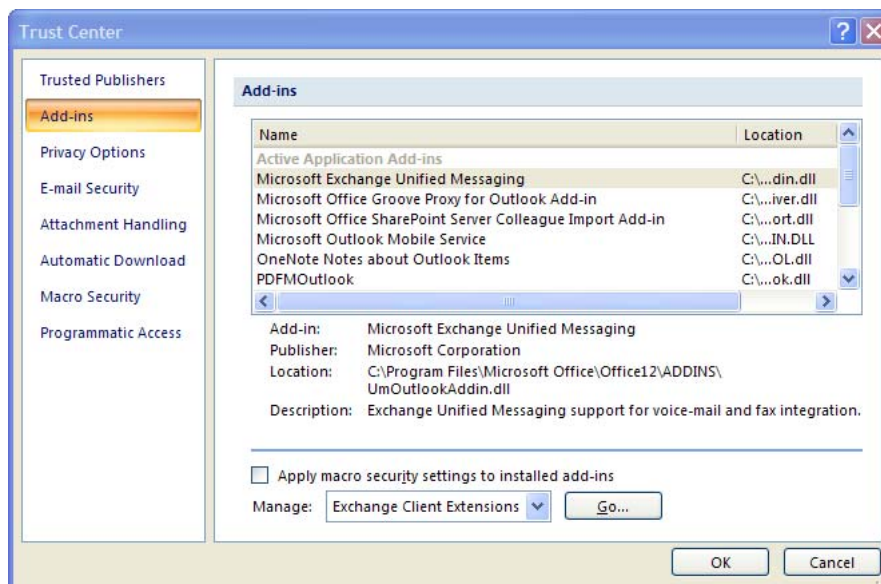
- 1 Exit Outlook and restart it.
- 2 Verify the Extension-related files are present; C:\Program Files\MessageLabs\Outlook Extension and the registry keys listed in [Table 3-1 on page 74](#).

If the files are not present, the install did not finish correctly. Uninstall, using the same method you used to install, and try again.

- 3 If the files are present, but the toolbar does not appear:

Outlook 2003: Open **Outlook > Tools > Options > Other > Advanced Options > Add-in Manager**.

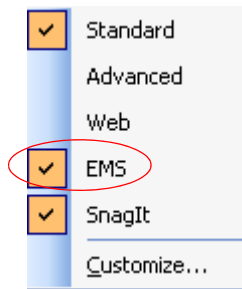
Outlook 2007: Open **Help > Privacy Options > Add-ins > Manage:** drop-down, select Exchange Client Extensions, and click **Go**.



If the Outlook Extension is in the add-in list and checked, go to [step 4](#).

- a. If the Extension is in the list, but not checked, check the box.
- b. If the Extension is not in the list:
 - (1) Close Outlook, and verify the process is gone from Task Manager.
 - (2) Open **C:\Documents and Settings\[username]\Local Settings\Application Data\Microsoft\Outlook** and delete `extend.dat`.
 - (3) Open Outlook. The Extension appears in the **Add-in Manager** list, and is checked.

- 4 Right-click the Outlook toolbar area. Verify the Extension appears, checked, in the list of applications.



- a. In the toolbar menu, select **Help > About Microsoft Office Outlook > Disabled Items**.
- b. If the Extension is there, select it, and click **Enable**.

Installing Custom Forms in Exchange 2000/2003 (Storage Management Only)

You must publish custom forms to the Organizational Forms Library on the Exchange Server for the storage management feature of the Outlook® Extension to work as described. The custom form files are included in the Outlook Extension installation package.

The Outlook® Extension custom forms are:

Archived.oft—Message class is IPM.Note.MessageOneStubbed

Locked.oft—Message class is IPM.Note.MessageOneLocked

If one has not yet been created, use Exchange System Manager to add a new folder to the Exchange Organizational Forms Library.

To add a new folder to Exchange Organizational Forms Library in Exchange 200/2003:

- 1 In System Manager, expand **Administrative Groups**.
- 2 Expand your organization's **Administrative Group**
- 3 Expand **Folders**
- 4 Right-click **Public Folders**, and select **View System Folders**.
- 5 Expand **Public Folders**, and select **EFORMS REGISTRY**
- 6 Right-click **EFORMS REGISTRY**, and select **New > Organizational Form**
- 7 In the dialog box that appears:
 - a. Type a name (such as `Extension`).
 - b. Type an optional Public folder description, (such as `Extension Forms`).

- c. Select the appropriate language.
- 8 Click the **Replication** tab, and add the Public Folder Stores from additional Exchange servers in your environment.
- 9 Click **OK**, then reopen the properties dialog for the new folder.
- 10 Right-click the new folder, select **All Tasks > Mail Enable**.
- 11 Click the **Permissions** tab, and configure a user account with Client Permissions, and Administrative Rights. This account is used to publish the forms to this folder.
- 12 Click **OK** to complete creating the new Organizational Forms Library.
- 13 Restart Microsoft Outlook® using the account previously specified with enhanced permissions.

To publish forms to the Exchange Organizational Forms Library:

- 1 In Outlook®, select **Tools > Forms > Choose Form...**
- 2 In the **Choose Form** dialog, **Look In** drop-down list, select `User Templates in File System`.
- 3 Click **Browse** and select the directory where the forms are present
- 4 In the **Choose Form** dialog list, select the `Archived.oft` form, then click **Open**.
- 5 In the newly opened message window, select **Tools > Forms > Publish Form As...**
- 6 In the **Publish Form As** dialog, **Look In** drop-down list, select `Organizational Forms Library`.
- 7 In the **Display Name** field, enter `MessageOneStubbed`, (capitalized as shown), then click **Publish**.
- 8 In Outlook®, select **Tools > Forms > Choose Form...**, and repeat this process to publish the `Locked.oft` form, using a Display Name of `MessageOneLocked`.

The extra client permissions and administrative rights can now be deleted. The newly published forms may not be available to users until the next time they start Microsoft Outlook®.

For more information on custom forms, see *How to Create an Organizational Forms Library in Exchange* at <http://support.microsoft.com/?kbid=244591>.

Installing Custom Forms in Exchange 2007 (Storage Management Only)

You must publish custom forms to the Organizational Forms Library on the Exchange Server for the storage management feature of the Outlook® Extension to work as described. The custom form files are included in the Outlook Extension installation package.

The Outlook® Extension custom forms are:

Archived.oft—Message class is IPM.Note.MessageOneStubbed

Locked.oft—Message class is IPM.Note.MessageOneLocked

If one does not yet exist, create an organizational forms library.

To create an organizational forms library in Exchange 2007:

(Refer to <http://support.microsoft.com/kb/933358> for more information.)

- 1 Click **Start**, point to **All Programs**.
- 2 Click **Microsoft Exchange 2007 Server**.
- 3 Click **Exchange Management Shell**.
- 4 Run the following command:

```
New-PublicFolder -Path "\NON_IPM_SUBTREE\EFORMS  
REGISTRY" -Name "My Organizational Forms Library"
```
- 5 Using an account belonging to the Exchange Administrators Group, log on to a client computer that is running Microsoft Office Outlook 2003 or later.
- 6 From the MFCMAPI folder, start the Microsoft Exchange Server MAPI editor (Mfcmap.exe.)

If you do not have the MAPI Editor, see: <http://go.microsoft.com/?linkid=5684182>.
- 7 If you do not already have one, create a MAPI profile.
- 8 In the **Session** menu, click Logon, and **Display Store Table**.
- 9 On the **MDB** menu, click **Open Public Store**, and click **OK**.
- 10 Expand **Public Root**, then **NON_IPM_SUBTREE**, then **EFORMS REGISTRY**.
- 11 Click the public folder you created earlier in this procedure.
- 12 Click the **PR_URL_NAME** property.
- 13 On the **Property Pane** menu, click **Modify Extra Properties**.
- 14 Click **Add**, then click **Select Property Tag**.
- 15 Select **PR_EFORMS_LOCALE_ID** from the list; click **OK**.

- 16 Click **OK**, then click **OK** again. A red mark appears next to the new `PR_EFORMS_LOCALE_ID` property.
- 17 Double-click **`PR_EFORMS_LOCALE_ID`**.
- 18 In the **Unsigned Decimal** field, type the desired locale ID, and then click **OK**.

For example, type 1033 for English, type 1040 for Italian, or a different ID for a different locale. To determine the locale ID for other areas see: <http://msdn2.microsoft.com/en-us/library/aa579489.aspx>
- 19 Exit MAPI editor.

To publish forms to the Exchange Organizational Forms Library:

- 1 In Outlook[®], select **Tools > Forms > Choose Form...**
- 2 In the **Choose Form** dialog, **Look In** drop-down list, select `User Templates in File System`.
- 3 Click **Browse** and select the directory where the forms are present
- 4 In the **Choose Form** dialog list, select the `Archived.oft` form, then click **Open**.
- 5 In the newly opened message window, select **Tools > Forms > Publish Form As....**
- 6 In the **Publish Form As** dialog, **Look In** drop-down list, select `Organizational Forms Library`.
- 7 In the **Display Name** field, enter `MessageOneStubbed`, (capitalized as shown), then click **Publish**.
- 8 In Outlook[®], select **Tools > Forms > Choose Form...**, and repeat this process to publish the `Locked.oft` form, using a Display Name of `MessageOneLocked`.

The newly published forms may not be available to users until the next time they start Microsoft Outlook[®].

For more information on custom forms, see *How to Create an Organizational Forms Library in Exchange* at <http://support.microsoft.com/?kbid=244591>.

Installing Historical Mail/Email Archive



Before you can install the Historical Mail/Email Archive software you need to prepare all the computers that will become VaultBox systems. To do this, you need to know the following information about each VaultBox system:

- Its name
- The drive on which you will install the software

- The location of the cache directory where email messages arrive by SMTP before transmission to the data center

CAUTION Required Drive Space

Be sure you identify a drive with enough space for seven times the expected volume of daily mail. If you fail to install the Historical Mail software on a drive with enough space, the feature will not work properly.

NOTE Enable SMTP Logging

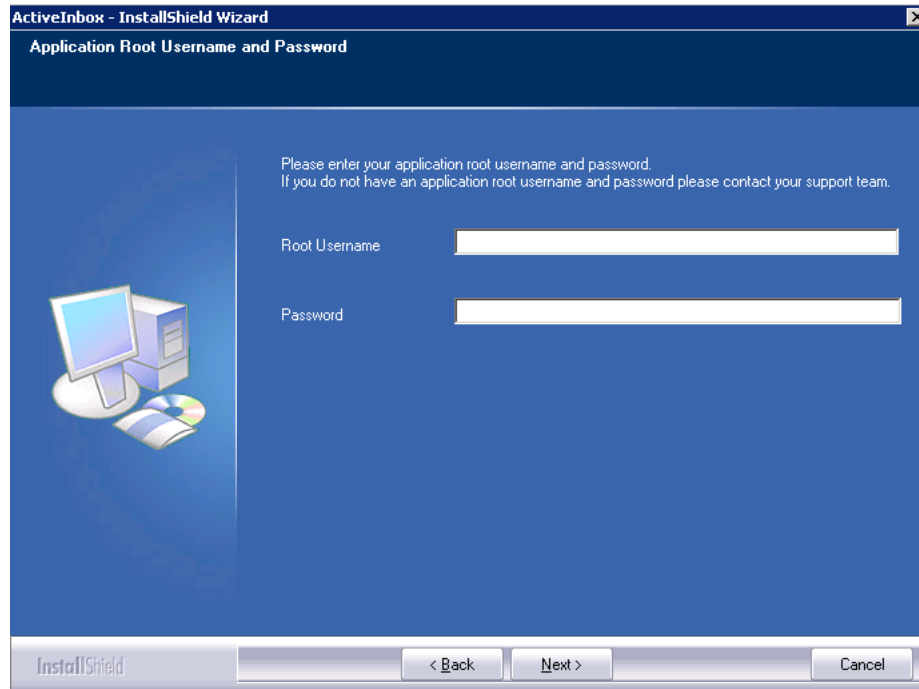
Verify that the following logs have been enabled for Email Archive audit tracking:

- On the Exchange server, confirm that logging through the SMTP virtual server is enabled and configure sufficient log file space to hold 7 days of logging.
 - On the VaultBox, enable SMTP logging of the Transfer service and configure sufficient log file space to hold 7 days of logging.
-

To install the Historical Mail software on a VaultBox system:

- 1 Access your Historical Mail (ActiveMailbox) installation package provided by Support. Locate and double-click **setup.exe**.
- 2 If you don't already have SQL installed, the wizard installs Microsoft SQL Server 2005 Express.
- 3 The InstallShield Wizard launches and guides you through the installation process.

- 4 In the **Root Username and Password** window, enter the user name and password for the service root account or a valid super administrator account. If you don't have this information, contact Support.



ActiveInbox - InstallShield Wizard

Application Root Username and Password

Please enter your application root username and password.
If you do not have an application root username and password please contact your support team.

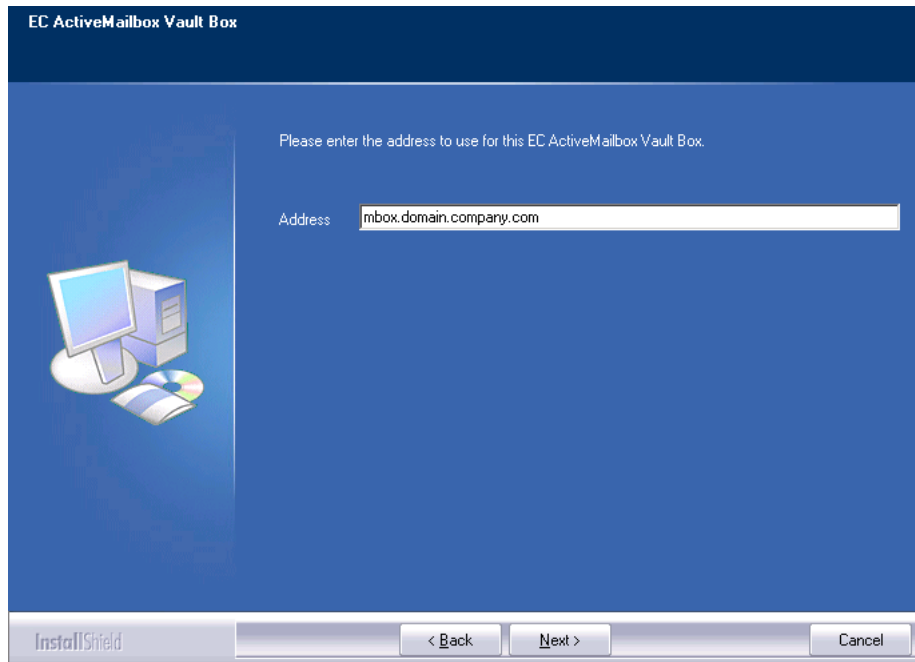
Root Username

Password

InstallShield

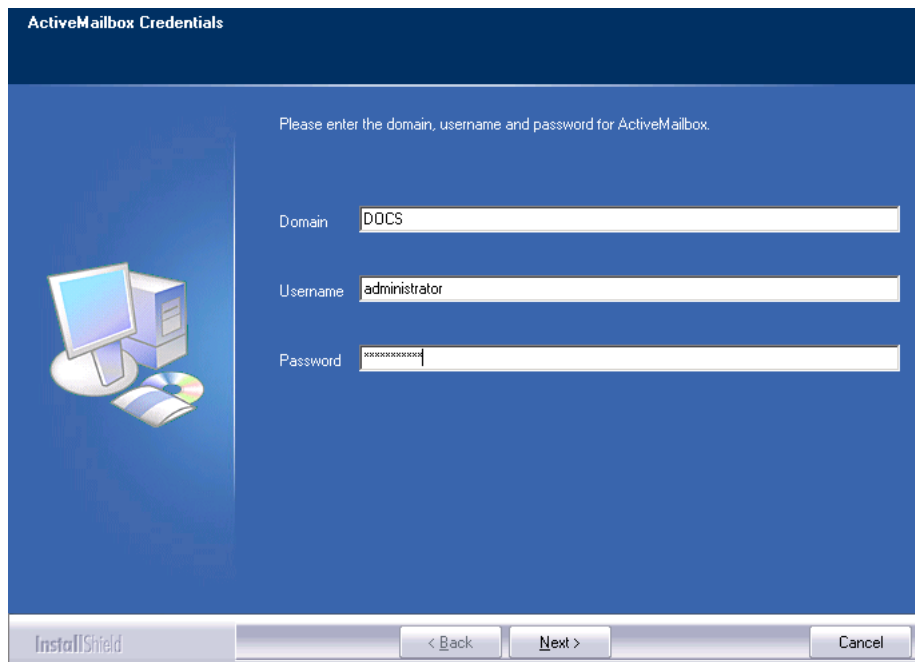
- 5 Click **Next**.
- 6 The **Available Components** window tells you which components are available to install. Click **Next**.
- 7 Select the components that you want to install, then click **Next**.
- 8 When prompted to allow the install to stop any IIS-related service, click **Yes**.
- 9 The **Destination Folder** populates by default. Click **Next** to accept the installation location, or click **Browse** to set a new location.

- 10 In the **ESS ActiveMailbox Vault Box** window, enter the address for the specific VaultBox system.



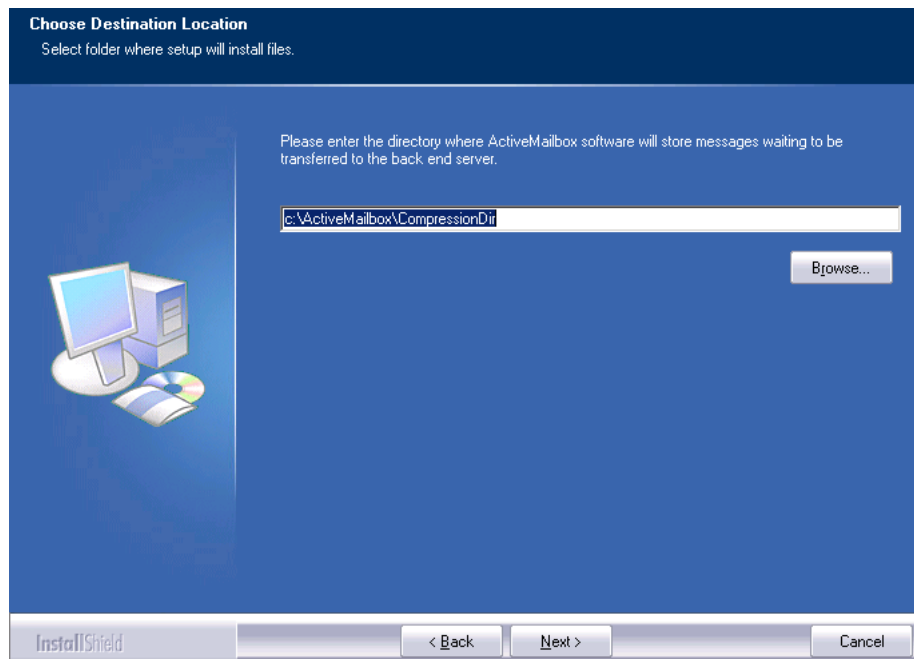
The screenshot shows the 'EC ActiveMailbox Vault Box' configuration window. The title bar reads 'EC ActiveMailbox Vault Box'. The main area has a blue background with a computer icon on the left. The text says 'Please enter the address to use for this EC ActiveMailbox Vault Box.' Below this is a text box labeled 'Address' containing the text 'mbox.domain.company.com'. At the bottom, there is an 'InstallShield' logo and three buttons: '< Back', 'Next >', and 'Cancel'.

- 11 In the **ESS ActiveMailbox Service Credentials** window, enter the requested domain, username, and password for the account. Click **OK**.



The screenshot shows the 'ActiveMailbox Credentials' configuration window. The title bar reads 'ActiveMailbox Credentials'. The main area has a blue background with a computer icon on the left. The text says 'Please enter the domain, username and password for ActiveMailbox.' Below this are three text boxes: 'Domain' with 'DQCS', 'Username' with 'administrator', and 'Password' with a masked password 'xxxxxxxxxx'. At the bottom, there is an 'InstallShield' logo and three buttons: '< Back', 'Next >', and 'Cancel'.

- 12** In the **Choose Destination Location** windows, separate screens prompt for destinations for the ActiveMailbox files and the directory for mail storage prior to transfer (compression directory). Whenever possible, accept the default location and respond **Yes** when prompted to create the directory.



- 13** Click **Next**. The **Start Copying Files** window lists the components to install.
- 14** Click **Next**. The **Setup Status** window displays installation progress.
- 15** When the installer completes, click **Finish**.

Configuring VaultBoxes



In order for the Historical Mail feature to function, you must configure settings on each VaultBox system in your environment.

Changing Settings in the VaultBox Console

The VaultBox coordinates the transfer of data from your organization's Exchange servers to the data center. You can view VaultBox status and set parameters governing data transfer using the VaultBox Console.

To launch the VaultBox Console, select **Start > Programs > MessageLabs > VaultBox Console** on the machine on which it is installed. The VaultBox Console appears.

From the VaultBox Console you can:

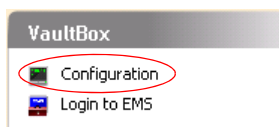
- Start and stop Storage Management, and edit Storage Management settings. If your organization uses the storage management feature, you must configure additional VaultBox settings. See "[Configuring Scanning and Data Transfer from the VaultBox Console](#)" on page 115 for more information.
- Start and stop Manual (User Classification) Retention and edit Manual Retention settings. If your organization uses the user classification retention feature, you must configure additional VaultBox settings. See "[User Classification Retention Policies](#)" on page 105 for more information.
- View **Transfer Service Status** fields.

The **Transfer Service Status** fields display the following parameters:

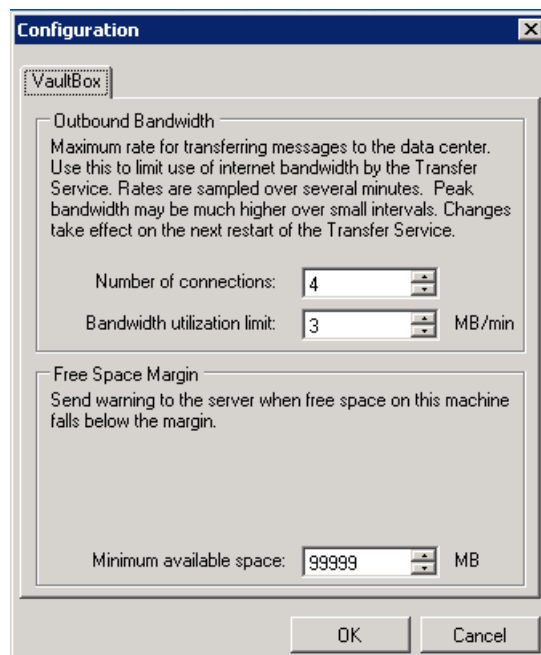
- **Queue**—The number of messages to be transferred to the data center
- **Rate**—The transfer speed, in messages/second and KB/second
- **Free Space**—The amount of space remaining on the VaultBox

To change data transfer settings:

- 1 In the **VaultBox** pane, click **Configuration**.



- 2 Click the **VaultBox** tab to display data transfer settings.



The **Outbound Bandwidth** pane controls data transfer between the Transfer Service and the data center.

- 3 In the **Number of connections** field, use the up/down arrows to alter the number of connections (threads) used by the process.
- 4 In the **Bandwidth Utilization limit** field, change the amount of bandwidth used for data transfer. (A setting of 0 in this field allows unlimited usage).
- 5 The **Free Space Margin** pane configures the VaultBox to send a warning message to the server when free space on the VaultBox machine falls below the set margin. In the **Minimum available space** field, set the threshold below which the storage management task should send a warning.
- 6 Click **OK**.

Monitoring VaultBoxes



Typically, you monitor VaultBox status through the VaultBox Console and Administration Console. However, if your organization uses a third party monitoring tool, Support recommends that you also monitor the data described in the table below.

NOTE **Hostname for data centers**

Several of the troubleshooting suggestions below require you to telnet to the [hostname] of the data center used by your organization. To find the appropriate hostname, refer to the Network Settings document provided by Support.

Table 3-3 VaultBox Monitoring

Data Type	Description	Alert When	Troubleshooting Suggestions
Free space on each designated VaultBox system	Ensure that adequate free space remains on both the C drive of the VaultBox system (where IIS puts intermediate files), the drive location of the VaultBox cache directory, and the Compression Directory.	Data drive is 10% full	<ol style="list-style-type: none"> 1 Clean up disk space outside of [Data Drive]:\activemailbox\compressiondir*. * 2 If used disk space still exceeds 10%, verify the Vaultbox can connect to the data center, as follows: <ul style="list-style-type: none"> • telnet [hostname]22 • If you do not get an OpenSSH response, the port is likely blocked; check the firewall. 3 If the connection is good, shut down, then restart the transfer service. 4 Wait one hour. If the disk space has not reduced, collect the SRTransferService.log files, and contact Support.
Number of files in a directory	[Data Drive]:\activemailbox\compressiondir*. *	More than 1000 files are present	<ol style="list-style-type: none"> 1 Verify the Vaultbox can connect to the data center, as follows: <ul style="list-style-type: none"> • telnet [hostname]22 • If you do not get an OpenSSH response, the port is likely blocked; check the firewall. 2 If the connection is good, shut down, then restart the transfer service. 3 Wait one hour. If the number of files has not reduced, collect the SRTransferService.log files, and contact Support.

Table 3-3 VaultBox Monitoring

Data Type	Description	Alert When	Troubleshooting Suggestions
Timestamp of files in a directory	[Data Drive]:\activemailbox\compressiondir*.*	Oldest file is older than 60 minutes	<ol style="list-style-type: none"> 1 Verify the Vaultbox can connect to the data center, as follows: <ul style="list-style-type: none"> • telnet [hostname]22 • If you do not get an OpenSSH response, the port is likely blocked; check the firewall. 2 If the connection is good, shut down, then restart the transfer service. 3 Wait one hour. If newer timestamps do not appear, collect the SRTransferService.log files, and contact Support.
CPU utilization	Using the Windows Performance Monitor, verify that the Total instance of the % Processor Time counter of the Processor performance counter object is less than 80 percent.		
Performance counters	The Message queue size counter of the Transfer Service object should be less than 10,000. Other counters under the Transfer Service are also useful for determining daily message volume.		

Table 3-3 VaultBox Monitoring

Data Type	Description	Alert When	Troubleshooting Suggestions
Services	<p>If you are using a separate monitoring tool, include the following services for your VaultBox system:</p> <ul style="list-style-type: none"> • SMTPSVC, which displays as Simple Mail Transfer Protocol (SMTP) • srtransfersvc, which displays as Selective Replication Transfer Service 	Selective Replication Transfer Service stops	<ol style="list-style-type: none"> 1 Restart transfer service 2 Examine general system logs for other service failures or system errors 3 If service fails to restart, or fails again within a 24-hour period, contact Support
Store driver and IIS SMTP service	Mail is not reaching the Vaultbox, or is not being transferred to the data center		<ol style="list-style-type: none"> 1 Verify the SMTP service on the Vaultbox is running. 2 Verify that the POP3 service on the Vaultbox is NOT running. 3 Verify the Store Driver is connected to the SMTP Service (the Administration Console Readiness check will indicate an error).

4 Administration

This chapter covers the following topics:

- ["Logging Into the Administration Console" on page 97](#)
- ["Administration Console Home" on page 98](#)
- ["Historical Mail Administration" on page 103](#)
- ["User Administration" on page 131](#)
- ["Enabling BlackBerry Forwarding" on page 152](#)
- ["Wireless Continuity for BlackBerry Administration" on page 154](#)
- ["Outlook® Extension Administration" on page 157](#)
- ["Mailboxes and Aliases" on page 158](#)
- ["Mailing Lists" on page 159](#)
- ["Notification" on page 159](#)
- ["Viewing Audit Reports" on page 167](#)
- ["Modifying System Settings" on page 171](#)
- ["Changing Your Account Settings" on page 178](#)
- ["Testing Email Continuity" on page 180](#)

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 141](#).
- **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 143](#).

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**.
-

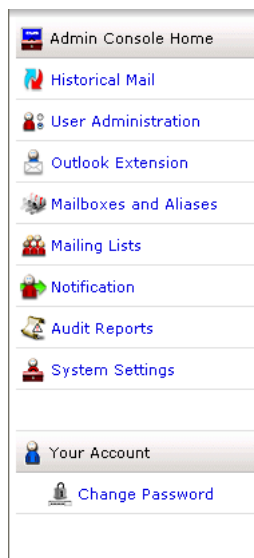
NOTE Some Described Features May Not Appear

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, calendar entries, 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 164 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 calendar synchronization	Reports the last time a Calendar 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.
*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).
Default RIM Synchronization (for Wireless Continuity for BlackBerry only)	Reports the last time a RIM synchronization completed successfully. If a scheduled synchronization is more than 12 hours overdue or if a synchronization reported as failed, the status check will report as failed. The <code>SyncManagerService.log</code> file on the server running SyncManager in your environment may contain information that is useful for debugging failures.

Table 4-2 Readiness Checks

Readiness Check	Descriptions
Authentication Manager (per server) (for Windows Authentication only)	Reports the last time a particular Authentication Manager connected to the data center. If an Authentication Manager is unable to connect to the data center, verify that the Authentication Manager service is running on the specified computer and that it can access the data center over port 443.
Controller Status (per server)	Reports the last time a particular RedirectorController connected to the data center. If a RedirectorController is unable to connect to the data center, verify that the Controller service is running on the specified computer and that it can access the data center over port 443.
RedirectorSink Status (for Exchange environments only)	Reports any Exchange servers that do not have a RedirectorSink installed, as well as any servers that have a RedirectorSink installed, but are not currently in communication with at least one RedirectorController. The best practice recommendation is that all Exchange 2000/2003 servers have the RedirectorSink installed, all Exchange 2007 Hub Transport servers have the RedirectorAgent installed, and that these be in communication with at least two RedirectorControllers.
*User Directory Status (for Exchange environments only)	Reports user ID conflicts detected by the SyncManager using primary email address.
VaultBox (for Email Archive only)	Reports the last time a VaultBox connected to the data center. If a VaultBox is not connected, verify that the Simple Mail Transfer Protocol (SMTP) service, Selective Replication Transfer Service, and VaultBox monitor are started. Additional information for debugging can be found in the <code>SRTransferService.log</code> files on the associated VaultBox.
Server Assigned to Replication Zone (for Email Archive only)	Reports any servers that are currently not assigned to a replication zone. All servers must be assigned to a replication zone.

NOTE RedirectorSink Communication

Support recommends that all servers be able to communicate with all RedirectorSinks for correct redirection of mail if an outage affects some RedirectorControllers and not others.

TIP Partial Activation and RedirectorSink Updates




After a partial activation, status updates of RedirectorSinks can take up to 90 seconds and it can take up to three minutes for these updates to display in the Administration Console. During this waiting period, `Updating Mail Routing Configuration` appears as a pending task in the Activity Log section.

Authentication Manager Status

The Authentication Manager allows end users to log in to the Email Continuity portal using their Windows username and password.

To access the Authentication Manager status screen click the **Details** link in the Email Security Services Authentication Manager readiness check entry.

Table 4-3 Authentication Manager Status icons

Icon	Definition
	The Authentication Manager is connected to the Email Security Services server.
	The Authentication Manager is not connected to the Email Security Services server.
	The Authentication Manager is connected to the Email Security Services server, but cannot authenticate users.

RedirectorController/RedirectorSink/RedirectorAgent Status

The RedirectorController is software that communicates with the data center and provides updates to the RedirectorSinks and RedirectorAgents. The RedirectorSink is An SMTP Event Sink that enables dynamic rerouting of messages, allowing some users to remain on the primary mail system while others use Email Continuity—a process called *Partial Activation*. Also transfers copies of mail to the VaultBox for users of Historical Mail. The RedirectorAgent is a custom transport agent that performs functions similar to the RedirectorSinks to support the partial activation feature for Email Continuity in Exchange 2007 environments.

To access the Email Security Services RedirectorController/RedirectorSink status screen click the **Details** link in the Email Security Services RedirectorSink readiness check entry.

Table 4-4 Redirector Status Icons







Icon	Definition
	Connected to the Email Security Services server.
	Disconnected from the Email Security Services server.

Table 4-4 Redirector Status Icons (Continued)

Icon	Definition
	Component not installed
	Status reporting disabled
	The server has users who are active on Email Continuity
	The server has no users active on Email Continuity

Historical Mail Administration



The Historical Mail feature of Email Continuity allows users to access stored email during an activation of Email Continuity using a searchable web-based interface. You identify email to be stored by including it in a policy.

Retention Policies

A retention policy defines the amount of time email messages are stored in the system. If no policy is applied to a message, a default policy of 30 days is used.

Changes to policy membership and policy retention periods can have significant impact to the way that mail is stored for your organization.

NOTE Mail Purging

A retention policy determines when a message is eligible to be purged from the data center, not the actual date the message will be purged. Purging is performed in the data center; you may notice a delay between the date a message no longer must be kept according to the governing policy, and the date it disappears from the server. Purging does not occur while the Email Continuity service is active.

NOTE Purge Delay for Query Based Legal Holds

There is a window of time between ESS identifying a message eligible for purging and when all records of that message are actually deleted. If a legal hold defined during this window includes a message already identified for purge, that message will still be deleted. Eligible messages queued for purging may be reflected in the estimated count of messages for a query based legal hold, but will be deleted when the next purge is performed.

Membership-based (Current Membership) Policies

For *membership-based* policies, a message is retained based on whether the sender or recipient is a member of the policy. The message is retained only as long as the user remains a member of the group to which the policy applies. When a user is no longer part of the policy group the message is eligible for purging. Updates to membership-based policies occur after a directory synchronization or when an administrator modifies the policy.

Example 1: For example, a user is initially a member of the `Sales Group`, which has a membership-based retention period of 50 days. When the user separates from the sales organization and becomes part of the `Assistant Group`, a new membership-based policy applies. The new retention period is 20 days. On the first day that the user is a member of the `Assistant Group`, mail collected during days 21-50 is eligible for purging.

Example 2: A user is a member of the `Marketing Group` retention policy, which has a 30 day retention period. The last 30 days of mail is routinely retained. One day, the user leaves the company and his mailbox is disabled, hidden, or deleted. The next day, because the user is no longer part of the membership-based policy, the user's last 30 days of retained mail is eligible to be purged.

Example 3: A user is initially a member of the `All Employees` retention policy, which has a 30 day retention period. An administrator increases the `All Employees` retention period to 45 days. The user's mail will now be retained for 45 days.

Example 4: A user is a member of the `VP` retention policy, which has a 365 day retention period. An administrator decreases the retention period for the `VP` policy to 90 days. The next day, the user's mail for days 91-365 is eligible for purging.

Capture-Based Policies

In a *capture-based* (or *time-of-capture*) policy, messages are retained based on the **user's group membership at the time the message was sent or received**. In capture-based policies, message retention is independent from the user's current role, and the policy governing retention does not change when the user changes group membership. This feature is useful if your organization is subject to regulations mandating the amount of time you must store email for employees in certain roles, such as accountants, sales representatives, or executives.

At the time a message is sent or received, it is associated with the specific capture-based policies that apply. Because these messages are stamped at time of capture, removal of a user from a group does not disassociate (or release) messages that have been associated with the policy. Alternatively, adding a user to a capture-based policy stamps all messages received after the user has been added, but does not retroactively stamp (or associate with the retention policy) messages previously received under a different capture-based or membership-based policy.

Example: A user is initially a member of the `Sales Group` retention policy, which has a 50 day retention period. The user then transfers to the `Assistant Group`, for which the retention period is 20 days. Mail captured prior to the transfer will still be retained for 50 days. Mail captured after the transfer will be retained for 20 days.

NOTE A Retention Grace Period Applies to User Changes

When users are removed from retention policies (whether manually by an administrator or because they have been marked deleted by the system), they are given a 30 day grace period before the policy no longer applies to them. This prevents messages from being immediately purged if a user is accidentally removed.

Be aware that the retention policy view will not show which users are pending removal during the 30 day grace period.

NOTE Storage Management Policies Have Higher Priority Than Retention Policies

If a message is stored under a storage management policy, it will not be purged even if it is eligible to be purged under a retention policy. See "[Storage Management](#)" on page 112.

User Classification Retention Policies

A *user classification* retention policy allows a defined group of users to determine which messages should be retained under the policy. For example, you can have a group, such as an accountants group, that identify all tax-related messages that should be included in a `Taxes` retention policy. Administrators can create custom folders within the users' Outlook Inboxes into which such messages are placed. Email Archive collects the messages from the named folder, and stores them for the amount of time defined in the policy.

Users assigned to these policies can refer to the *Email Archive User Guide* for instructions on using this feature.

To configure Manual Retention (User Classification) Task schedule settings:

- 1 Launch the VaultBox Console to configure User Classification retention schedule settings. To launch the VaultBox Console, from the Windows Start menu, select **Start > Programs > MessageLabs > VaultBox Console** on the machine on which it is installed. The VaultBox Console appears.
- 2 If **Start** is shown in this section, continue on to the next step. If **Stop** is shown, click **Stop** to halt Manual Retention Task processing.

3 Click **Edit Settings**.

- 4 In the **Manual Retention Settings** window, click squares in the day/time grid to indicate when the Harvester can scan Exchange for eligible messages. A blue square indicates scanning can take place during the hour; a white square indicates scanning is prohibited during that hour. You can click individual squares to change their status, or click days or hours to turn processing on or off for that entire day (row) or hour (column).

TIP Schedule Scanning During Off-hours

To limit the load on the Exchange server, schedule scanning during periods of lower user activity such as after business hours and on weekends.

When the message retention data has been collected, it is placed in a queue for archiving in the data center through the Transfer Service component. This data transfer continues until the queue is drained, regardless of the settings on this screen.

- 5 Set the delay between consecutive scans. This determines how long to wait after finishing a scan to start another one. The amount of time it takes to complete a scan of Exchange varies according to the amount of data to be analyzed and transferred. If the amount of scheduled time expires before a scan completes, the Harvester finds an appropriate stopping point and resumes scanning from that point during the next scheduled period. If scanning completes within the scheduled period, the Harvester waits for the amount of time configured in the **Delay between consecutive scans** field before starting another scanning cycle. Use the up/down arrows to set the amount of time to wait between consecutive scans during a scheduled scanning period.

- 6 Set the number of incremental scans between full scans. An incremental scan only checks messages created or modified since the last scan. Use the up/down arrows to set the number of incremental scans to be run until before performing a full scan.
- 7 Check **Do a full scan on the next run** if you want to run a full (rather than incremental) scan. This should be done if you have changed your retention policy, such as altering the period a retention policy covers.
- 8 Click **OK** to save the changed settings.
- 9 Click **Start** to restart Manual Retention Task processing with the new settings.

Retention Policy Best Practices

Retention policies should be carefully constructed and implemented so as to achieve your organizational objectives. The following best practices will help you avoid unintended consequences.

- **Determine your business requirements before setting up a retention policy.**

Retention policies should reflect your organization's overall records retention and compliance objectives. Before setting up any retention policies, determine what you are trying to achieve, under what constraints your organization works (such as financial, organizational, statutory), and rank the types of retention you want to achieve from most to least important. Planning for your needs in advance can save the time and frustration from having to change retention policies after implementation.

- **Historical Mail settings do not override Exchange settings.**

It is up to you to determine that your retention policies mesh smoothly with those on your Exchange server, and vice versa. For example, don't set your retention policy for 14 days when your Exchange server purges all messages after 30 days.

- **Higher priority policies always override lower priority policies, even when of shorter duration.**

Retention policies with a higher priority will always override those of a lower priority, even when the lower priority policy has a longer duration. For example, if an `Executive` retention policy specifies a retention duration of three years and is ranked higher than a `Legal` retention policy that specifies a retention of five years, then a CEO who was a member of both groups would only have his messages retained for three years.

- **Retention for user classification retention policies should be set no fewer than 30 days.**

To function properly, user classification policies must be set to retain mail for at least 30 days.

- **Set the default retention duration to at least 30 days.**

Make sure your retention policy is sufficient to achieve all organization objectives. Older messages can always be purged when necessary, but they cannot be reconstructed after purging if they are suddenly needed later.

- **Overlap durations for Email Archive and Storage Management policies.**

If you have both Email Archive and Storage Management (*stopping*) components, there should be at least one week duration overlap to ensure that no items set to be stopped will be deleted before stopping. For example, if Storage Management is set to start at 30 days, basic retention duration should be set to at least 37 days.

- **Avoid using membership-based policies, where possible.**

Membership-based policies are appropriate for retaining messages for continuity activations or for legal holds. They are not an adequate substitute for capture-based policies.

Creating Retention Policies

Retention policies allow you to store email for periods of time other than the 30-day default. To create a retention policy, you must:

- 1 Create a retention policy (give it a name and determine the number of days mail retained under this policy should be kept).
- 2 Decide the type: membership-based, capture-based, or a user-classified policy.
- 3 Decide who it applies to (determine its scope). The scope of the policy determines to which users the policy applies. The scope can be assigned based on lists, servers, and individuals. Group membership (based on lists or servers) is updated automatically when SyncManager is run.
- 4 Decide what should happen when users are deleted from the system: either keep their mail for the length of time set in the policy, or delete the mail.
- 5 Prioritize the policy. If a message is subject to more than one policy, the keep or delete decision is made based on the priority of the retention policy. You assign priority by rearranging the policies in the user interface, so that the most important ones appear higher in the list.

Then, at designated intervals, the system's purge function evaluates each message to determine:

- 1 Which policies apply to this email? Each message can be subject to multiple policies. If none of your organization's policies apply, then the 30 day default policy is used.
- 2 Is Email Continuity active for the user? Mail will not be purged during an activation. When the activation is over and the system returns to a Ready state, retention policies will be applied.
- 3 Is the message stored under a legal hold?
- 4 Is the message stored under a storage management policy?
- 5 Of the retention policies that apply to this email, which one is highest in the priority list?
- 6 Based on the highest priority policy, should this message be kept or marked eligible for purging?

Then the system marks the message as eligible to be purged, or allows it to remain in the archive.

WARNING Highest Priority Policy Takes Precedence over Duration Period

A policy's priority determines whether a message should be retained or purged. If a message is subject to a highest priority policy with a retention period of 90 days, as well as a lower priority policy with a retention period of 180 days, the message will be deleted after 90 days.

WARNING Changes to Policies are Recorded

Any changes you make to a policy are logged. To see a policy's history, click **Edit** and scroll to the **Change History** section at the bottom of the page.

Policy deletions are recorded in the data center. To obtain information about deleted retention policies, contact Support.

To create a retention policy:

- 1 From the Administration Console, click **Historical Mail**.
- 2 Click **Retention Policies**. The **Retention Policies** page displays.
- 3 Click **Create a new retention policy**. The **Retention Policies Details** page displays.
- 4 In the **Name** box, type a unique name for the new profile.
- 5 In the **Retain Mail for** box, type the number of days for the retention period.

- 6 Select the type of retention policy. Note that after you have selected a type, you cannot change it.

If you select a User Classification retention policy, choose a name for the folder that users will place the applicable mail into, and type it in the **Mail Folder** field. If you want to have this folder created automatically in users' Inboxes, click the **Automatically create this folder in user mailboxes** check box.

- 7 Click **Submit**. This returns you to the retention policy page. Note that it now includes information on the new policy. Repeat this process until you create all retention policies needed.

To add users to a retention policy:

- 1 Select a retention policy and click **Select Users**. The **Select Users** page appears.
- 2 Identify the users you want to add to the policy. You can locate and select users to add based on several criteria. For example:
 - a. To add all administrators to a retention policy, click the **User Sets** tab, select All Administrators, and click **Add**.
 - b. To add all users that are part of a specific mailing list or lists, click the **Mailing Lists** tab. Search for the correct mailing list or lists (you can use % as a wildcard). When search results display, select the ones you want and click **Add**.

NOTE Lists are Dynamically Updated

You don't have to manually add users to a list, or delete users when membership changes. The list is updated whenever the SyncManager runs, and whenever you change the policy.

NOTE Deletion of Distribution Lists Used in Retention Policies

If a distribution list used by a retention policy is deleted (that is, fails to sync to the data center during scheduled data transfer operations), the distribution list is scheduled to be purged after 30 days, and a fault alert notice is sent to each member of the fault alerts notifications list.

- c. To add all users with mailboxes on one or more email servers, click the **Servers** tab. Select the appropriate server listings and click **Add**.
 - d. To add users individually, click the **Users** tab. Search for the appropriate user or users. When search results display, select the one or ones you want and click **Add**.
- 3 Click **Add** to move the selected users to the **Add users to the profile:** field on the right.
 - 4 When you added all appropriate users to the retention policy, click **Next**. The **Confirm** page displays.

- 5 Examine the contents of the **Confirm** page, which lists all changes you are making to the retention policy. If the data is correct, click **Submit**.

To prioritize retention policies:

- 1 From the Administration Console, click **Historical Mail**.

WARNING Retention Policy Changes Go Into Effect Immediately Upon Saving

Reprioritize policies with care.

- 2 Click **Retention Policies**.
- 3 Click **Reorder/Reprioritize Retention Policies**. The user interface changes so that **DRAG** appears next to each retention policy.
- 4 Drag and drop a policy to a new location; the higher up in the list, the greater its priority.
- 5 When you're satisfied with the list, click **Save New Ordering**.

Q What happens to stored mail when a user is moved from one Exchange Organization or Administration Group to another?

- A The system allows you to associate the mail collected when a user was in one group and moves to another. The system detects a user ID conflict when more than one instance of an email address is captured in a sync. The conflict is reported, and can be resolved by Administrative action. After the conflict is resolved (that is, the multiple instances of the email address are determined to be the same user), mail stored with the first instance becomes associated with the second instance.

For more information about resolving user ID conflicts, see ["Resolving User ID Conflicts Automatically" on page 175](#) and ["Resolving User ID Conflicts Manually" on page 150](#).

Using Retention Policies to Implement Legal Holds

You can use the current membership policies to implement legal holds on mail for designated individuals. For example, if your organization needed to retain all email sent or received by two individuals in the organization, you would:

- 1 Create a current membership type retention policy with the maximum retention period (99999 days).
- 2 Include both individuals in the policy scope.
- 3 Grant the policy the highest priority (that is, move it to the top of the policy list).

No email governed by the policy will be purged by Email Archive, starting from the date the policy is implemented.

WARNING Exchange Membership Required for Legal Hold Policies

If you use a current membership policy to effect a legal hold, care must be taken never to remove the individuals covered by the policy from Active Directory, or their mail may be purged. Under membership policy, mail is only retained for users included in Exchange unless the **When users are deleted, keep them in the policy** option was enabled when creating the policy.

Query-Based Legal Holds

Email Archive Reviewers can create legal holds on collections of mail resulting from Archive Searches. These work similarly to retention policies, except:

- The Reviewer identifies the messages to be kept, and
- The messages are saved for an indefinite period of time, rather than a set number of days.

Legal Hold policies always have highest priority, because the messages in it are retained until an administrator removes the hold.

To remove a Legal Hold from a collection of messages:

- 1 From the Administration Console, click **Historical Mail**.
- 2 Click **Retention Policies**. The **Retention Policies** page displays.
- 3 Identify the Legal Hold policy, and click **Delete**. A confirmation box appears.
- 4 Click **Delete** to confirm.

Storage Management

To help reduce the size of Exchange mailboxes without using personal storage folders (PST) files, MessageLabs provides a storage management, or *stubbing* feature that collects large attachments from mailboxes, replaces them with HTML links, and moves them into storage. Administrators can set storage management policies based on the number of days the message has been in the user's mailbox, and according to the size of an attachment, allowing different thresholds for standard and inline attachments.

Creating Storage Management Policies

Storage management policies work independently from retention policies; a user's mail does not need to be subject to a retention policy in order to be subject to a storage management policy. Stored email will be searchable within the Email

Archive, however. Storage management policies also have a higher priority than retention policies; if a message has been stubbed it will not be purged, even if it should be purged according to a retention policy.

Storage management policies are set through the Administration Console. Before creating storage management policies, consider that:

- A minimum time period must elapse before a message can be stored; the default is 90 days. To change the minimum period, contact Support.
- You can apply storage management policies to all users, all administrators, defined mailing lists, servers, or individual users.

NOTE Deletion of Distribution Lists Used in Storage Management Policies

If a distribution list used by a storage management policy is deleted (that is, fails to sync to the data center during scheduled data transfer operations), the distribution list is scheduled to be purged after 30 days, and a fault alert notice is sent to each member of the fault alerts notifications list.

-
- You must have at least one VaultBox installed to implement storage management policies. You can implement multiple storage management policies for each VaultBox, but you can associate only one VaultBox with each storage management policy. If you want the same storage management policy in effect across your whole organization, you must create a separate, identical policy for each VaultBox. The VaultBox must have access to the Exchange server.
 - VaultBoxes used to support the Import Manager **cannot** be used in storage management policies.
 - On a periodic basis, a Harvester on the VaultBox searches the Exchange server for email attachments eligible to be stored. The Harvester coordinates transfer of the message to the data center, and replacement of the attachment with the HTML link by Exchange.
 - Note that Harvester cannot open a user's mailbox if it contains more than 500 folders (this is an Exchange limit). To ensure Harvester can process such mailboxes, users will need to consolidate folders down under the 500 folder limit.
 - A stored message will be removed from storage only when:
 - It is deleted from the server **OR** the user has been removed **AND**
 - There is no other retention policy that requires it to be kept
 - Using the command line interface, you can unstub all messages for a user who has been removed from all storage management policies. Contact Support for more information.
 - If more than one user has the same message, only one copy is stored in the archive.

- If an attachment has been archived to a PST file using the Outlook® storage function, Email Archive will not retain the attachment unless the email is subject to a retention policy. Any other process by which the user archives and deletes messages will only retain the stubs, and the original, consequently, will be deleted from the data center.
- The following message classes are eligible for storage management: IPM.Note and IPM.Note.MessageOneStubbed. Within these classes, the following attachment types are not eligible for storage management:
 - OLE attachments
 - Attachments made by reference (such as through the Sharepoint® system),
 - Calendar items
 - Contacts
 - Embedded messages
- For storage management purposes, inline attachments are defined as messages whose Content-Type field is `multipart/related`, when viewing the SMTP source of a message. These are often HTML images embedded in an HTML-formatted email.
- Windows Rights Management messages are not supported for Storage Management, because stubbing the encrypted attachment portion of the message makes the message unusable in Outlook and in Email Archive.

From an end-user's perspective, the storage management feature works slightly differently depending on how email is accessed—through Outlook®, the Outlook® Extension, or the webmail interface. For more information, please refer to the *User's Guide to Storage Management* or the online help provided with the Extension.

To create a storage management policy:

- 1 From the Administration Console click **Historical Mail**.
- 2 Click **Storage Management Policies**.
- 3 Click **Create a new storage management policy**.
- 4 In the **Storage Management Policy** section **Name** field, type a name for the storage management policy.
- 5 In the **Storage Management Criteria** section, enter age and size criteria as follows:
 - In the **If the message is older than:** field, enter the minimum number of days an email must be in the Inbox before it is eligible for storage management.
 - In the **If the attachment is larger than:** field, enter the minimum size an attachment must be to be eligible to be stubbed (default is 100K).

- In the **If the attachment is an inline attachment and larger than:** field, enter the minimum size an inline attachment must be to be eligible for storage management (default is 100K).
- 6 In the **VaultBox** section, select the appropriate VaultBox from the drop-down list.
 - 7 Click **OK**.

Like retention policies, storage management policies are also implemented according to their priority. A storage management policy's priority is determined by its place on the list in the user interface; higher priority policies appear at the top of the list. There must be two or more storage management policies in place for the Reorder/Reprioritize Policies option to appear.

To prioritize storage management policies:

- 1 From the Administration Console click **Historical Mail**.
- 2 Click **Storage Management Policies**.
- 3 Click **Reorder/Reprioritize Policies**. The user interface changes so that each retention policy is preceded by the word **DRAG**.
- 4 Drag and drop a policy to a new location; the higher up in the list, the greater its priority. Repeat until the policies are in the desired priority order.
- 5 When you're satisfied with the list, click **Save New Ordering**. To undo the new ordering, click **Revert**.

Configuring Scanning and Data Transfer from the VaultBox Console

To use the storage management feature, you must have at least one VaultBox installed. The VaultBox is responsible for coordinating the transfer of data from your organization's Exchange servers to the data center.

The VaultBox Harvester component communicates with the data center to determine storage management policy criteria. The Harvester scans the Exchange server looking for messages subject to storage management policies. The Harvester gathers the messages to be stubbed, and when the attachment

data has been collected, it is placed in a queue for transfer to the data center through the Transfer Service component. This data transfer continues until the queue is drained, regardless of the settings on this screen.

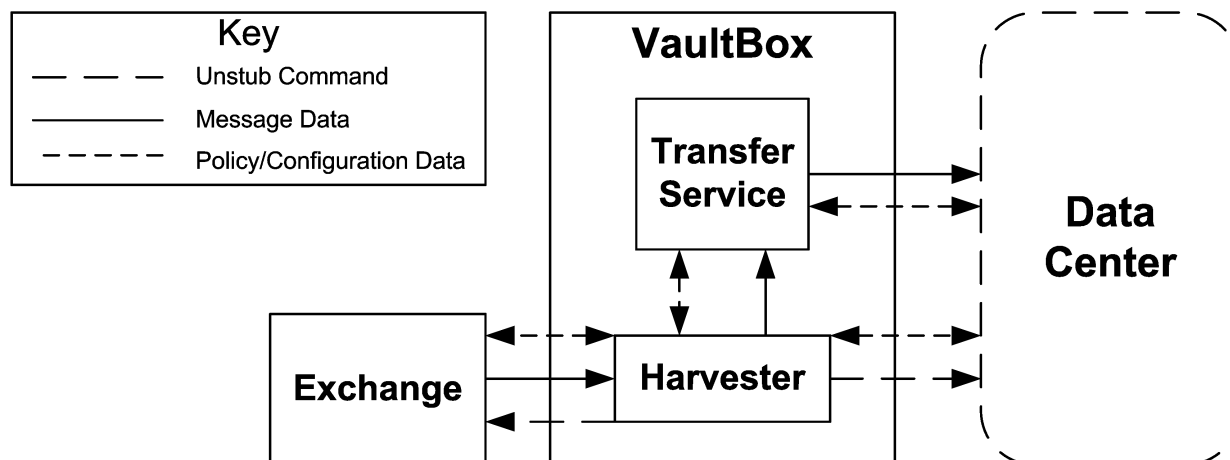


Figure 4-1 Data Transfer for Storage Management

You use the VaultBox Console to configure Exchange scanning and Transfer Service parameters. To launch the VaultBox Console, from the Windows Start menu select **Start > Programs > MessageLabs > VaultBox Console** on the machine on which it is installed. The VaultBox Console appears.

The Transfer Service Status fields display following parameters:

- **Queue**—The number of messages to be transferred to the data center
- **Rate**—The transfer speed, in messages/second and KB/second
- **Free Space**—The amount of space remaining on the VaultBox

To change data transfer settings for Storage Management:

- 1 In **VaultBox** section, click **Configuration**.
- 2 Click the **VaultBox** tab to display data transfer settings.

The **Outbound Bandwidth** section controls data transfer between the Transfer Service and the data center. In the **Number of connections** field, use the up/down arrows to alter the number of connections (threads) used by the process.

- 3 In the **Bandwidth Utilization** limit field, change the amount of bandwidth used for data transfer. (A setting of 0 in this field allows unlimited usage).
- 4 The **Free Space Margin** section prevents the storage management task from using excessive disk space. In the **Minimum available space** field, set the space threshold below which the storage management task should suspend activity.
- 5 Click **OK**.

To configure Storage Management parameters:

- 1 Open the **VaultBox Console**. Under **Storage Management Task**, if Storage Management processing is not running, **Start** will be shown and you can continue on to the next step.

If Storage Management processing is running, then **Stop** is shown. Click **Stop** to halt Storage Management Task processing.

- 2 Click **Edit Settings**. The **Message Storage Management Settings** screen appears.

- 3 On the graph, click squares in the day/time grid to indicate when the Harvester can scan Exchange for eligible messages. A blue square indicates scanning can take place during the hour; a white square indicates scanning is prohibited during that hour. You can click individual squares to change their status, or click days or hours to turn processing on or off for that entire day (row) or hour (column).

TIP Schedule Scanning During Off-hours

To limit the load on the Exchange server, schedule scanning during periods of lower user activity such as after business hours and on weekends.

- 4 In the **Delay between consecutive scans** field, use the up/down arrows to set the amount of time to wait between scans during a scheduled scanning period. The amount of time it takes to complete a scan of Exchange varies according to the amount of data to be analyzed and transferred. If the amount of scheduled time expires before a scan completes, the Harvester finds an appropriate stopping point and resumes scanning from that point during the next scheduled period. If scanning completes within the scheduled period, the Harvester waits for the amount of time configured in the **Delay between consecutive scans** field before starting another scanning cycle.

- 5 In the **Deleted message cleanup interval** field, use the up/down arrows to set the frequency at which the Harvester examines Exchange for deleted messages containing stubs. Periodically, the Harvester must resync with the Exchange server to make sure that changes are reflected in the data center. For example, an attachment may have been stubbed and stored in the data center according to a storage management policy. If the end user later deletes the message, the data center needs to be updated to reflect that the attachment no longer must be stored. This periodic synchronization is controlled by the **Deleted message cleanup interval**.
- 6 Storage Management does not typically collect messages that users have deleted. However, if you want Storage Management to consider messages in users' Deleted Items folders eligible for storage, click the **Apply Storage Management to Deleted Items** check box.
- 7 Click **OK** to save the new settings.
- 8 Click **Start** to restart the Storage Management Task with the new settings.

Harvester Operation and Data Logging

When the Harvester searches mailboxes for attachments that are eligible for storage management, it does so by dividing the analysis into segments of time, and looking at each mailbox for eligible attachments within that slice of time. For example, if your organization stores attachments older than six months, the Harvester would establish time slices such as 6-9 months old, 9-12 months old, or 12-15 months old. It would search all applicable mailboxes for eligible mail for the 6-9 month period, then search all mailboxes for the 9-12 month period, and so on. It would not look at a single mailbox for all eligible attachments from 6-15 months old at one time.

During a scanning task on an individual mailbox, the Harvester gathers up to 100 messages at a time, and processes these messages together. If the Harvester encounters an error when connecting to a mailbox, it pauses for five minutes, then reattempts to connect. If it fails four times, the Harvester moves on to the next mailbox, and the retry attempts are listed in the summary log as faults.

Harvester data is collected in a file called HarvesterAudit.log (located in C:\ by default). This log provides administrators with high-level information on the completion of Harvester tasks. It provides:

- **Storage activity per user, per time slice.**

If there were no attachments eligible for storage within the time slice, no data is logged. If a user had attachments eligible for storage in the time slice, the Harvester logs a message such as:

```
Stubbing scan of messages from 10/24/2005 9:50:21 PM to 1/22/2006 9:50:21 PM for user cn=test208,
cn=recipients,ou=first administrative group,o=acme demo
```

and test completed: stubbed 2 attachments (4.0 MB) in 2 messages; sent 2 messages to datacenter; 0 errors.

If the Harvester has to pause, then reconnect to the mailbox, the final log entry contains information about each of the interrupted attempts. Processing status definitions are provided in [Table 4-5](#).

- **Summary information for each run**

The Harvester processes each Storage Management policy separately. It logs messages recording the starting time and the name of the policy. If the task is interrupted (due to an error, or if the amount of allotted scanning time expires, for example), the Harvester resumes the task on the next restart. When the Harvester has finished processing all time slices, it generates the summary for the run. A sample summary looks like this:

```
Stubbing scan for storage management policy Admin completed
at 2:30:10 AM on 8/30/2007 Processed 10 of 10 mailboxes:
10 succeeded, 0 had faults. Stubbed 20 attachments (7.5
MB) in 20 messages; sent 20 messages to datacenter
```

The summary report also lists any errors encountered during processing.

- **User Summary Table in CSV, if enabled**

The Harvester can provide a per-user summary table, available in CSV format. To enable this report, you must edit the `HarvesterAudit.log4net.config` file and turn on debug level logging. This report can generate a large amount of data, so it is not recommended as a default setting. A sample of the CSV file looks like this:

```
User,Status,Messages Stubbed,Attachmens Stubbed,Stubbed
Attachment Size (bytes),Messages Imported,Errors
"cn=seight,cn=recipients,ou=first administrative
group,o=testcompanion",Completed,2,2,785741,0,0
"cn=sfive,cn=recipients,ou=first administrative
group,o=testcompanion",Completed,2,2,785741,0,0
```

Table 4-5 Harvester Status Definitions

State	Definition
Not Started	The mailbox has not yet been scanned by the Harvester.
In Progress	The mailbox is currently being scanned. This message appears when the task is interrupted—either because the allotted time expired, or there is no more space on the disk for sending messages to the data center.
Completed with Faults	Some messages from the mailbox have been processed, but the Harvester had to pause and restart at least once.
Completed	The mailbox was successfully examined for the time slice.
Failed	All attempts to connect to the mailbox failed; the mailbox was not scanned.

NOTE Log File Does Not Rotate

HarvesterAudit.log does not rotate like other log files. You can manually rotate the file whenever the storage management task is not running.

Removing (Unstubbing) Files for a User

You can remove (unstub) all messages for a user after the messages have been stubbed.

To unstub all messages for a user:

- 1 Log into the Administration Console.
- 2 Click **User Administration**, then click **Export**. The **Export User Information** page appears.
- 3 Export the User Information file.
 - a. Click the **Export** button. A **File Download** dialog box appears.
 - b. In the **File Download** dialog box, click **Save**. A **Save As** window appears.
 - c. Navigate to the location where you want to save the CSV file.
 - d. If desired, provide a custom name for the file, but do not change the file suffix or file type.
 - e. Click **Save**.
- 4 Within the CSV file, locate the user whose message you want to unstub. Note the **SystemID** value for that user.
- 5 Remove the user from the storage management policy. (Access the policy through the **Administration Console > Historical Mail > Storage Management**.)
- 6 Log into the VaultBox using the service account.
- 7 Open a command prompt and navigate to the ActiveMailbox directory (usually `C:\Program Files\MessageLabs\ActiveMailbox\`).
- 8 Run the following command, with quotation marks around the SystemID value you noted for the user from the CSV file.

```
Unstub "<SystemID>" -verbose
```
- 9 Check the log file (usually `C:\UnstubCmd.log`) for any messages indicating skipped files. Run the `unstub` command again if any skips are shown in the log file.

Storage Reports

The service reports on the amount of data stored in the archive under retention policies.

If storage management is installed, reports are provided for the amount of data stored under storage management policies.

NOTE Storage Usage Data

- 1 You may notice inconsistencies between the numbers in policy statistics reports versus the number of mailboxes synchronized. The inconsistencies will resolve after the statistics are recalculated.
 - 2 Because a message or attachment can be subject to multiple retention policies, there may be a discrepancy between the sum of all the policy data and the aggregate storage data. In these situations, the Aggregate Statistics entry reflects the correct value.
 - 3 The default policy (30 days) will cause a number of additional messages that are not held for an explicit policy to be visible in the totals. This occurs when users are deleted or removed from a membership-based policy
-

These reports are updated daily. The following information is provided.

Table 4-6 Storage Reports Data

Category	Field	Description
Retention Policies—General Information		
	Type	Category of retention policy. Only Current Membership is available for Historical Mail. <ul style="list-style-type: none"> • Membership-based • Capture-based • User Classification
	Policy Name	The name of the retention policy
	Retention	The length of time the messages governed by the policy are kept.
Retention Policies—Statistics		
	Users	The number of users included in the scope of the policy.
Storage Management Policies—General Information		
	Name	The name of the storage management policy
Storage Management Policies—Criteria		
	Minimum age	The minimum number of days a message must have been in a user's mailbox before it is eligible for storage management.
	Attachment size	The minimum size an attachment must be to be eligible for storage management.
	Inline content size	The minimum size an inline attachment must be to be eligible for storage management.

Table 4-6 Storage Reports Data (Continued)

Category	Field	Description
	VaultBox	The VaultBox to which the policy applies.
Storage Management Policies—Statistics		
	Users	The number of users to whom the policy applies.
	Messages	The number of messages affected by the policy.
	Total size	The amount of storage space consumed by messages under the policy.
	Aggregate Statistics	Cumulative storage statistics for retention policies and storage management policies

To view storage reports:

- 1 From the Administration Console, click **Historical Mail**.
- 2 Click **Storage Report**. The **Storage Report** screen appears.

Reviewer Groups

Archive Reviewers have the ability to search and read email in users' archives. You can designate any user as an archive reviewer. The individual does not have to have a personal email archive; that is, her personal user account does not need to be part of a retention policy. In most cases, you don't want to grant a reviewer unlimited access to your organization's historical email. Instead, you control the level of access by creating Reviewer Groups that define the email that is exposed to a designated set of reviewers. You can configure the Scoped Reviewer Group to include:

- The identities of the reviewers,
- The email accounts to be made available, and
- If desired, additional search criteria such as date and time ranges for the material provided.

For example, you could specify that reviewers John Doe and Jill Smith can view all email sent and received by the Sales group between September 1 and September 30, 2006.

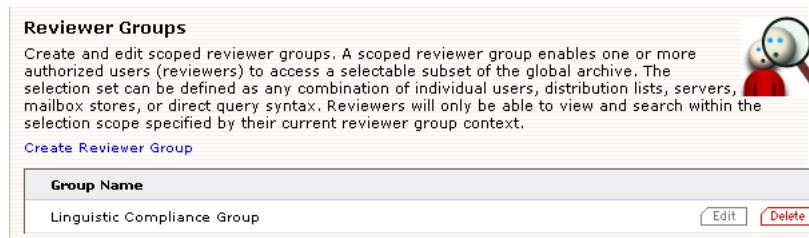
You also can make the queries very specific, such as all emails that include a particular term. To do this, you must use the same query language that is used to perform advanced searches in the archive. For more information, see ["Advanced Reviewer Searches" on page 124](#).

NOTE The Service Audits Creation and Management of Reviewer Groups

All actions taken by administrators regarding reviewer groups (adding them, editing them, changing the scope of data available to them) are included in the audit trail.

To create a reviewer group:

- 1 From the Administration Console, click **Historical Mail > Reviewer Groups**. The **Reviewer Groups** screen appears.



- 2 Click **Create Reviewer Group**. The **Reviewer Group Name** screen appears.
- 3 In the **Name** field, type a name for the group, and click **Next**. The **Scope** screen appears.

NOTE Reviewer Group Names Limited to 37 Characters

Reviewer Group names can be no longer than 37 characters. The system will not allow you to create groups with longer names, nor will it allow you to edit the names of existing groups to a name longer than 37 characters.

- 4 The scope of the group identifies the accounts made available for review. You can define the scope by User Sets, Mailing Lists, Servers or individual Users; click the appropriate tab to include accounts 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.
 - c. Click **Add**. Repeat until all are listed in the right section.

- 5 To limit the material available for review using additional criteria, click **Click to show/hide advanced options**.

▼ [Click to show/hide advanced options](#)

Specify a query expression to be used to constrain the scope of the selection criteria. An expert user may decide to define selection criteria only in terms of a query expression.

The more typical usage of this feature is to add some additional criteria in addition to the user scope selection. For example, it may be desirable to add a date range constraint to the review scope. This can be done by specifying the date query terms on this form.

Examples:

- ◆ Select only email with a date later than a specific time
emaildate: >2002-12-25T12:00:00
- ◆ Select only email within a given date range
emaildate: >2002-12-25T12:00:00 AND emaildate: <2003-12-25T12:00:00

Query Text:

- 6 In the **Query Text** box, define the criteria the material accessible to the reviewers. See ["Advanced Reviewer Searches" on page 124](#).
- 7 Click **Next**. The Reviewers screen appears.
- 8 You can select reviewers using mailing lists, or select individual users.
- 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. Click **Add**. Repeat until all are listed in the right section.

NOTE Mailing List Membership is Dynamic, not Static

If you select a mailing list, the list membership will be re-evaluated and, if necessary, changed based on the latest sync from the Active Directory environment.

- 9 Click **Next**.
- 10 A summary of the Scoped Review Group you have created appears. To enable the reviewer group, click **OK**. The newly created group appears in the list on the **Reviewer Groups** page. From the **Reviewer Groups** page you can edit review groups by clicking the **Edit** button adjacent to the Review Group's name. Similarly, you can delete review groups by clicking the **Delete** button.

Advanced Reviewer Searches

You can create complex reviewer scopes using an advanced search syntax. Use the fields described in [Table 4-7](#) to define searches:

- That use specific terms, such as "all messages that include the phrase, 'Quarterly Report.'"

- That use comparisons, such as “all messages sent between December 25 and August 1st,” or “all messages greater than 4 KB but less than 8 KB.”
- In which terms appear in proximity to other terms, such as “terms that appear within four words of each other” or “words that appear within four words of each other, in a specified order.”
- That use the Boolean operators AND, OR, and NOT to refine searches, such as “messages from bob@genericorp.com that are smaller than 4 KB.”

Table 4-7 Searchable Fields

Field	Description	Type	Format, If Specific
attachedfiles	A comma-separated list of all filenames.	String	
body	The content of the message.	String	
emaildate	Date specified in the Date portion of the message header.	Date	Date only: YYYY-MM-DD Date and time: YYYY-MM-DDThh:mm:ssZ You must use a 24-hour clock when specifying time. T is a required constant that identifies the following characters as times; Z is an optional UTC time-zone identifier.
envrecipients	The list of recipients contained in the message envelope.	String	
envsender	The sender contained in the message envelope	String	
filename	When searching for an attachment, (“isattachment” = 1) the filename of the attachment; otherwise, blank.	String	
isattachment	Indicates whether or not the document is an email attachment or a message (1 = attachment; 0 = message)	Integer	isattachment:1 isattachment:0
mailcc	Recipients listed in the Cc header of the message.	String	
mailfrom	Sender in the From header of the message.	String	
mailsubject	Subject of the message	String	
mailto	Recipients listed in the To header of the message.	String	
receivedate	Date message was received by your email server.	Date	

Table 4-7 Searchable Fields (Continued)

Field	Description	Type	Format, If Specific
recipients	Recipients listed in one or more of the following <ul style="list-style-type: none"> The list of recipient information contained in the message envelope The To header of the message. The Cc header of the message 	String	
senders	List of senders in the message envelope or the From header of the message.	String	
size	Size of document (message or attachment) in bytes.	Integer	Express sizes in bytes. For example, 4 KB as 4096
totalsize	Size of the message, in bytes, including all attachments.	Integer	Express sizes in bytes. For example, 4 KB as 4096

To build advanced searches:

- **To search for a term in any field**, type: `field:term` where `field` is one of the fields in [Table 4-7](#) and `term` is the value you want to find. To find a phrase, enclose it in double quotation marks. For example:
 - To find all messages sent from the email address `bob@genericcorp.com`, type: `mailfrom:bob@genericcorp.com`
 - To find all messages that include the phrase 'Quarterly Report' in the subject field, type: `mailsubject:"Quarterly Report"`
- **To search for mail using a range of dates or a range of sizes**, type `field:range (start, end)` where `field` is `emaildate`, `totalsize`, or `size`, and `range` defines the beginning and ending points of the search. For example:
 - To find all messages sent between December 25, 2003 and August 1, 2005, type `emaildate:range(2003-12-25, 2005-08-01)`
 - To find all messages with a total size that is at least 4 KB but no greater than 8 KB, type `totalsize:range(4096, 8192)`
- **To search for messages sent on or before a specific date, or that are less than or equal to a specific size**, type `field:range(min, value)`, where `field` is `emaildate`, `totalsize` or `size`, `min` declares the end value, and `value` is the date or minimum size. For example:
 - To find messages sent on or before December 25, 2003, type `emaildate:range(min, 2003-12-25)`
 - To find messages with a total size less than or equal to 4 KB, type `totalsize:range(min, 4096)`

- **To search for messages that fall on or after a specific date, or that are greater than or equal to a certain size**, type `field:range(value, max)` where `value` is the date or size, and `max` indicates that the value is starting date or size. For example:
 - To find messages sent on or after August 2, 2005, type `emaildate:range(2005-08-02, max)`
 - To find all messages with a total size greater than or equal to 4 KB, type `totalsize:range(4096, max)`
- **To search for words in proximity to each other, in any order**, type `near(arg, arg, n=numericValue)`, where `arg` is a word you want to find, (use as many as are required, following each by a comma), `n` is a constant that indicates the following `numericValue` is the proximity for the search.
 - To find the word “lunch” within five words of “Joe’s”, in any order, type `near(lunch, Joe’s, n=5)`
 - To find the words plane, bike, boat or car appearing within four words of each other, in any order, type `near(plane, bike, boat, car, n=4)`
- **To search for words in proximity to each other, in an exact order**, type `onear(arg, arg, n=numericValue)`, where `arg` is a word you want to find, (use as many as are required, following each by a comma) `n` is a constant that indicates the following `numericValue` is the proximity for the search.
 - To find the word “bank” within two words of “deposit”, in that order, type `onear(bank, deposit, n=2)`
 - For example, to find the words plane, bike, boat or car, in that order, within four words of each other, type `onear(plane, bike, boat, car, n=4)`
- **To combine search expressions using AND, OR and NOT** (Boolean operators), you can use AND and OR between terms, or use NOT as a prefix to find terms that do NOT match the specified criteria. For example:
 - To find messages from bob@genericcorp.com that are smaller than 4 KB in size, type `mailfrom:bob@genericcorp.com AND totalsize:range(4096, max)`
 - To find messages that include either the phrase “financial report” or the phrase “balance sheet” and were sent before December 25 2003 or after August 1st 2005, but not between those dates, type `NOT (emaildate:range(2003-12-25, 2005-08-01)) AND (“financial report” OR “balance sheet”)`

Search Limitations

The maximum message size that can be fully indexed in the data center archive is 50 MB. Message bodies or individual attachments that are larger than 50 MB are partially indexed using available header fields and metadata.

Q There is a message I think should be in the archive, but I am unable to find it there. Why can't I find it?

A A message may not be archived for one of the following reasons:

- The message never reached your inbound email server (for example, being quarantined for spam or security reasons).
- The recipient of the message is not covered by any retention policy.
- The date of the message falls outside the range of the retention policy covering the user.

Q I can find an archived message based on the title or date, but not by searching for words within the message content. Why can't I find these messages by content?

A There are certain categories of content that are archived and the header information indexed, but the content itself cannot be indexed. These categories include:

- XML files
- Media files (audio/video/image type)
- Non-standard binary files
- Password-protected ZIP files
- Message bodies or individual attachments that are larger than 50 MB
- Documents with corrupt or malformed content
- Documents with corrupt or invalid content-type information

These items can still be recovered.

Replication Zones

Replication Zones allow you to associate specific Exchange servers with a preferred series of VaultBoxes within your environment. For smaller environments, there may only be a single Replication Zone and all Exchange servers are members of this zone. Administrators of larger environments can create multiple zones to segment and load balance replication traffic to specific VaultBoxes. After Replication Zones have been created and all servers have been assigned to a zone, a corresponding DNS Forward Lookup Zone should be created in the environment for each Replication Zone defined within ESS. Within

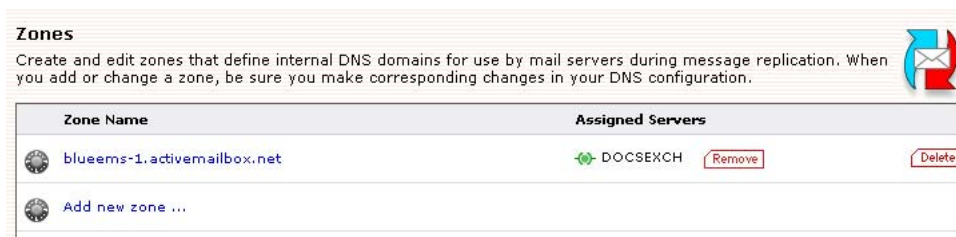
that Forward Lookup Zone, MX records should be created using the fully qualified domain name of the VaultBoxes using appropriate weighting of records to create the preferred routing topology.

NOTE Replication Zones Apply to Servers, not to Users

Replication Zone routing corresponds to the server that bifurcates the message (typically the first Exchange Server to touch a message), not the server on which a particular user resides.

To assign servers to replication zones:

- 1 From the Administration Console, select **Historical Mail**.
- 2 Click **Replication Zones**. The **Zones** page displays, containing a list of Exchange Servers.



- 3 Click **Add new zone...**
- 4 In the text box that displays:
 - a. Enter the name of the zone you want to add and click **Submit**. The newly added zone displays above the **Add new zone...** button.
 - b. In the bottom section of the **Zones** page, for each server you want added to the new zone, click the appropriate **Add to zone...** link.
- 5 Repeat for each zone, as needed.

Email Recovery Archives

Email Recovery Archives collect messages from the archive based on criteria you specify. Some sample definitions of Recovery Archives might include:

- All messages for user John Jones between January 1, 2006 and September 1, 2006.
- Mail for all users between the time of a last known good tape backup and a recent activation period.
- Mail for all users on the mailing list Sales between July 1, 2006 and August 1, 2006.
- Mail for all users on the Executive mailing list between a last known good tape backup and a recent activation period.

After you create an Email Recovery Archive, you can use the RecoveryManager to restore the messages in it to end users' mailboxes, or to a designated mailbox for review.

There are two kinds of Recovery Archives:

- **Time-based Recovery Archives** allow you to select start and end dates to create the archive.
- **Activation-based Recovery Archives** allow you to account for the time between your last known good backup, and an activation of Email Continuity. This type of recovery archive includes only messages for the users who were activated.

NOTE RecoveryManager Upgrade May Be Required

In order to use the Time-based and Activation-based Archives, you must be running the 6.0 or greater version of the RecoveryManager software.

To create a Time-based Recovery Archive:

- 1 From the Administration Console, click **Historical Mail**.
- 2 Click **Email Recovery**.
- 3 Click **Create a Time Based Recovery Archive**.
- 4 Type a name for the archive in the **Name** field.
- 5 In the **Include email from** field:
 - a. Select **click to edit** to use the calendar to define a start date.
 - b. Select **click to edit** to use the calendar to define an end date.
- 6 Click **Next**.
- 7 Identify the users whose messages must be collected in the archive. You can choose all users, or select by mailing list, by server, or individual user. Click the appropriate tab to select users for inclusion in the set 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 (using % for 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.
- 8 Click **Add**. Repeat until all are listed in the right section.
- 9 Click **Next**. A summary screen describing the Email Recovery Archive you've defined appears.
- 10 Click **OK**.

To create an Activation-based Recovery Archive:

- 1 From the Administration Console, click **Historical Mail**.
- 2 Click **Email Recovery**.
- 3 Click **Create an Activation-based Recovery Archive**.
- 4 Type a name for the Email Recovery Archive in the **Name** field
- 5 In the **Include email from** field:
 - a. Select **click to edit** to use the calendar to define a start date.
 - b. From the drop-down list, select an activation to serve as the end date for the archive.
- 6 Click **Next**.
- 7 Identify the users whose messages must be collected in the archive. In Activation-based Recovery Archives, only users who were part of the activation can be included. You can choose all these users, or select by mailing list, by server, or individual user. Click the appropriate tab to select users for inclusion in the set 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.
- 8 Click **Add**. Repeat until all are listed in the right section.
- 9 Click **Next**. A summary screen describing the Email Recovery Archive you've defined appears.
- 10 Click **OK**.

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.

NOTE Password Change Option Not Available for Customers with Windows Authentication

Because the Windows Authentication feature does not require separate Email Continuity passwords, this feature does not apply to organizations using Windows Authentication.

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.

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.
- If the user's mail is subject to retention policies, those policies are listed here.

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 133](#)
- ["Resetting Multiple Passwords By Template" on page 133](#)
- ["Resetting Multiple Passwords by CSV Import" on page 135](#)

Resetting an Individual User's Password

NOTE Password Change Option not Available for Customers with Windows Authentication

Because the Windows Authentication feature does not require separate Email Continuity passwords, this feature does not apply to organizations using Windows Authentication.

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.

WARNING Not for Use with Windows Authentication

This feature is not available if your organization uses the Windows Authentication feature.

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 4-8 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
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 135](#).

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 149](#). 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 data
- Click 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 4-9 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 4-10 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 143
Creating Help Desk Users	"Assigning Help Desk Privileges" on page 144
Changing the user attributes imported from Active Directory	"Changing User Attributes Imported from Active Directory" on page 172
Changing the Global Address List attributes displayed in the webmail interface	"Displaying Global Address List (GAL) Attributes" on page 173
Configuring email routing	"Configuring Email Routing" on page 173
Modifying the organization's email disclaimer	"Changing the Email Disclaimer" on page 175
Configuring automatic resolution of conflicting user IDs	"Resolving User ID Conflicts Automatically" on page 175
Setting user deletion notification thresholds for SyncManager	"Sync Notify Settings" on page 176
Customizing the Home Page	"Customizing the Home Page" on page 176
Customizing the Welcome Wizard	"Customizing the Welcome Process" on page 178
Changing the root account password	"Changing Your Password" on page 179
Installing RedirectorSinks using the RedirectorManager	"Configuring RedirectorManager" on page 57
Creating Reviewer Groups for Email Archive	"Reviewer Groups" on page 122

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 97](#) 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 158](#) 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 97](#) 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 141.](#)) 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 97](#) 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 97](#) 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.

NOTE Passwords with Windows Authentication

If Windows Authentication is installed, Help Desk Users cannot reset users' passwords.

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 97](#) 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 97](#) 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.



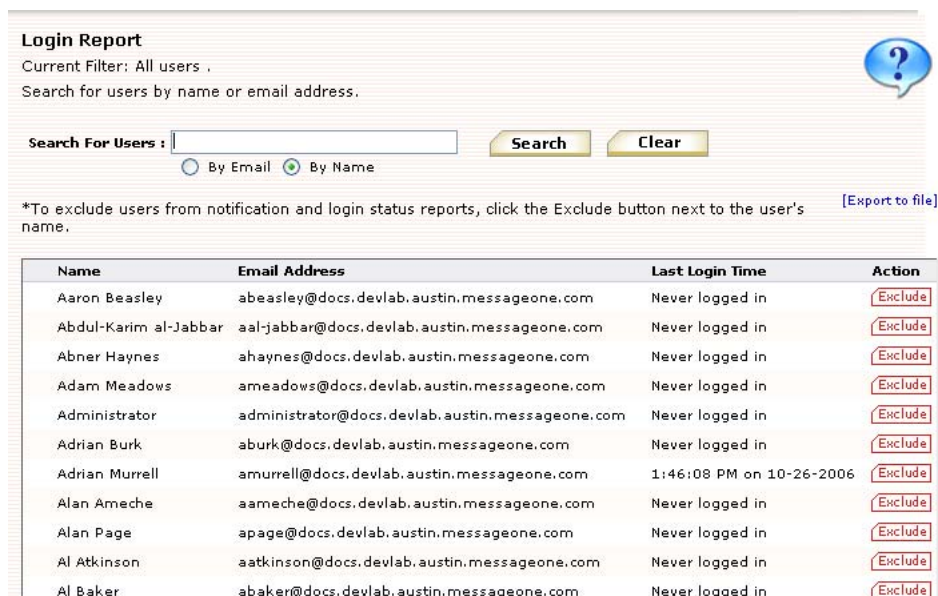
The screenshot shows the 'Login Status' screen. At the top, it says 'Login Status' and 'View reports on login activity. Please note that excluded users are not included in the summary counts or in the report views.' There is a help icon (question mark in a blue circle) to the right. Below this, there 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 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 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 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.

NOTE Login Status Includes webmail Login Only

If the Outlook® Extension has been installed, users may be using Outlook during the activation.

- 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 4-11, "Exported User Data"](#).

Note that the last data column (Custom Data) consists of custom user attributes synchronized from Active Directory, so the entries will be different for each organization. For more information on collecting custom attributes from Active Directory, see ["Changing User Attributes Imported from Active Directory" on page 172](#).

Table 4-11 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 4-11 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
Custom Data	Street Address
	Comment
	Company
	Fax Number
	Home Phone Number
	Cell Phone Number
	Phone Number
	Title
	Street Address
	Zip Code
	State
	City
	Last Name
	First Name
	Pager
	Country/Region
	Office
Department	

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 138](#).

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**.

Resolving User ID Conflicts Manually

During a Directory sync, the SyncManager looks for potential user ID conflicts using primary email addresses. When SyncManager encounters more than one instance of a primary email address, the system sends out a notification to persons on the fault notifications list, and adds the potential conflict to the list displayed on the **User ID Conflict Resolution** screen. In most cases, the instances of the primary email address refer to the same, single end user, and by resolving the conflict, you ensure that mail collected for the first instance is associated with the second instance. The system offers multiple ways to resolve such conflicts. Root-level administrators can configure the system to resolve them automatically using certain criteria (see ["Resolving User ID Conflicts Automatically" on page 175](#)) and Super Administrators and Email Continuity Administrators can resolve conflicts manually using the processes described here.

Q What if the conflict is genuine; that is, the same primary email address actually belongs to two different users?

- A** For example: You had a user Joe Smith (jsmith@organization.org) for whom you had retained mail. Joe Smith left the organization, but his mail was still subject to retention policies. A year later, you hired Jill Smith, and assigned the email address jsmith@organization.org. SyncManager would detect the conflict, but you would not want to resolve it using the methods described

here, as that would associate Joe's retained mail with Jill's new mail. Instead, you must assign a new primary email address to either Joe or to Jill.

To resolve multiple user ID conflicts using CSV upload:

If you are doing a planned migration of users, and anticipate many user ID conflicts, you can prepare a spreadsheet identifying the users and upload it to the system. When the spreadsheet is uploaded, the conflicts are resolved after the next Directory sync.

- 1 Prepare a CSV file in the format displayed in [Table 4-12](#)
- 2 From the Administration Console, click **User Administration**.
- 3 Click **User Conflicts**.
- 4 In the **Upload user resolution information** section, click **Browse**, then select the CSV file.
- 5 Click **Submit**.

NOTE Manual Directory Sync May Be Required

Changes uploaded by CSV go into effect after the next directory sync. You may want to perform a manual sync to have the changes take place as soon as possible.

Table 4-12 Sample Conflict Resolution CSV

Primary Email Address	New Exchange Legacy DN
suzy@lab104.organization.org	/o=E2K7-Lab104/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=suzy

To resolve user ID conflicts individually:

Each instance of duplicate primary address information encountered by the SyncManager is provided. For each instance in the list, you can determine whether the email addresses belong to the same user, and if so, resolve them.

- 1 In the **Resolving User ID Conflicts Individually** section, identify a user and, in the **Resolve User** column, click **Details**.
Both instances of the primary email address are provided, along with the Exchange Legacy DN value.
- 2 For the user, select one of the following:
 - I am unsure whether these are the same user. Keep these addresses in a conflict state until I find more information.
 - These addresses belong to the same user. Resolve the conflict, and store all mail together for this user in the system.

- These addresses belong to different users. The first instance will be deleted, and only mail for the second instance will be retained as of the next directory sync.
 - These addresses belong to different users. I must create a new primary email address for one of the users. Remove this conflict from the list, but do not create new directory information until the next sync.
- 3 Click **Submit**.
 - 4 If you chose to resolve the conflict, the user appears in the **Users Resolved** section. To delete the user from the list, click **Remove**.

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.

Wireless Continuity for BlackBerry Administration



After you have synchronized BlackBerry data to the data center, and distributed the client software to users' devices, you can use the Administration Console to manage the Wireless Continuity for BlackBerry feature. There is also a data logging interface installed on the handheld device as part of the agent. The agent-installed interface allows you to send diagnostic information to Support.

Managing Users and Devices

To manage BlackBerry user information in the Administration Console:

- 1 From the Administration Console, click **BlackBerry Administration**. The **BlackBerry Administration** page appears. For each device user, the page provides an overview of the account.
- 2 For more information, choose a device and click **Details**. The **Mailbox information** page appears. Data fields are described in [Table 4-13](#).

You can export device information for all BlackBerry users synced with your Email Continuity environment. The export process provides a comma-separated values (CSV) file and includes all information shown on the **Mailbox Information** page, except for Login History data.


- 3 If a device misses a device check-in interval or experiences other issues, the reset process pushes all contact information to the device. To reset a device, click **Reset**.

- 4 For any version 6.2 or higher agent listed on the **BlackBerry Device Information** page, you can send diagnostic information directly to Support by clicking the **Upload Diags** button displayed next to each version agent. This button does not display for version 6.1 and older agents.

Table 4-13 Mailbox Information Page

Field	Description
Name	The user name.
Email Address	The mail address associated with the device.
Server	The server associated with the device.
Mailbox Store	The mailbox store associated with the device.
State	The user's current continuity state: Active, Ready, or Recovery.
Last Login	The time the device last connected with the data center.
Outlook Extension Version	The Outlook Extension version the user has installed, if any.
Outlook Version	The Outlook version installed, if known.
BlackBerry PIN	The device PIN.
BlackBerry Enterprise Server	The BES to which the device is attached.
Email Continuity BlackBerry Agent Version	The version of the BlackBerry Continuity agent software installed on the device.
BlackBerry Handheld Software Version	The BlackBerry Handheld Software Version the user has installed, if known.
BlackBerry Platform Version	The firmware version on the device, if known.
BlackBerry Model	The model number of the user's BlackBerry device.
BlackBerry Carrier	The user's wireless service provider. This data can only be displayed when it is provided by the user's wireless service provider. Otherwise, this field is blank.
Phone Number	The phone number of the user's BlackBerry device. (Displayed only for device versions 6.2 and higher.)
Pending Signal Request	The last pending signal request for this user, if any. (Displayed only for device versions 6.2 and higher.)
Last Contact from BlackBerry	The time and date from the last contact with the device.
Login History	The time, status, and IP address from the last Login.

To view information about a device using the interface installed with the device agent:

- 1 The BlackBerry must be on and the agent must be installed.
- 2 Select the **Wireless Continuity for BlackBerry** icon  on the BlackBerry main menu.
- 3 Click the scroll button on the device. The agent message appears at the top of the screen.
- 4 Basic information about the device appears on the screen. This information includes:

- The state of the agent (Running or Stopped).
- The state of the device—Initial, if the agent is installed but has not been registered with the data center, then either Ready or Active, when Email Continuity is activated.
- Number of sent messages since the last activation.
- Number of received messages since the last activation.

Using Device Menu Options in Standard Display Mode

Access the menu options by clicking the scroll button. Menu options that appear on the Standard Display are:

Table 4-14 Standard Display Menu Options

Option	Description
Select	Provides access to Copy and Cancel Selection options.
Advanced Display	Provides the Advanced Display view, which provides more detailed information about the agent and the BlackBerry device.
Send Diags to Support	Sends a message to Support that contains a log file.
Stop Agent	Stops the agent.
Close Menu	Closes the pop-up menu of options and returns you to the agent display screen.
Close	Closes the agent interface and returns you to the BlackBerry main menu. (Applies only to agents version 6.1 and earlier.)

Using Device Menu Options in Advanced Display Mode

Access the menu options by clicking the scroll button. Menu options that appear on the Advanced Display are:

Table 4-15 Advanced Display Menu Options

Option	Description
Select	Provides access to Copy and Cancel Selection options.
Standard Display	Provides the Standard Display view.
Send Diags to Support	Sends a message to Support that contains a log file.
Stop Agent	Stops the agent.
Clear Statistics	Clears all statistics stored on this BlackBerry.
Copy Diagnostics	Copies diagnostic information so that you can email it. Preferred method is to use <i>Send Diags to Support</i> .
Normal/Verbose Logging	Toggles between normal logging and more detailed (verbose) logging. Verbose logging logs additional information for use by Support.

Table 4-15 Advanced Display Menu Options

Option	Description
Close menu	Closes the pop-up menu of options and returns you to the agent display screen.
Close	Closes the agent interface and returns you to the BlackBerry main menu.

Viewing Device Advanced Display Information

The Advanced Display shows read-only information about the agent and the BlackBerry on which it is running. When you are viewing the Advanced Display, the pop-up menu displays an option to return to the Standard Display.

Table 4-16 Advanced Display Read-only Information

Field	Description
Agent	Whether the agent is Running or Stopped.
State	Ready or Active.
Sent Email	The number of messages sent since the last activation.
Received Email	The number of messages received since the last activation.
Push Messages	The number of push messages received (push messages are sent from Email Continuity to the BlackBerry device).
Backend	The data center Email Continuity is running on.
PIN	The PIN number for this BlackBerry device
Agent version	The version of the agent running on this BlackBerry device.
JDE compatibility	The version of the Java Development Environment (JDE) with which this BlackBerry device is compatible.
Inbox	The inbox associated with this BlackBerry device.
BES	The address of the BES with which this BlackBerry device is associated.

Outlook® Extension Administration



The Outlook® Extension allows users to interface with various service features directly from their Outlook Inbox. (For information on how to use the features, refer to the online help provided with the Extension.) After the Outlook Extension has been enabled by Support, log into the Administration Console and click **Outlook Extension**. The **Outlook Client Information** screen appears.

The Outlook Client Information screen provides a list of users, and indicates whether they have installed the extension and polled the data center. You can search for a specific user, then click the **Details** button to display:

- The user's login history, including which versions of the extension and Outlook® are installed.
- A list of policies that apply to the user.

To enable or disable the Extension:

- 1 To disable an individual user so that the Extension cannot be used, click the **Disable** button adjacent to the user's name.
- 2 To enable or disable Outlook Extension features for all users:
 - a. On the **Outlook Client Information** screen, click **Manage Features**.
 - b. Use the check boxes to select features to activate; a check mark means the feature is active. Changes won't be effective until the user restarts Outlook.
 - c. Click **OK**.

To export the list of users:

- 1 Click **Export**. The **File Download** screen appears.
- 2 Select either:
 - **Open**, to open the file in Excel
 - **Save**, to save the file to your computer, or
 - **Cancel**
- 3 Click **OK**.

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 178](#).

- 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 138](#).

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)

NOTE %_tempPassword% and %autologinUrl% Not Applicable to Windows Authentication

Because separate Email Continuity passwords are not required for Windows Authentication customers, these variables are not included.

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.



<p>All welcome messages contain the individual's username, temporary password, and URL to access the service.</p> <p>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.</p> <p>Users who have not changed their temporary passwords, or who have not been sent a welcome message, do not yet have a permanent password.</p> <p>If a user does not provide notification information, the user cannot be contacted when the service is activated.</p> <p>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.</p>	<p>3 users have not received an initial welcome message. Show users ...</p> <ul style="list-style-type: none"> Welcome users who have not been sent an initial welcome message... Re-send welcome message to any user(s)... <p>All welcomed users have responded. Show users ...</p> <ul style="list-style-type: none"> Re-send welcome message to users who have not responded ... Send a welcome message to users who do not have a permanent password ... <p>All users that have completed the Welcome Wizard have configured their notification information. Show users ...</p> <ul style="list-style-type: none"> 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.

Reminders

By default, all reminder messages provide a link to the service website, the individual's username, and a link to the "forgot password" feature. You can customize the reminder message as you wish.



Remind users who have not responded to the welcome message by logging in and either providing notification information or stating they have no alternate means of notification.	▶ Send a reminder to welcomed users who have not responded ...
Remind users who stated they have no alternate means of notification. If notification information is not provided, the user cannot be contacted when the service is activated.	▶ Send a reminder to users who chose not to provide notification options ...
Remind users to keep their notification information up-to-date.	▶ Send a reminder to users to keep their notification information current ...

- 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 100](#));
- Distribution lists used in retention policies have been deleted (See ["Retention Policies" on page 103](#));
- Distribution lists used in storage management policies have been deleted (See ["Creating Storage Management Policies" on page 112](#));
- The percentage of users or mailing list members exceeds the configured threshold. (See ["Sync Notify Settings" on page 176](#))

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 167](#).

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 167](#)
- ["Test Reports" on page 168](#)

For auditing and tracking purposes, Email Archive maintains an audit trail for events that:

- Create or update a reviewer group
- Search the organization's email archive
- Generate an Email Archive recovery archive file

See the following sections for more information:

- ["Mail Searches Reports" on page 168](#)
- ["Reviewer Groups Reports" on page 169](#)
- ["User Classification Reports" on page 170](#)

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 145.](#))
 - 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.

Mail Searches Reports

The Mail Searches report includes information on searches of the organization's historical email. (Searches which users conduct of their personal email archives are not recorded or able to be audited.) The columns of the search history report provide the following information:

Table 4-17 Mail Searches Report Fields

Column	Description	Values
Event	The activity involved	Global mail search indicates any kind of search of the company email archive by a Reviewer Scoped mail search using reviewer group name—indicates a search performed by a scoped reviewer group participant. Building active recovery archive from search—indicates generation of a recovery archive.
Actor	Name and email address of the Reviewer who initiated the event	
Date	The time and date the event was initiated	<ul style="list-style-type: none"> • Time is shown using hh:mm:ss AM/PM format, based on a 12-hour clock and your time zone. • Date is shown in MM-DD-YYYY format.
Originating IP	The IP address of the system used for the event	

To run a Mail Searches report:

- 1 From the Administration Console navigation menu, click **Audit Reports**.
- 2 Click **Mail Searches**. The **Mail Searches Report** page appears.

TIP Narrowing Report Results

You can narrow the range of report results that appear by using the search interface at the top of the reports page.

- 3 To export the report to a CSV file, click **Export**. A **File Download** dialog box appears.
 - a. In the **File Download** dialog box, click **Save**. A **Save As** window appears.
 - b. Navigate to the location where you want to save the report file.
 - c. If desired, provide a custom name for the file, but do not change the file suffix or file type.
 - d. Click **Save**.

NOTE Response Time

Depending on the amount of data in the report, the export and save process may take a few minutes.

NOTE Export Content Unaffected by Search

All exports includes all report content. Any search you do when viewing the content does not limit the amount of information exported.

Reviewer Groups Reports

The Reviewer Groups report displays changes to Scoped Reviewer Groups and includes the following data.

Table 4-18 Reviewer Groups Reports Fields

Column	Description	Values
Event	Action taken	<ul style="list-style-type: none"> • For example, that a reviewer was removed or added. • A reviewer's email address was removed or added. • A View link; click this link to see a complete list of defined Scope Review Groups.
Actor	Name and email address of the person responsible for the event	

Table 4-18 Reviewer Groups Reports Fields

Column	Description	Values
Date	The time and date the event was initiated	<ul style="list-style-type: none"> Time is shown using hh:mm:ss AM/PM format, based on a 12-hour clock and your time zone. Date is shown in MM-DD-YYYY format.
Originating IP	The IP address of the system used for the event	

To run a Reviewer Groups Report:

- 1 From the Administration Console navigation menu, click **Audit Reports**.
- 2 Click **Reviewer Groups**. The **Reviewer Groups History Report** page appears.
- 3 By default, the report includes all activity from the past six months. If desired you can use the Search button to limit the alter the displayed report contents to include only certain users.
- 4 To export the report to a CSV file, click **Export**. A **File Download** dialog box appears.
 - a. In the **File Download** dialog box, click **Save**. A **Save As** window appears.
 - b. Navigate to the location where you want to save the report file.
 - c. If desired, provide a custom name for the file, but do not change the file suffix or file type.
 - d. Click **Save**.

User Classification Reports

User Classification Reports display lists of User Classification audited events. When you run a report, you can export the results to a CSV file.

To run a User Classification Report:

- 1 From the Administration Console navigation menu, click **Audit Reports**.

- Click **User Classification**. The **User Classification History Report** page appears.

User Classification History Report
View a list of the EMS User Classification audited events.
Use the *Export* button below to save this information to a file to document outage incidents or include in DR test plans and audit reports.

Search from: [03/09/08 01:54pm](#)
Search to: [09/09/08 01:54pm](#)

Search For Classified Messages:

By Actor Email
 By Actor Name
 By Policy
 By Smtip ID
 By Subject

Search **Clear**

Subject	SMTP ID	Policy	Actor	Audit Date
No audit events found.				

Prev | Next

Export

- To change the search dates or times, click the **Search from** or **Search to** links. Use the pop-up calendar to change the date and time.
- Enter the search data in the search field. You can use % as a wildcard for any search.
- Click a radio button to choose the type of search.
 - By Actor Email
 - By Actor Name
 - By Policy
 - By Smtip ID
 - By Subject
- Click **Search**. The report appears.
- To export the report to a CSV file, click **Export**. A **File Download** dialog box appears.
 - a. In the **File Download** dialog box, click **Save**. A **Save As** window appears.
 - b. Navigate to the location where you want to save the report file.
 - c. If desired, provide a custom name for the file, but do not change the file suffix or file type.
 - d. Click **Save**.

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.

Changing User Attributes Imported from Active Directory

Administrators using the root account can change which data fields are synchronized from Active Directory. Certain attributes are required; these are listed in [Table 4-19](#).

Table 4-19 Required Attributes

Attribute Name	Attribute Display Value
cn	Display Name
rdn	Display Name
mailnickname	User ID
displayName	Display Name
legacyexchangedn	Mailbox ID
mail	Email Address
proxyaddresses	Other Email Addresses
sAMAccountName	User Name
othermailbox	Other Mailbox
uid	User Id
distinguishedname	Not displayed in user interface
userAccountControl	Not displayed in user interface
msExchHideFromAddressLists	Not displayed in user interface
msExchMasterAccountSid	Not displayed in user interface

To change the attributes imported from Active Directory:

- 1 From the Administration Console, click **System Settings**.
- 2 Click **User Import**. The **Available User Attributes** screen appears.
- 3 To remove an attribute, so that it is not imported from Active Directory, select the attribute's check box and click **Remove**.
- 4 Active Directory contains many attributes, and your organization may also have custom attributes. Note that custom attributes imported by SyncManager are not available for use within Email Continuity, but can be used for integrated AlertFind applications. To add an attribute to the list that SyncManager captures:
 - a. In the search field, type the attribute's name.
 - b. Select the **By Display Name** or **By Attribute Name** radio button.
 - c. Click **Search**. Results appear in the section below.
 - d. Select the check box and click **Add**.

Displaying Global Address List (GAL) Attributes

During an activation, Global Address List attributes (synced from Active Directory) are displayed in the webmail interface. (To see them: from within the webmail interface, click **Contacts**. Select `Global Address List` in the drop-down list, then click a user in the **Display Name** column. The user's GAL attributes appear in the user's profile screen.) Administrators logged in under the root account can change the attributes that are displayed. There is a limited set of attributes available. You can only remove attributes from this list; you cannot add new attributes (such as custom attributes) to it.

To change the attributes displayed in Global Address List:

- 1 From the Administration Console, click **System Settings**.
- 2 Click **Address List Display**. The **Global Address List Display** screen appears.
- 3 To remove an attribute, so that it is not displayed in the Global Address List, select the attribute's check box and click **Remove**.

To restore an attribute that has been removed:

- 1 In the **Additional Properties** section, click the check box next to the attribute.
- 2 Click **Add**.

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 15](#), and ["Mail Routing—Outbound During Activation" on page 16](#). 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**.

Resolving User ID Conflicts Automatically

In some situations, such as when you are transitioning from Exchange 2003 to 2007, where only one Administrator category is permitted, SyncManager may detect high numbers of user ID conflicts. (See ["Configuring the SyncManager" on page 49](#) for more information.) You can choose to have administrators resolve conflicts manually, or you can configure the system to handle them automatically using various criteria. There are four separate options for resolving user ID conflicts:

- **Manual resolution.** This is the default setting, and requires that all user ID conflicts must be resolved manually by an Administrator. See ["Resolving User ID Conflicts Manually" on page 150](#) for more information.
- **Primary email address.** If the primary email address is the same, the users are determined to be the same person, and the conflict is resolved.
- **All Emails.** All aliases in the mailbox of first instance of the user ID are also present in the second instance of the user ID. The second instance can have additional aliases associated with it, but all of the first instance ones must be there. If only some or most are present, the action fails and an administrator must resolve the conflict manually.
- **Active Directory Attribute.** Choose a custom or default attribute from Active Directory to confirm that the users identified as having IDs in conflict are the same person. Examples are User ID, phone number, or cell phone number.

To configure the method by which user ID conflicts are resolved:

- 1 From the Administration Console, click **System Settings**.
- 2 Click **User ID Resolution**.
- 3 In the **User Resolution Type** field, select the resolution method from the drop-down list.

- 4 If you selected the `Active Directory Attribute` method, select the attribute from the **Active Directory Attribute** drop-down list.
- 5 Click **Submit**.

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 164](#).

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 4-20](#).

Table 4-20 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.

Table 4-20 Home Page Preferences Links

Link Name (Administration Console)	Link Name (displayed on Home Page)	Function
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 2.](#))

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 160](#).

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 165](#).) 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@genericcorp.com could receive email through the webmail interface through the email address aandrews@genericcorp.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.

If the Outlook® Extension has been deployed, end users can choose to continue to send and receive their email using Outlook. See the online help provided with the extension for more information. To compare Email Continuity webmail features with Outlook Extension features, see ["About the Outlook Extension" on page 7](#).

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 white background, containing the word "Activate" in 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.

If your implementation includes the partial activation feature, the **Selecting the Scope of the Activation** page displays.

- 4 To activate your whole environment, select `Activate` for the Whole Email Environment. To activate for a subset of users, select `Activate Email Continuity` for a subset of users, and choose the users to activate:
 - a. To select one or more predefined User Sets.
 - (1) Click the **User Sets** tab.
 - (2) Select a set and click **Add**.
 - (3) Repeat until all the sets you want appear in the **Activate** list.
 - b. To select one or more servers or server groups:
 - (1) Click the **Servers** tab.
 - (2) Select a server or server group and click **Add**.
 - (3) Repeat until all the servers and groups you want appear in the **Activate** list.
 - c. To select one or more users:
 - (1) Click the **Users** tab. The list of available users displays as empty.
 - (2) In the **Search** box, type a name or email address, (or part of the name or address plus % as a wildcard) and click **Search**. All users that meet the entered search criteria appear.
 - (3) Select a user and click **Add**.
 - (4) Repeat until all the users you want appear in the **Activate** list.
 - d. Click **Next**.

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.

- 5 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.
- Use contact information, but not edit or add new contacts.

Note that the size of a message when it is displayed in webmail may be different from the message's displayed size when it is recovered. This is because webmail and Outlook use different storage formats, which calculate message size differently.

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

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

7 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 187](#)
- ["Restoring Mail to Users' Mailboxes" on page 189](#)
- ["Completing Recovery from an Activation" on page 200](#)

Discovery Archives contain messages bundled into archives using various features of Email Archive. These include search-based archives and time-based archives. Depending on the type of archive you are recovering, you may choose to recover messages into a single mailbox or into multiple users' mailboxes. See ["Recovering Mail from Discovery Archives" on page 201](#) for more information.

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.

For partial activations, recovery can be done on a server-by-server, group-by-group, or mailbox-by-mailbox basis.

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.

- 3 If you want to recover your entire environment, select **Start Recovery for All Users**. Otherwise, select **Start recovery for some users**, leave others in the **Active** state, and identify the users to recover, as follows:
 - a. Select the appropriate tab (**User Sets**, **Mailing Lists**, **Servers**, or **Users**), and select an item on the list.
 - b. Click **Add**. The selected item moves to the **Start recovery for these users** list.
 - c. Repeat until all the users you want to recover appear in the list.
 - d. Click **Next**.

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.

- 4 Click **Next**. The message composition page containing the default message displays.
- 5 Edit the **Subject** or **Text** of the message as needed.
- 6 Click **Next**. The **Confirmation** page displays.
- 7 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.

- 8 In the **Archive Name** box, type a name for the archive file (for example, `Archive_10_12_06`).
- 9 Click **Next**. The Administration Console displays a summary of all recovery steps to be taken.
- 10 Review the recovery steps summary.
- 11 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, or to restore the contents of a recovery archive. If you are recovering from an activation, make sure you have created a recovery archive (during the initial recovery process) before launching the RecoveryManager.

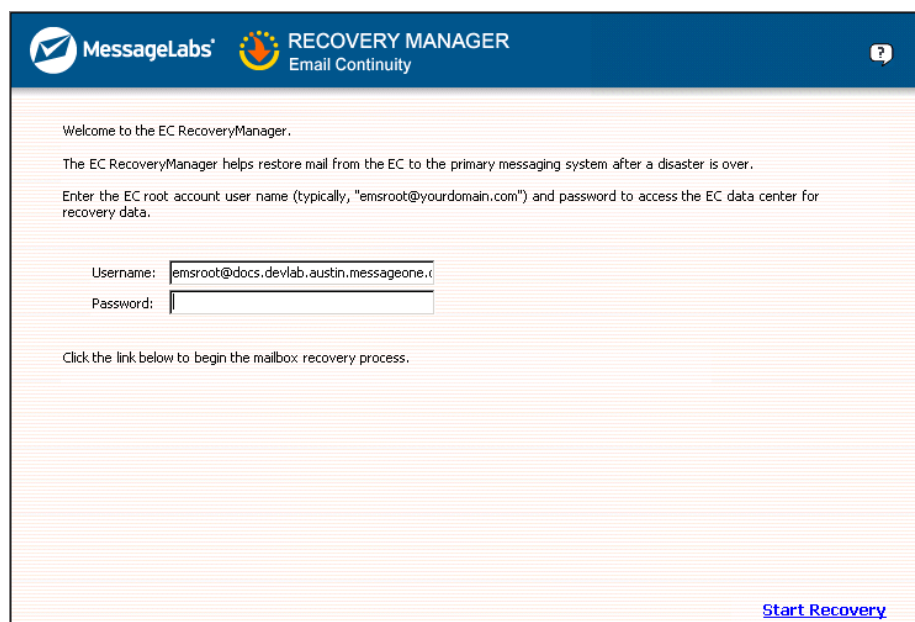
NOTE Recovery and Blackberry Devices

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 recover email from an activation or from a recovery archive:

- 1 On the ESS server, from the Windows Start menu select **Programs > MessageLabs > RecoveryManager**.



MessageLabs RECOVERY MANAGER
Email Continuity

Welcome to the EC RecoveryManager.

The EC RecoveryManager helps restore mail from the EC to the primary messaging system after a disaster is over.

Enter the EC root account user name (typically, "emsroot@yourdomain.com") and password to access the EC data center for recovery data.

Username:

Password:

Click the link below to begin the mailbox recovery process.

[Start Recovery](#)

- 2 Log in to 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:

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 Either:
 - Select the **Activation Recovery** radio button if you are recovering from a typical activation of Email Continuity, or
 - Select the **Active Recovery** radio button if you are recovering mail from a Discovery archive, Time-based recovery archive, or Activation-based recovery archive.

NOTE Activation Recovery vs. Active Recovery

If you have no Discovery, Time-based, or Activation-based recovery archives to recover, you will receive an error message. Choose **Activation Recovery** instead.

6 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.

MessageLabs RECOVERY MANAGER
Email Continuity

Enter information about your mail system.

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: Exchange 2000/2003/2007

Directory Settings

Global Catalog Server:
docsdc.docs.devlab.austin.messageone.com

Advanced ...

Mailbox Access Settings

EC needs a MAPI profile to logon to Exchange. This profile is only used to open the Exchange store. If the profile doesn't exist it will be created.

MAPI Profile:
EC MessageLabs

Edit ... Delete

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](#)

7 Configure mail settings. Information displayed here reflects settings from the SyncManager. Any changes made here affect the SyncManager, if it runs on the same server. Typically, these settings are not changed during recovery.

For Exchange 2000/2003/2007 platforms:

- a. From the **Platform** drop-down list, select Exchange 2000/2003/2007.
- b. In the **Directory Settings Global Catalog Server** box, select or enter the name of the global catalog server
- c. For **Mailbox Access Settings**, select a MAPI profile from the drop-down list.
- d. During a typical recovery, directory information is compiled as part of the process, which can be a time-consuming step in large environments. 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.
- e. Click **Continue**.

For Exchange 5.5 platforms:

- a. From the **Platform** drop-down list, select Exchange 5.5.
- b. In the **Directory Settings** box, enter the name of the Exchange server.

- c. For **Mailbox Access Settings**, select a MAPI profile from the drop-down list.
- d. 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.
- e. Click **Continue**.

NOTE Advanced Settings

- **LDAP Port**—The default port is 389. If the server listens on another port, change this to the port the server uses. If Exchange 5.5 is installed on a Windows 2000/2003 global catalog server, this setting must be changed; Exchange 5.5 traditionally runs on port 389 so, by default, the LDAP port will be different.
 - **LDAP Max Results**—Exchange 5.5 has a default setting of 100 results returned, but Exchange 2000 has a default setting of 1000 results returned. If this value has been changed on the Exchange server, change the value here to correspond.
-

- 8 Email Continuity analyzes the 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**.

MessageLabs RECOVERY MANAGER
Email Continuity

EC RecoveryManager is ready to recover mail from the recovery archive into your mail system. The Recovery Progress box on the left shows the statistics of recovered users. You can import all users at once, or a subset of users based on server or mailing list, or you can manually select users. If there's mail in the EC Dropbox, the link to import dropbox will be active.

Recovery Progress	
Mailboxes in Archive:	1089
Recovered:	0
User Status ... View Log	

Analysis Results	
Matched to a user:	1089
Unmatched mailboxes:	0
Analyze Again	

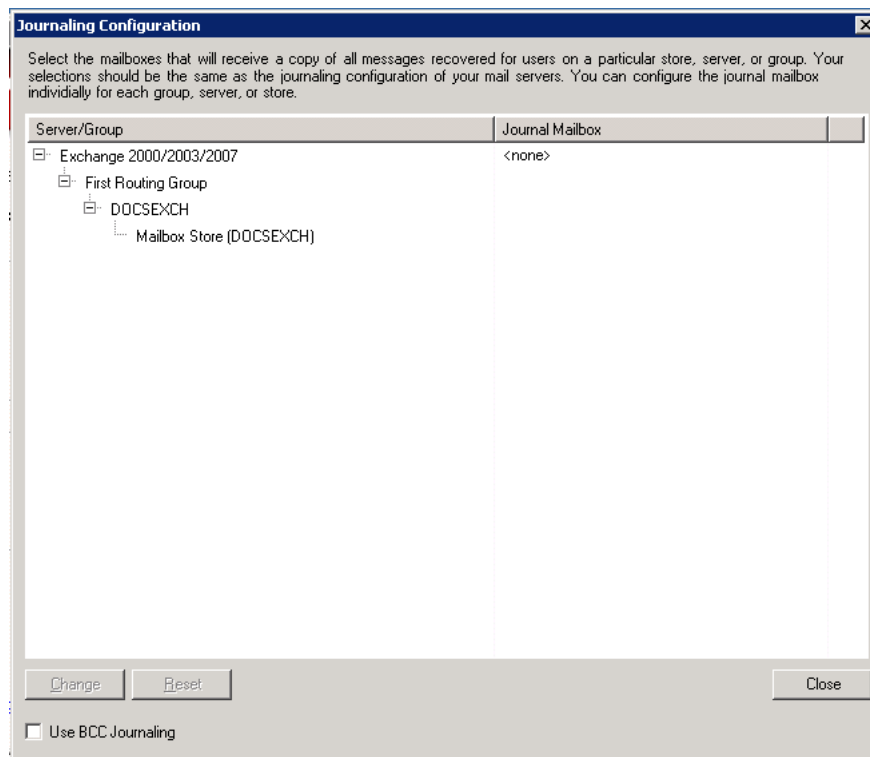
- [All Users](#)
Recover all users with mail in their EC mailboxes
- [Users on Specific Server](#)
Select users to recover by routing group, server, or store
- [One or More Select Users](#)
Pick individual users to recover
- [Group of Users](#)
Select users to recover by mailing list membership
- [EC Dropbox](#)

[Configure Journaling ...](#) [Return to Recovery Archive List](#)

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.
- 9 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**.

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.

10 Select the set of users for recovery from the right column.

- **All Users**—The All Users option imports email data for all users who were activated during the outage, used the 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 server groups for recovery. (Servers without users that need recovery 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**.
 - (3) When you finish adding users to the list for recovery, click **Continue**.

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 and 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.

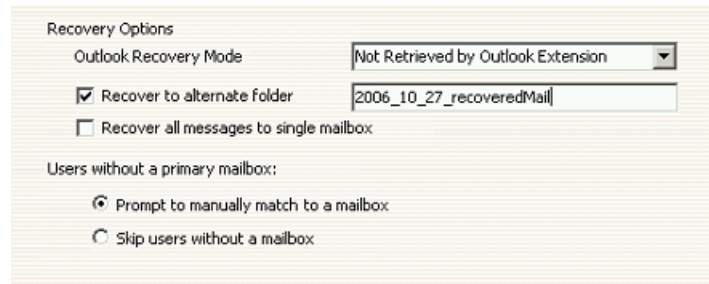
- **Group of Users**—The Group of Users option recovers users based on Exchange distribution list membership. When selected, the display lists all distribution lists with members who have email that needs recovery. If you select this option:
 - (1) Select a group of users and then click **Add**.
 - (2) Click **Continue**.
- **Email Continuity Drop Box**—The Email Continuity 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 which 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.

- 11 Identify the mail to recover from the **Outlook Recovery Mode** drop-down list:
 - a. Choose `Not Retrieved by Outlook Extension` to recover only email processed by the webmail interface.
 - b. Choose `Retrieved by Outlook Extension` to recover only email processed by the Extension.
 - c. Choose `All messages` to recover email from both the Extension and webmail.

12 Choose how to restore the mail.

- a. To recover all mail from the activation to a designated folder within users' mailboxes, click the **Recover to alternate folder** check box and type a name for the folder in the field.



Recovery Options

Outlook Recovery Mode: Not Retrieved by Outlook Extension

Recover to alternate folder: 2006_10_27_recoveredMail

Recover all messages to single mailbox

Users without a primary mailbox:

Prompt to manually match to a mailbox

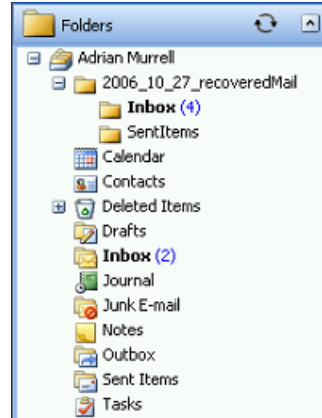
Skip users without a mailbox

NOTE Recovering Discovery Archives

The **Recover to alternate folder** option is the only available option for Discovery archives.

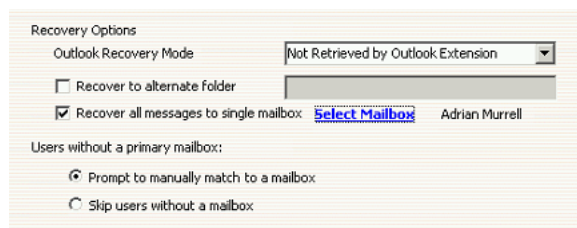
To import a Discovery archive, you can also leave both the **Recover to alternate folder** and the **Recover all messages to single mailbox** options unchecked. This will import the messages into a folder labeled with the reviewer's user name with subfolders **Inbox** and **Sent Items**.

After Recovery is completed, messages will appear in users' mailboxes like this:

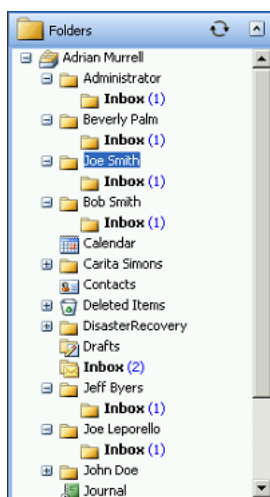


For Discovery archives, the messages are imported into the folder you specified, with a subfolder labeled with the user name of the user who created the archive, with additional subfolders **Inbox** and **Sent Items**.

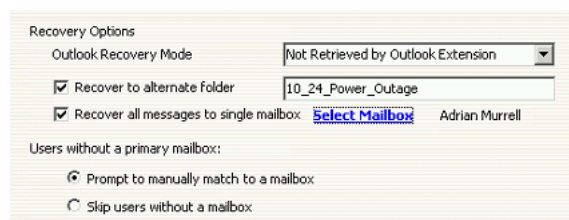
- b. To recover all messages from the activation to a single mailbox (such as an administrator mailbox, for troubleshooting purposes), click **Recover all messages to single mailbox** and, in the dialog that appears, select the mailbox.



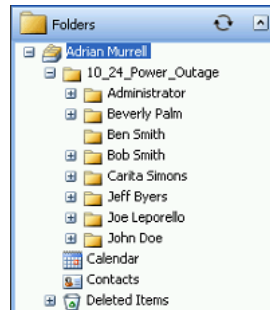
After Recovery is completed, messages will appear in the designated mailbox like this:



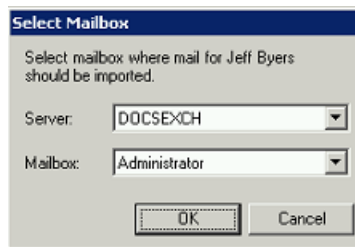
- c. To recover all messages to a single mailbox but place them in a designated folder, complete both the **Recover to alternate folder** and **Recover all messages to single mailbox** options.



After Recovery is completed, messages will appear in the designated mailbox like this:



- 13** 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** to reroute unmatched mailboxes later.
- 14** Click **Start Recovery** to begin importing data for selected users.
- 15** The RecoveryManager downloads email data from the ESS 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**.
- 16** When the mail for all selected users has completed recovery, click **Continue**.
- 17** 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 is only imported once; the RecoveryManager skips already recovered user accounts, even if they are members of other 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.

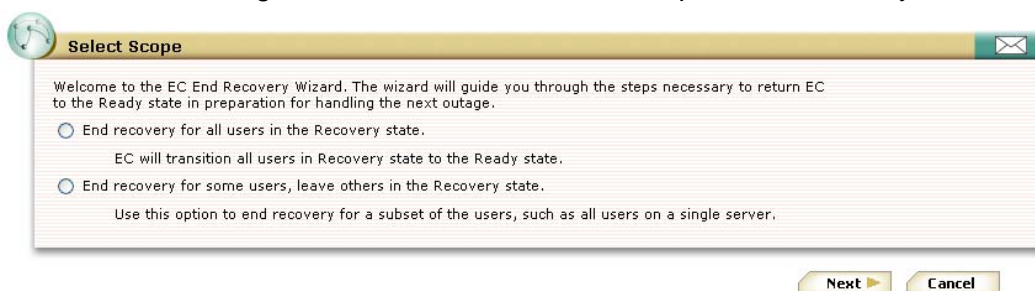
Ending recovery permanently deletes activation email data from the webmail interface. Ensure that all email data is successfully imported into the primary mail system before completing this process. All recovery archives can be downloaded for a period of 30 days after initial creation; however, after 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 rectangular button with a green border and the text "End Recovery" in black.

- 2 Using the radio button, select the scope of the recovery. Click **Next**.

A dialog box titled "Select Scope" with a globe icon on the left and a close button on the right. The text inside reads: "Welcome to the EC End Recovery Wizard. The wizard will guide you through the steps necessary to return EC to the Ready state in preparation for handling the next outage." Below this are two radio button options: "End recovery for all users in the Recovery state." (with subtext "EC will transition all users in Recovery state to the Ready state.") and "End recovery for some users, leave others in the Recovery state." (with subtext "Use this option to end recovery for a subset of the users, such as all users on a single server."). At the bottom right are "Next" and "Cancel" buttons.

Select Scope

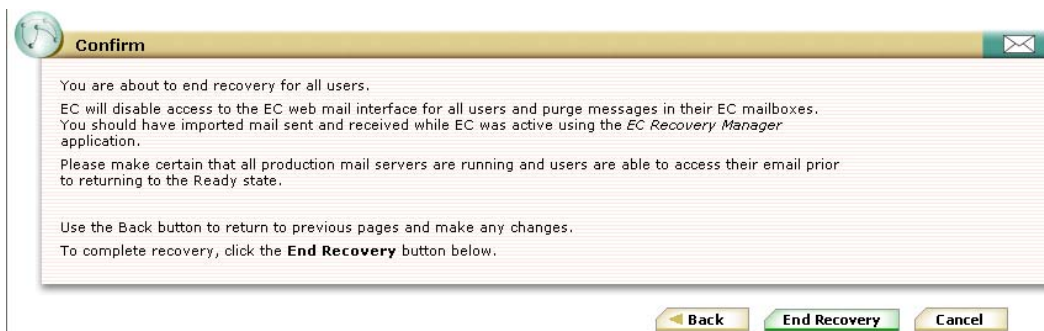
Welcome to the EC End Recovery Wizard. The wizard will guide you through the steps necessary to return EC to the Ready state in preparation for handling the next outage.

End recovery for all users in the Recovery state.
EC will transition all users in Recovery state to the Ready state.

End recovery for some users, leave others in the Recovery state.
Use this option to end recovery for a subset of the users, such as all users on a single server.

Next **Cancel**

- 3 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.

A dialog box titled "Confirm" with a globe icon on the left and a close button on the right. The text inside reads: "You are about to end recovery for all users. EC will disable access to the EC web mail interface for all users and purge messages in their EC mailboxes. You should have imported mail sent and received while EC was active using the EC Recovery Manager application. Please make certain that all production mail servers are running and users are able to access their email prior to returning to the Ready state. Use the Back button to return to previous pages and make any changes. To complete recovery, click the End Recovery button below." At the bottom are "Back", "End Recovery", and "Cancel" buttons.

Confirm

You are about to end recovery for all users.
EC will disable access to the EC web mail interface for all users and purge messages in their EC mailboxes. You should have imported mail sent and received while EC was active using the *EC Recovery Manager* application.
Please make certain that all production mail servers are running and users are able to access their email prior to returning to the Ready state.
Use the Back button to return to previous pages and make any changes.
To complete recovery, click the **End Recovery** button below.

Back **End Recovery** **Cancel**

Recovering Mail from Discovery Archives

Email Archive Reviewers create Discovery Archives containing messages found during Archive searches. Email Archive Administrators use the RecoveryManager to deliver Discovery Archive contents to a designated mailbox so that it can be examined by appropriate personnel. For more information on creating a Discovery Archive, see the *Email Archive Reviewer Guide*.

To recover a Discovery Archive:

- 1 From the ESS server, select **Start > Programs > MessageLabs > RecoveryManager**.
- 2 Log in to RecoveryManager.
- 3 Click **Start Recovery**.
- 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 box. (If a profile doesn't exist, one will be created in the next step of the process.)
- 5 Select the **Active Recovery** radio button.
- 6 Click the appropriate archive from the list and click **Continue**. This downloads metadata about the recovery archive into the working directory.

When configuring these mail settings, you provide information that allows the RecoveryManager to access the primary mail system. Information that displays here reflects settings from the SyncManager component. Any changes you make here affect the SyncManager component, if it runs on the same server. Typically, these settings are not changed as part of recovery.

For Exchange 2000/2003/2007 platforms:

- a. From the **Platform** drop-down list, select Exchange 2000/2003/2007.
- b. In the **Directory Settings Global Catalog Server** box, select or enter the name of the global catalog server
- c. For **Mailbox Access Settings**, select a MAPI profile from the drop-down list.
- d. 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.

e. Click **Continue**.

For Exchange 5.5 platforms:

- a. From the **Platform** drop-down list, select Exchange 5.5.
- b. In the **Directory Settings** box, enter the name of the Exchange server.
- c. For **Mailbox Access Settings**, select a MAPI profile from the drop-down list.
- d. 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.
- e. Click **Continue**.

NOTE Advanced Settings

- **LDAP Port**—The default port is 389. If the server listens on another port, change this to correspond to the port the server uses. If Exchange 5.5 is installed on a Windows 2000/2003 global catalog server, this setting must be changed; Exchange 5.5 traditionally runs on port 389 so, by default, the LDAP port will be different.
- **LDAP Max Results**—Exchange 5.5 has a default setting of 100 results returned, but Exchange 2000 has a default setting of 1000 results returned. If this value has been changed on the Exchange server, change the value here to correspond.

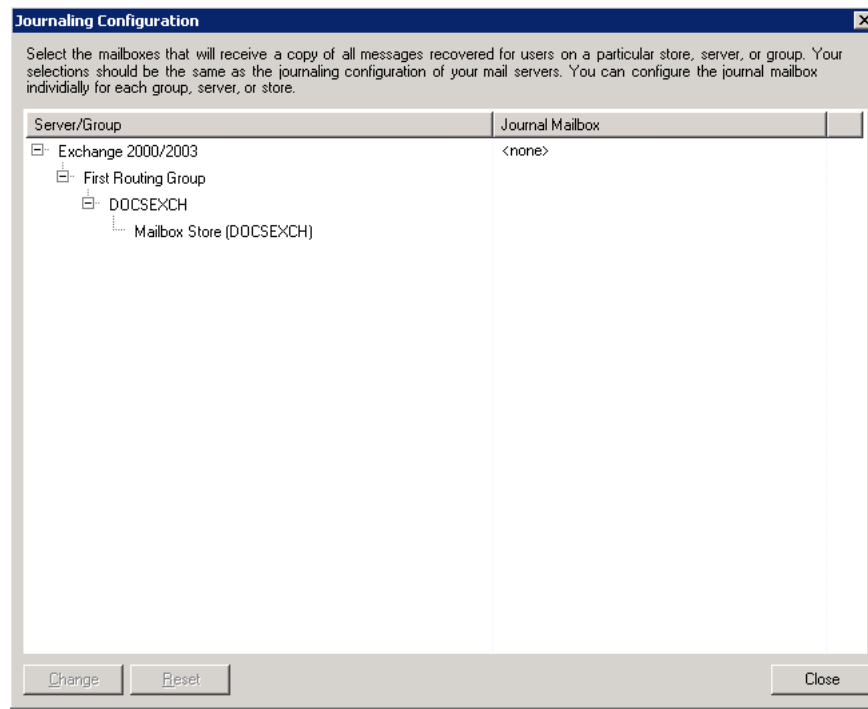
Email Continuity analyzes the recovery archive to match up mailboxes in the archive to users' mailboxes in the primary mail system. This process can take several minutes. When it completes, click **Continue**.

The main RecoveryManager page controls how the archive is recovered. Status indicators display in the left column of the page.

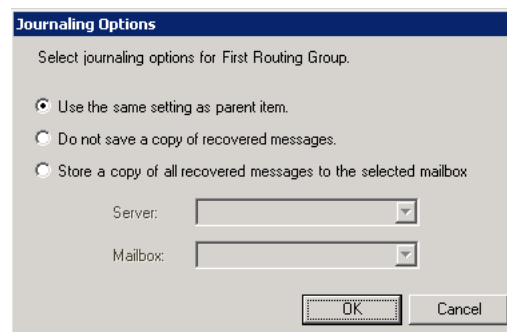
- **Mailboxes in Archive**—The total number of mailboxes in the archive.
- **Recovered**—The number of mailboxes for which mail has been recovered.
- **Matched to a user**—Displays how many user account can and cannot be matched to an account on the primary mail system. This also provides an option for reanalysis of the archive.
- **Unmatched mailboxes**—The number of mailboxes that cannot be associated with a user in the primary mail system.

- 7 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. Highlight the group, server or store you want to configure.
- c. Click **Change**.



- d. 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.
- e. Click **OK**.

- 8 Click **Discovery Archive**.

- 9 From the **Server** drop-down list, select the server for the Discovery Archive.
- 10 From the **Mailbox** drop-down list, select a user's mailbox for the Discovery Archive.
- 11 Click **Continue**.
- 12 Choose how to restore the mail.
 - a. To recover all mail to a designated folder within users' mailboxes, click the **Recover to alternate folder** check box and type a name for the folder in the field.

The messages are imported into the folder you specified, with a subfolder labeled with the user name of the user who created the archive, with additional subfolders **Inbox** and **Sent Items**.

- 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.

- d. You can also leave both the **Recover to alternate folder** and the **Recover all messages to single mailbox** options unchecked. This will import the messages into a folder labeled with the reviewer's user name with subfolders **Inbox** and **Sent Items**.

- 13 Click **Start Recovery** to begin importing data.
- 14 The RecoveryManager component downloads email data from the Email Security Services server and imports it to the appropriate mailbox and mailbox folder. 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 Cancellling the Recovery Process

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

- 15 When the mail for all selected users has completed recovery, click **Continue**.
- 16 If you need to recover another archive, click **Select another archive to recover** to return to the RecoveryManager main screen. If not, select **Exit ESS RecoveryManager**.
- 17 Log in to the designated email account to view the contents of the Discovery Archive.

Index

Symbols

.NET Framework 20

A

account requirements

coexistence environments 26

Exchange 2000/2003 24

Exchange 2007 25

Exchange 5.5 23

See also permissions

Activation (Email Continuity)

defined 2

customizing message on log in screen 177

overview 183

partial 2

reports 167

starting 183

starting recovery from 187

Activation-Based Recovery Archives 130

Administration Console 98

AlertFind

integration limitations 40

integration requirements 40

aliases, creating 159

archives

discovery 201

recovery 129

attachments

storage management of 112

audit 167

audit trail

for email routing configuration 173

viewing 167

Authentication Manager, See Windows Authentication Manager

B

BCC Journaling 193

browsers, supported

for administration 13

for users 14

C

cached mode 33

coexistence environments

account requirements 26

server software requirements 22

supported features 19

D

DCOM

See Microsoft Distributed Component Object Model

Discovery Archives

defined 201

active recovery 190

importing 197

message import 197

recovering mail from 201

reviewer groups to create 122

dropbox 179

E

Email Archive

activation-based recovery archives 130

advanced search options 124

current membership retention policies 104

discovery archives 201

legal holds 111

reviewer groups 122

storage management 112

time-based recovery archives 130

time-of-capture retention policies 104

user classification retention policies 105

See also Historical Mail

Email Continuity

defined 2

activating 183

changing message to users during each state 177

completing recovery 200

partial activation 2, 184

restoring mail to user mailboxes 189

starting recovery 187

states of 4

testing 180

welcoming users 160

Exchange 2000/2003

account requirements 24

interaction with service components 11

server software requirements 20

supported features 19

Exchange 2007

account requirements 25

interaction with service components 11

server software requirements 21

supported features 19

transport agent 60

Exchange 5.5

account requirements 23

server software requirements 20

supported features 19

excluded users
 changing status for multiple users 138
 creating 149

F

fault alerts
 adding users to notification list 164
 for user deletion during sync 176
 for user ID conflicts 150
 readiness checks that trigger 100
 firewall requirements 14

G

gateway requirements 14
 Global Address List 173

H

hardware
 clustering (active/active) 20
 requirements 17
 requirements for Historical Mail 17

Harvester

defined 10
 data collected and logged by 118
 how it works 118
 scheduling 117

help desk users 144

Historical Mail

defined 9
 advanced search options 124
 configuring VaultBoxes for 90
 hardware requirements 17
 installing (software) 86
 legal holds 111
 recovery archives 129
 replication zones 128
 retention policies 103
 reviewer groups 122
 routing requirements 16
 storage management 112
 storage reports 121

home page 176

HTTPS 13

I

internet browsers. See browsers

L

LDAP

connection 52
 max results 192, 202
 port 192, 202

legal holds 111, 112

logging in

to Email Continuity via a welcome message
 160

to the administration console 97
 using Windows Authentication 4

login status of users 145

M

mail searches reports 168

MAPI 191

MAPI/CDO 20

MDAC

See Microsoft Data Access Components

message transfer agent

See MTA

messages

adding disclaimer to 175

maximum size imported to archive 9

undeliverable placed in dropbox 179

Microsoft Data Access Components (MDAC) 20

Microsoft Distributed Component Object Model
 (DCOM) 21

Microsoft Internet Connectivity Wizard 13

Microsoft Internet Information Server (IIS) 21

Microsoft SQL Server 21

Mozilla Firefox

See browsers

MTA 14, 183

MX Record

during activation 183

for replication zones 129

used for forwarding mail 174

used for sending outbound mail during activation 174

N

networking requirements 13

next hop routing

inbound, configuring 173, 174

inbound, described 15

outbound during activation, configuring 174

outbound during activation, described 16

O

operating systems

supported 19

Outlook Extension

defined 7

authentication of users for 74, 75

custom forms for in Exchange 2000/2003 83

custom forms for in Exchange 2007 85

enabling and disabling 158

exporting list of users 158

- feature comparison with webmail 8
- including mail in recovery mode 196
- installing 72
- limitations 34
- registry keys updated for 74
- requirements 33
- users active with 157
- using during activation 183

P

Partial Activation

- defined 2

passwords

- changing administrator 179
- Email Continuity 133
- resetting multiple users' 133
- root account 43
- Windows Authentication of 4

permissions

- Exchange, See account requirements
- help desk user 144

policies

- retention
 - creating 109
 - current membership 104
 - legal holds 112
 - prioritizing 111
 - time-of-capture 104
 - user classification 105
 - using to implement legal holds 111

storage management

- creating 114
- prioritizing 115

- preferences, editing home page 176

- proxy requirements 14

- proxy servers 8

R

readiness checks

- overview 100
- sending fault alerts when failed 164

Recovery

- defined 2
- completing 200
- of discovery archives 201
- restoring mail to user mailboxes 189
- starting (from an activation) 187

Recovery Archives

- defined 129
- creating 130
- restoring mail from 189
- types 130

RecoveryManager

- defined 2
- installation 43
- See also Recovery

RedirectorAgent

- defined 2
- installing 60

RedirectorController

- defined 2
- installation 43
- planning placement 36
- status screen 102

RedirectorManager

- defined 2
- configuring 57
- installation 43
- upgrading 59

RedirectorSink

- defined 2
- installing
 - on clustered Exchange servers 59
 - standalone 58
- planning 35
- planning placement 35
- status screen 102
- upgrading RedirectorManager 59

- reminders, sending 163

- replication zones 128

reports

- activation 167
- audit 167
- mail searches 168
- of users in the welcome process 163
- Outlook Extension 157
- reviewer group 169
- storage 121
- test 168

requirements

- account 23
- communications 13
- firewall 14
- gateway 14
- hardware 17
- hardware for Historical Mail 17
- messaging software 19
- networking 13
- operating systems 19
- proxy 14
- routing for historical mail 16
- server software 20
- service software 18
- SMTP connector for Historical Mail 17

reviewer groups
 defined 122
 advanced search options for 124
 reports 169
 restoring mail from discovery archives 201
 RFC-822 34
 root account
 logging in using 98

S

SMTP
 connector for Historical Mail 17
 gateway servers 35
 message gateway 14
 used in Windows Authentication 28
 Storage Management
 defined 112
 configuring VaultBoxes for 115
 harvester 10
 policies 114
 reports 121
 scheduling 117
 Storage Management Policies
 See policies, storage management
 store and forward mail routing 15
 stubbing
 See Storage Management
 SyncManager
 defined 2
 configuring 49
 configuring user deletion to trigger alert 176
 installation 43
 port used 13
 setting schedules for 49
 synchronizing RIM data 62

T

test
 Email Continuity 180
 reports 168
 Time-Based Recovery Archives 130
 transition alerts 165
 transition reports 167

U

undeliverable mail 179
 user ID conflict
 global settings for resolving 175
 identified by SyncManager 49
 resolving manually 150
 users
 activating Email Continuity for 183
 adding manually to Email Continuity 158

attributes
 displayed in Global Address List 173
 imported from Active Directory 172
 changing status in the system 138
 changing status of those who have opted out 138
 creating aliases for 159
 defining sets of 139
 deletion during sync, configuring warnings 176
 excluding from the service 138, 149
 granting administrative privileges to 143
 help desk 144
 keeping stored mail for when new mailbox is created 49, 150, 175
 login status of 145
 passwords for 133
 restoring mail to after an activation 189
 retaining mail for 103
 searching information 131
 sending reminders to 163
 updating contact information 139
 uploading sets of 139
 welcoming to the service 160

V

VaultBox
 defined 3
 communications with data center 11, 12
 components
 for Historical Mail 10
 configuring
 for Historical Mail 90
 for storage management 115
 console 90
 hardware requirements 17
 installing 86
 preinstallation requirements 39
 replication zones for 128

W

Warnings, See Fault Alerts
 welcome process
 about 160
 changing status for multiple users 138
 including pages in welcome wizard 178
 Windows Authentication
 defined 4
 and changing users' passwords 133
 limitations 28
 requirements 27
 Windows Authentication Manager
 defined 3
 status screen 102

Wireless Continuity for BlackBerry

defined 5

administration 154

limitations 32

managing users and devices 154

provisioning 62

requirements 28

sending instructions to users 71

synchronizing RIM data 62

