

Email Management Services Administrator Guide

For Exchange Environments



Version D6.25-C6.12 (3/2015)

Licensed Customer Confidential

MessageOne

Table of Contents

| | |
|---|-----------|
| Table of Contents | i |
| Task Reference | vi |
| Legal Notices | x |
| About This Book | xi |
| 1. Intended Audience | xi |
| 2. Conventions | xi |
| 3. Product Documentation | xii |
| 1. About Email Management Services | 1 |
| 1.1. Component Products..... | 1 |
| 1.2. Data Center/EMS Admin Console..... | 2 |
| 1.3. Client-Side Software..... | 2 |
| 1.3.1. About SyncManager | 4 |
| 1.3.2. About Redirector Components | 5 |
| 1.3.3. About the VaultBox | 5 |
| 1.3.4. About RecoveryManager | 7 |
| 1.3.5. Interaction of Components..... | 8 |
| 1.4. Current Software Versions | 8 |
| 2. About Email Continuity | 10 |
| 2.1. Email Continuity Functions | 10 |
| 2.2. Email Continuity Components and Data Transfer | 11 |
| 2.2.1. About Windows Authentication Manager | 12 |
| 2.2.2. About the Outlook Extension | 13 |
| 2.2.3. About Wireless Continuity for BlackBerry | 15 |
| 2.3. Email Continuity States | 18 |
| 2.4. Email Continuity Administration | 20 |
| 3. About Historical Mail/Email Archive | 21 |
| 3.1. About Historical Mail/Email Archive | 21 |
| 3.2. About Continuity Archive | 22 |
| 3.2.1. Continuity Archive Requirements | 22 |
| 3.3. About Enterprise Archive | 23 |
| 3.3.1. Enterprise Archive Requirements | 24 |
| 3.4. About Storage Management | 25 |
| 3.5. About Import & Export Manager | 25 |
| 3.6. About Email Archive On-Premises Journaling | 26 |
| 3.7. About Failed Message Tracking | 27 |
| 3.7.1. Failed Message Tracking Additional Information and Limitations | 27 |
| 3.8. About Folder Synchronization | 28 |
| 3.8.1. Folder Sync Additional Information and Limitations | 28 |
| 3.9. Email Archive Roles | 29 |
| 3.10. About Retention Policies | 30 |
| 3.10.1. Retention Policy Best Practices | 31 |
| 3.10.2. Membership-Based (Current Membership) Policies | 32 |
| 3.10.3. Capture-Based Policies | 33 |
| 3.10.4. User Classification Retention Policies | 34 |
| 3.10.5. Query-Based Retention Holds | 37 |
| 3.11. About Email Recovery & Archives | 37 |
| 3.11.1. Time-Based Recovery Archives | 37 |
| 3.11.2. Activation-Based Recovery Archives | 37 |
| 3.11.3. Search-Based Recovery Archives | 38 |
| 3.11.4. Discovery Archives | 38 |

| | |
|--|------------|
| 3.11.5. Failed Message Archive | 39 |
| 3.11.6. Email Continuity Recovery Archives | 39 |
| 3.12. Historical Mail/Email Archive Administration | 40 |
| 4. EMS Controller and Environment Prerequisites | 41 |
| 4.1. Prerequisites for All Installations | 41 |
| 4.1.1. Communications Prerequisites | 42 |
| 4.1.2. Hardware Requirements | 46 |
| 4.1.3. User Permissions Requirements | 47 |
| 4.1.4. Software Requirements | 47 |
| 4.1.5. Virtualization | 56 |
| 4.2. Prerequisites for Optional Features | 56 |
| 4.2.1. Redirector Component Prerequisites | 57 |
| 4.2.2. On-Premises Journaling Prerequisites and Limitations | 60 |
| 4.2.3. Stored/Archived Mail Prerequisites | 61 |
| 4.2.4. Windows Authentication Prerequisites | 66 |
| 4.2.5. Outlook Extension Prerequisites and Limitations | 67 |
| 4.2.6. Wireless Continuity for BlackBerry Prerequisites | 71 |
| 4.2.7. Folder Sync Prerequisites | 77 |
| 4.2.8. AlertFind Integration Prerequisites | 78 |
| 5. Install and Configure EMS Controller and Environment | 79 |
| 5.1. Install Required Service Software | 80 |
| 5.2. Configure the SyncManager | 82 |
| 5.3. Install and Configure Optional Features | 86 |
| 5.3.1. Install Redirector Components | 87 |
| 5.3.2. Configure On-Premises Journaling | 92 |
| 5.3.3. Configure VaultBoxes | 92 |
| 5.3.4. Install Outlook® Extension | 96 |
| 5.3.5. Install Custom Forms for Storage Management | 108 |
| 5.3.6. Deploy Wireless Continuity for BlackBerry | 111 |
| 5.3.7. Mobile App Support Configuration | 121 |
| 5.4. Configure Enterprise Archive Features | 123 |
| 5.4.1. Configure Scanning and Data Transfer for Storage Management Policies | 123 |
| 5.4.2. Harvester Operation and Data Logging | 126 |
| 5.4.3. Configure Scanning and Data Transfer for User Classification Retention Policies | 128 |
| 6. Administering EMS | 131 |
| 6.1. EMS Admin Console | 131 |
| 6.1.1. EMS Admin Console Home | 132 |
| 6.1.2. EMS Readiness Checks | 135 |
| 6.1.3. Authentication Manager Status | 140 |
| 6.1.4. RedirectorController/RedirectorSink/RedirectorAgent Status | 140 |
| 6.2. User Administration | 141 |
| 6.2.1. Search User Information | 141 |
| 6.2.2. Reset User Passwords | 143 |
| 6.2.3. Change Status for Multiple Users | 148 |
| 6.2.4. Update a User's Contact Information | 150 |
| 6.2.5. Define User Sets | 150 |
| 6.2.6. User Permission Levels | 151 |
| 6.2.7. Assign Super Administrator Privileges | 153 |
| 6.2.8. Assign EMS Administrator Privileges | 155 |
| 6.2.9. Assign Help Desk Privileges | 156 |
| 6.2.10. Review Login Status | 157 |
| 6.2.11. Export Users' Contact Information | 158 |
| 6.2.12. Exclude Users or Mailboxes | 160 |

| | |
|---|------------|
| 6.2.13. Resolve User ID Conflicts | 161 |
| 6.3. Mobile App Administration | 164 |
| 6.3.1. Enable Mobile App End-User Access | 164 |
| 6.3.2. Users Download & Access Mobile App | 164 |
| 6.4. Mailboxes and Aliases | 165 |
| 6.4.1. Add Mailboxes (Users) Manually | 165 |
| 6.4.2. Create Aliases | 166 |
| 6.5. Mailing Lists | 167 |
| 6.6. Notification | 167 |
| 6.6.1. Welcome New Users | 167 |
| 6.6.2. Send Reminders | 175 |
| 6.6.3. Manage EMS Fault Alerts | 176 |
| 6.6.4. Manage Email Continuity Transition Alerts | 177 |
| 6.6.5. Send Custom Notifications | 178 |
| 6.7. View EMS Audit Reports | 179 |
| 6.7.1. User Administration Reports | 179 |
| 6.7.2. Notification Reports | 181 |
| 6.7.3. System Settings Reports | 182 |
| 6.8. Modify System Settings | 184 |
| 6.8.1. User Import: Change User Attributes Imported from Active Directory | 184 |
| 6.8.2. Address List Display: Display Global Address List (GAL) Attributes | 185 |
| 6.8.3. Email Routing: Configure Mail Routing | 186 |
| 6.8.4. Network Restrictions | 191 |
| 6.8.5. Password Policy | 193 |
| 6.8.6. Email Disclaimer | 194 |
| 6.8.7. AlertFind Mapping | 195 |
| 6.8.8. User ID Resolution | 196 |
| 6.8.9. Sync Notify Settings | 197 |
| 6.8.10. End User Pages Settings | 198 |
| 6.8.11. Change Logo Image | 202 |
| 6.8.12. Archive Search UI | 202 |
| 6.9. Help and Downloads | 202 |
| 6.10. Change Your EMS Password | 203 |
| 7. Administer Email Continuity | 204 |
| 7.1. Log Into the Email Continuity Admin Console | 204 |
| 7.2. Activate Email Continuity | 204 |
| 7.3. Recover From an Activation | 206 |
| 7.3.1. Start Recovery from an Activation | 207 |
| 7.3.2. Restore Mail to Users' Mailboxes | 208 |
| 7.3.3. Complete Recovery from an Activation | 217 |
| 7.3.4. Create an Activation-Based Recovery Archive | 218 |
| 7.4. Configure BlackBerry Forwarding | 219 |
| 7.5. Wireless Continuity for BlackBerry Administration | 221 |
| 7.5.1. Configuration Parameters | 221 |
| 7.5.2. Manage Users and Devices | 222 |
| 7.5.3. View Information on the BlackBerry Device | 224 |
| 7.6. Outlook® Extension Administration | 227 |
| 7.7. View Email Continuity Audit Reports | 229 |
| 7.7.1. Activation History Reports | 229 |
| 7.7.2. Test History Reports | 230 |
| 7.8. Access Email Continuity Mailboxes | 231 |
| 7.8.1. Access Your Mailbox | 231 |
| 7.8.2. View Undeliverable Mail in the Dropbox | 232 |
| 7.9. Test Email Continuity | 232 |

| | |
|--|------------|
| 8. Administer Historical Mail/Email Archive | 235 |
| 8.1. Historical Mail/Email Archive Admin Console | 235 |
| 8.2. Replication Zones | 236 |
| 8.3. Manage Retention Policies | 237 |
| 8.3.1. Create Retention Policies | 237 |
| 8.3.2. Reconciling User ID Conflicts For Retention Policy Users | 243 |
| 8.3.3. Query-Based Retention Holds | 244 |
| 8.3.4. Use Retention Policies to Simulate Retention Holds | 246 |
| 8.4. Reviewer Groups | 247 |
| 8.4.1. Reviewer Group Email Scope Advanced Options | 251 |
| 8.5. Storage Management | 261 |
| 8.5.1. About Storage Management Policies | 261 |
| 8.5.2. Manage Storage Management Policies | 263 |
| 8.5.3. Return Stubbed Files to User's Mailbox | 268 |
| 8.5.4. Unstub Command Line Tool | 269 |
| 8.6. Storage Reports | 270 |
| 8.6.1. Retention Policy Statistics Report | 271 |
| 8.6.2. Storage Management Policy Statistics Report | 272 |
| 8.6.3. Aggregate Statistics Report | 274 |
| 8.6.4. Daily Message Volume Report | 274 |
| 8.7. Create and Recover Archives | 275 |
| 8.7.1. Time-Based Recovery Archives | 275 |
| 8.7.2. Activation-Based Recovery Archives | 277 |
| 8.7.3. Search-Based Recovery Archives | 279 |
| 8.7.4. Discovery Archives | 279 |
| 8.7.5. Use RecoveryManager to Restore Archives | 280 |
| 8.8. On-Premises Journaling Administration | 287 |
| 8.8.1. Managing On-Premises Journaling Addresses | 287 |
| 8.8.2. On-Premises Journaling Readiness Checks | 288 |
| 8.9. Folder Sync Administration | 289 |
| 8.9.1. Folder Sync Servers | 290 |
| 8.9.2. Folder Sync Enabled Users | 292 |
| 8.9.3. Folder Sync Advanced Settings | 294 |
| 8.9.4. Folder Sync Readiness Checks | 295 |
| 8.10. View Historical Mail Audit Reports | 296 |
| 8.10.1. Archive Searches History Reports | 296 |
| 8.10.2. Archive Activity History Reports | 298 |
| 8.10.3. Recovery Archives History Reports | 299 |
| 8.10.4. Retention Policies History Reports | 300 |
| 8.10.5. Reviewer Groups History Reports | 301 |
| 8.10.6. User Classification History Reports | 303 |
| 9. EMS Cloud Services | 305 |
| 9.1. About EMS Cloud Services | 305 |
| 9.1.1. New Terms and Concepts | 305 |
| 9.1.2. Special Considerations for Office 365 Hybrid Environments | 305 |
| 9.1.3. Administration Console Updates | 309 |
| 9.2. Microsoft Office 365 Prerequisites | 312 |
| 9.2.1. Requirements | 312 |
| 9.3. Microsoft Office 365 Installation | 313 |
| 9.3.1. Configuring Journaling for Office 365 Users | 313 |
| 9.4. Microsoft Office 365 Administration | 316 |
| 9.4.1. Unstubbing Office 365 Users | 316 |
| 9.4.2. EMS Email Archive and Office 365 Users | 317 |
| 9.4.3. Office 365 Best Practices | 317 |

- 10. EMS Expanded Archive Services319**
 - 10.1. About Expanded Archive Services 319
 - 10.2. About EMS Microsoft Lync Archiving 319
 - 10.3. EMS Lync Archive Prerequisites & Limitations 320
 - 10.3.1. Planning 320
 - 10.3.2. Prerequisites 325
 - 10.3.3. Limitations 326
 - 10.4. EMS Lync Archiving Installation 326
 - 10.4.1. Configure Lync Server Archiving 326
 - 10.4.2. Install Client Software 327
 - 10.4.3. Configure EMS Client for EMS Lync Archiving 327
 - 10.5. EMS Lync Archiving Administration 331
 - 10.5.1. EMS Lync Archiving Retention Policy 331
 - 10.5.2. Create EMS Lync Archiving Reviewer Groups 332
 - 10.5.3. Reviewer Created Lync Instant Message Retention Holds 334
 - 10.5.4. Reviewer Created Lync Instant Message Discovery Archives 334
 - 10.5.5. EMS Lync Archiving Statistics 334
 - 10.5.6. EMS Lync Archiving Administration Advanced Topics 336
- 11. Getting Support339**
 - 11.1. Support Overview 339
 - 11.2. Contact Customer Support 339
 - 11.2.1. Prior to Contacting Support 339
 - 11.2.2. Service Requests and Telephone Authorization Form 340
 - 11.3. Service Availability 340
 - 11.4. Improve Customer Support 341
- Index342**

Task Reference

| | |
|--|-----------|
| 1. About Email Management Services ----- | 1 |
| 2. About Email Continuity ----- | 10 |
| 3. About Historical Mail/Email Archive ----- | 21 |
| 4. EMS Controller and Environment Prerequisites ----- | 41 |
| Task 4.1. Grant Exchange administrator permissions for Exchange 2003: | 53 |
| Task 4.2. Grant 'Send As' and 'Receive As' permissions for Exchange 2003: | 53 |
| Task 4.3. Grant 'Send As' and 'Receive As' permissions in Single Environment Exchange 2007, 2010 or 2013 Configurations | 54 |
| Task 4.4. Grant 'Send As' and 'Receive As' permissions in Exchange 2003/2007/2010 Coexistent Con- figurations..... | 54 |
| Task 4.5. Grant 'Send As' and 'Receive As' permissions in Exchange 2007/2010/2013 Coexistent Con- figurations..... | 55 |
| Task 4.6. Add the EMS account to the local administrator group of the BES group: | 74 |
| Task 4.7. Enable TCP and Name Pipes to have access to the BES database: | 74 |
| Task 4.8. Verify that the MDS server is a push server and has an appropriate listening port configured: 75 | |
| Task 4.9. Verify IT policies:..... | 76 |
| 5. Install and Configure EMS Controller and Environment ----- | 79 |
| Task 5.1. Install service software:..... | 80 |
| Task 5.2. Launch the SyncManager Setup Wizard manually:..... | 83 |
| Task 5.3. Configure the SyncManager: | 83 |
| Task 5.4. Configure distributed synchronization with SyncManager:..... | 86 |
| Task 5.5. Install RedirectorSink on clustered Exchange servers: | 87 |
| Task 5.6. Install the RedirectorAgent:..... | 89 |
| Task 5.7. Remove the RedirectorAgent: | 89 |
| Task 5.8. Install RedirectorManager: | 90 |
| Task 5.9. Configure On-Premises Journaling..... | 92 |
| Task 5.10. Change data transfer settings:..... | 93 |
| Task 5.11. Authenticate users through the command line (prior to Outlook Extension deployment):...98 | |
| Task 5.12. Create an Outlook Authentication Update schedule for all users | 100 |
| Task 5.13. Manually run an Outlook Authentication Update. | 100 |
| Task 5.14. Overwrite Outlook Authentication token | 101 |
| Task 5.15. Install the Outlook Extension using Group Policy:..... | 102 |
| Task 5.16. Upgrade the Outlook Extension using Group Policy: | 103 |
| Task 5.17. Enable or disable the Outlook Extension using Group Policy: | 103 |
| Task 5.18. Remove the Outlook Extension using Group Policy:..... | 104 |
| Task 5.19. Install the Outlook Extension manually..... | 104 |
| Task 5.20. Remove the Outlook Extension manually:..... | 104 |
| Task 5.21. Customize Outlook Ribbon Tab and Group Names | 105 |
| Task 5.22. Add a new folder to Exchange Organizational Forms Library in Exchange 2003:..... | 108 |
| Task 5.23. Create an organizational forms library in Exchange 2007/2010:..... | 109 |
| Task 5.24. Publish forms to the Exchange Organizational Forms Library: | 110 |
| Task 5.25. Synchronize RIM data:..... | 111 |
| Task 5.26. Download the client agent..... | 114 |
| Task 5.27. Configure the agent:..... | 115 |
| Task 5.28. Assign software applications to users:..... | 116 |
| Task 5.29. Remove the Blackberry agent for all users:..... | 116 |

| | |
|---|-----|
| Task 5.30. Remove the Blackberry agent for one user: | 116 |
| Task 5.31. Create and share the application directory: | 118 |
| Task 5.32. Define the application directory in the BlackBerry Administration Service: | 118 |

| | |
|---|------------|
| Task 5.33. Download the client agent | 119 |
| Task 5.34. Add and publish the application: | 119 |
| Task 5.35. Create and populate the software configuration: | 120 |
| Task 5.36. Configure the application deployment schedule to deploy the application as soon as possible (optional): | 120 |
| Task 5.37. Assign the software configuration to a user: | 120 |
| Task 5.38. View the status of a job: | 121 |
| Task 5.39. Change data transfer settings for Storage Management: | 124 |
| Task 5.40. Configure Storage Management parameters | 125 |
| Task 5.41. Configure Manual Retention (User Classification) Task schedule settings: | 128 |
| 6. Administering EMS | 131 |
| Task 6.1. Log into the EMS Admin Console: | 132 |
| Task 6.2. Search user information: | 142 |
| Task 6.3. Reset a user's password: | 143 |
| Task 6.4. Change multiple users' passwords: | 144 |
| Task 6.5. Create a password import CSV file: | 146 |
| Task 6.6. Import passwords by CSV file: | 147 |
| Task 6.7. Change status flags for users: | 149 |
| Task 6.8. Edit a user's contact information: | 150 |
| Task 6.9. Create a user set: | 150 |
| Task 6.10. Create a super administrator: | 154 |
| Task 6.11. Remove super administrator privileges | 154 |
| Task 6.12. Assign administrative privileges to an account: | 155 |
| Task 6.13. Remove administrative privileges from an account: | 155 |
| Task 6.14. Grant a user Help Desk privileges: | 156 |
| Task 6.15. Remove Help Desk privileges from an account: | 156 |
| Task 6.16. Review login status: | 157 |
| Task 6.17. Generate a CSV spreadsheet of emergency contact data for all users: | 159 |
| Task 6.18. Exclude a user: | 160 |
| Task 6.19. Remove individual users from the Excluded list (reinstate them in the system): | 160 |
| Task 6.20. Remove multiple users from the Excluded list (reinstate them in the system): | 161 |
| Task 6.21. Resolve multiple user ID conflicts using CSV upload: | 162 |
| Task 6.22. Resolve user ID conflicts individually | 163 |
| Task 6.23. Enable End-User Mobile App Access | 164 |
| Task 6.24. Add a mailbox (user) to EMS: | 166 |
| Task 6.25. Create an alias: | 166 |
| Task 6.26. View mailing lists and members of each list: | 167 |
| Task 6.27. Send a welcome message to users not yet welcomed: | 170 |
| Task 6.28. Re-send a welcome message to any user: | 171 |
| Task 6.29. Re-send welcome message to users who have not responded: | 172 |
| Task 6.30. Send welcome message to users who have not set a permanent password: | 173 |
| Task 6.31. Automatically send welcome messages to new users: | 174 |
| Task 6.32. Send a reminder: | 175 |
| Task 6.33. Add a user to the fault alerts list: | 176 |
| Task 6.34. Remove a user from the fault alerts list: | 177 |
| Task 6.35. Add users to the transition alerts list | 177 |
| Task 6.36. Remove a user from the transition alerts list: | 177 |
| Task 6.37. Send a custom message: | 178 |
| Task 6.38. View any of the user administration reports: | 180 |
| Task 6.39. View notification reports: | 181 |
| Task 6.40. View system settings reports: | 183 |
| Task 6.41. Change the attributes imported from Active Directory: | 185 |
| Task 6.42. Change the attributes displayed in Global Address List | 186 |
| Task 6.43. Restore an attribute that has been removed: | 186 |

| | |
|--|------------|
| Task 6.44. Configure the routing path for forwarded mail: | 187 |
| Task 6.45. Configure the path for outbound mail during an activation: | 189 |
| Task 6.46. Disable Store and Forward | 190 |
| Task 6.47. Enable 3rd-party external archive support | 191 |
| Task 6.48. Configure network restrictions: | 192 |
| Task 6.49. Set authentication method. | 193 |
| Task 6.50. Set password lock out policy: | 194 |
| Task 6.51. Set password constraints | 194 |
| Task 6.52. Add disclaimer text to the end of each message sent by the service: | 194 |
| Task 6.53. Configure AlertFind mapping: | 195 |
| Task 6.54. Configure the system-wide method for resolving user ID conflicts: | 197 |
| Task 6.55. Configure the user/mailling list deletion percentage at which a warning message is sent: | 198 |
| Task 6.56. Display/hide all the Preferences or Help prompts from the end-user's Home page: | 200 |
| Task 6.57. Enable/disable individual links in the Preferences section of the Home page: | 200 |
| Task 6.58. Change the text displayed to end users on the Home Page: | 200 |
| Task 6.59. Set your own logo: | 202 |
| Task 6.60. Enable Classic Email Archive Interface | 202 |
| Task 6.61. Change your password: | 203 |
| 7. Administer Email Continuity ----- | 204 |
| Task 7.1. Activate Email Continuity | 205 |
| Task 7.2. Initiate recovery: | 207 |
| Task 7.3. Recover mail from an activation: | 209 |
| Task 7.4. Complete recovery from an activation | 218 |
| Task 7.5. Create an Activation-based Recovery Archive: | 218 |
| Task 7.6. Configure a BlackBerry device for BlackBerry forwarding: | 220 |
| Task 7.7. View BlackBerry user and device information: | 222 |
| Task 7.8. Export BlackBerry device details | 223 |
| Task 7.9. Reset a BlackBerry device: | 223 |
| Task 7.10. Send BlackBerry device logs/diagnostics to Support: | 224 |
| Task 7.11. View information about a device using the interface installed with the device agent: | 224 |
| Task 7.12. Enable or disable the Extension: | 227 |
| Task 7.13. Export the list of users: | 228 |
| Task 7.14. View an Activation History Report | 229 |
| Task 7.15. View a Test History Report: | 230 |
| Task 7.16. Access your webmail account during an activation: | 232 |
| Task 7.17. View undeliverable mail during an activation: | 232 |
| Task 7.18. Start a test of Email Continuity: | 232 |
| Task 7.19. Start recovery from a test | 233 |
| 8. Administer Historical Mail/Email Archive ----- | 235 |
| Task 8.1. Assign servers to replication zones: | 236 |
| Task 8.2. Create a retention policy | 239 |
| Task 8.3. Add users to a retention policy | 241 |
| Task 8.4. Prioritize retention policies | 242 |
| Task 8.5. Delete a Retention Hold | 244 |
| Task 8.6. Edit a Retention Hold and view a hold's change history | 245 |
| Task 8.7. Create a Reviewer Group: | 247 |
| Task 8.8. Edit a Reviewer Group: | 249 |
| Task 8.9. Delete a Reviewer Group: | 250 |
| Task 8.10. Create a Storage Management policy | 264 |
| Task 8.11. Prioritize Storage Management policies | 266 |
| Task 8.12. Edit Storage Management policies | 267 |
| Task 8.13. Delete Storage Management policies | 268 |
| Task 8.14. Unstub all messages for a user: | 268 |

| | |
|---|------------|
| Task 8.15. View storage reports: | 271 |
| Task 8.16. Create a Time-Based Recovery Archive: | 276 |
| Task 8.17. Create an Activation-Based Recovery Archive: | 277 |
| Task 8.18. Recover a Historical Mail archive to user mailbox(es): | 280 |
| Task 8.19. Add On-Premises Journaling Address | 287 |
| Task 8.20. Delete On-Premises Journaling Address | 288 |
| Task 8.21. Assign Exchange Servers to Folder Sync Servers | 291 |
| Task 8.22. Remove Exchange Servers from Folder Sync Servers | 291 |
| Task 8.23. Enable users for Folder Sync | 292 |
| Task 8.24. Disable users for folder sync | 293 |
| Task 8.25. View an Archive Searches History Report: | 297 |
| Task 8.26. View a Archive Activity History Report: | 298 |
| Task 8.27. View a Recovery Archives History Report: | 299 |
| Task 8.28. View a Retention Policies History Report: | 301 |
| Task 8.29. View a Reviewer Groups History Report | 302 |
| Task 8.30. View a User Classification Report: | 303 |
| 9. EMS Cloud Services ----- | 305 |
| Task 9.1. Configuring Journaling for Office 365 Users | 313 |
| 10. EMS Expanded Archive Services ----- | 319 |
| Task 10.1. Install and configure EMS Client Software | 327 |
| Task 10.2. Configure EMS Client for EMS Lync Archiving | 328 |
| Task 10.3. Edit EMS Lync Archiving Retention Policy | 332 |
| Task 10.4. Create EMS Lync Archiving Reviewer Group | 333 |
| Task 10.5. View EMS Lync Archiving statistics | 335 |
| 11. Getting Support ----- | 339 |

Legal Notices

Copyright© 1998-2015 MessageOne. 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 MessageOne. Reproduction prohibitions do not extend to distribution among the employees of licensed customers or for use in activities conducted by MessageOne partners in the course of sales, marketing, training, or support.

“Business Continuity that makes Business Sense,” EMS, SyncManager, RedirectorSink, RedirectorController, RecoveryManager, and OneSwitch are trademarks of MessageOne.

AlertFind® is a registered trademark of MessageOne.

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 LICENSE file in the installation directory.

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

About This Book

This chapter contains the following sections:

- ["Intended Audience" on page xi](#)
- ["Conventions" on page xi](#)
- ["Product Documentation" on page xii](#)

1. 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.

2. 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 5-1 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 "Product Documentation" on page xii . |
| bold | Name of a screen, section, pane, box, or option in the user interface. The name of an executable file. | On the Select Permissions page, locate the Access Info pane of the User Account panel. To begin the installation, double-click setup.exe . |

Table 5-1 Typographical Conventions (Continued)

| Display Format | Definition | Examples |
|---------------------------|---|---|
| <i>Bold italic</i> | The name of a menu, button, or tab. | From the <i>Start</i> menu, select <i>Programs</i> . |
| serif | An entry you must type manually. A value you type in a box or select from a list. A field value that appears in the user interface. | At the command prompt, type <code>cmd</code> . From the Filter drop-down list, select <code>Starts with</code> . The Source field now reads <code>Imported from File</code> . |

3. Product Documentation

The following documentation is available for Email Management Services:

- *Email Management Services Suite Administration Guide*
This book is a comprehensive document for installing, configuring and administering the Email Management Services suite of products.
- *Email Management Services Email Continuity User Guide*
This user guide describes the use of the Email Management Services Email Continuity user interface and services, including webmail usage.
- *Network Settings Guide*
This document provides location-specific IP addresses and Message Transfer Agent (MTA) information based on the location of the MessageOne data center.

The following materials are available for Email Archive:

- *Email Management Services Email Archive Reviewer Guide*
This document focuses on actions available to users designated as archive reviewers, such as creating and searching Discovery Archives.
- *Email Management Services Email Archive User Guide*
This document explains how to use Email Archive, such as how to access and search historical email.
- *Email Management Services Import Manager Guide*
This document describes the Import Manager which imports email messages from local information stores into the EMS data center.
- *Email Management Services Export Manager Guide*
This document describes the Export Manager which exports email messages from the EMS data center to local information stores.

- *Storage Management User Guide*

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

The following documentation is available for Email Management Services mobile users:

- *Mobile Access User Guide*

This user guide describes the use of the Email Management Services mobile web-based and iOS App services, including limitations.

- *Wireless Continuity for BlackBerry User Guide*

This user guide describes the use of the Email Management Services Wireless Continuity for BlackBerry interface and services, including software prerequisites and limitations.

For the latest version of any document, contact Support.

1. About Email Management Services

The Email Management Services suite of products provides a total solution for email continuity, recovery, and archiving needs.

This chapter covers the following topics:

- 1) ["Component Products" on page 1](#)
- 2) ["Data Center/EMS Admin Console" on page 2](#)
- 3) ["Client-Side Software" on page 2](#)
 - ["About SyncManager" on page 4](#)
 - ["About Redirector Components" on page 5](#)
 - ["About the VaultBox" on page 5](#)
 - ["About RecoveryManager" on page 7](#)
 - ["Interaction of Components" on page 8](#)
- 4) ["Current Software Versions" on page 8](#)

1.1. Component Products

The Email Management Services suite includes the following product components. Each product uses software housed at the Data Center (see ["Data Center/EMS Admin Console" on page 2](#)) and on your organization's mail servers (see ["Client-Side Software" on page 2](#)).

- **Email Continuity:** Email Continuity is an alternative email service that takes the place of your primary email system during a planned or emergency outage. See ["About Email Continuity" on page 10](#) for more information.
- **Historical Mail/Email Archive:** Historical Mail/Email Archive captures and archives incoming and outgoing mail messages and attachments according to criteria you define in configurable retention policies. These messages and attachments are stored in a secure data center. For more details, see ["About Historical Mail/Email Archive" on page 21](#).

EMS also includes the options of:

AlertFind Integration: If your organization uses AlertFind, you can take advantage of regular synchronization to extend your Active Directory data to the AlertFind service. Directory synchronizations from Active Directory to the EMS data center take place according to the schedule established in the EMS SyncManager component. In a

separate process run in the data center, MessageOne migrates the Active Directory data you've selected to the AlertFind application. With AlertFind integration, you can update your directory data as often as once per day. For more information, see:

- ["AlertFind Integration Prerequisites" on page 78](#)
- ["AlertFind Mapping" on page 195](#)

Mobile App end-user access: The EMS Mobile Apps provide the ability for end-users to access Email Continuity and Email Archive functionality through native application interfaces. The features that are available to the end-user depend upon which EMS services have been purchased by your organization. For more information see:

- ["Mobile App Support Configuration" on page 121](#)
- ["Mobile App Administration" on page 164](#)

Cloud Services support: The EMS Email Archive function provides support for external "Cloud-based" email platforms. EMS Cloud Services currently supports Microsoft Office 365 in hybrid environments. For more information see:

- ["About EMS Cloud Services" on page 305](#)

1.2. Data Center/EMS Admin Console

Each client-side component of the suite interacts with software that resides in the Email Management Services **Data Center**. Your organization's authorized administrators and users can access these data center features and functions using the web-based **EMS Admin Console**. See the following chapters for instructions on accessing these features:

- ["Administer Email Continuity" on page 204](#)
- ["Administer Historical Mail/Email Archive" on page 235](#)

1.3. Client-Side Software

Each component product of the Email Management Services suite requires that you install certain **client-side components** (often called **service software**) in your organization's mail environment. For information about installing these components see ["Install Required Service Software" on page 80](#).

Table 1-1 Email Management Services Components - Client Environment

| Component | Description |
|--|--|
| Synchronization Component | |
| Required for all EMS installations. | |
| SyncManager™ | <p>Software that synchronizes your local directory, calendar and contact information with the data center.</p> <p>The SyncManager is installed in your mail server environment. See "About SyncManager" on page 4.</p> |
| Redirector (Mail Routing) Components | |
| <p>For <i>Email Continuity</i> users, Redirector components are required to enable the optional <i>partial activation</i> feature (a process where some users remain on the primary mail system while others use Email Continuity).</p> <p>For users of <i>stored mail/archive components</i>, Redirector components are required to transfer copies of mail to the VaultBox for processing.</p> | |
| RedirectorSink™ | <p>An SMTP Event Sink required to enable dynamic rerouting of messages.</p> <p>The RedirectorSink is installed on one or more of your Exchange servers. Exchange 2003 servers only support RedirectorSinks, and do not use RedirectorAgents. See "About Redirector Components" on page 5.</p> |
| RedirectorAgent | <p>A custom transport agent that performs functions similar to the RedirectorSinks to support partial activation in Exchange 2007 environments.</p> <p>The RedirectorAgent is installed on all of your Exchange 2007 Hub Transport servers. The RedirectorAgent is not supported on Exchange 2007 Edge servers. See "About Redirector Components" on page 5.</p> |
| RedirectorController™ (also called the EMS Controller) | <p>Software that communicates to the data center and provides updates to the RedirectorSinks and RedirectorAgents.</p> <p>The RedirectorController is installed in your environment. See "About Redirector Components" on page 5.</p> |
| RedirectorManager™ | <p>A centralized console to install, upgrade and maintain RedirectorSinks on standalone Exchange servers.</p> <p>The RedirectorManager is installed in your environment. See "About Redirector Components" on page 5.</p> |
| Mail/Storage/Archiving Component | |
| Required only for organizations using stored mail/archive features. | |
| VaultBox™ | <p>Software responsible for accepting messages from customer's mail servers, and encrypting, compressing, and transferring messages to the data center.</p> <p>The VaultBox must be installed in your environment on a dedicated server. This can be the same server on which the SyncManager and RecoveryManager are installed or another dedicated server. See "About the VaultBox" on page 5.</p> |

Table 1-1 Email Management Services Components - Client Environment

| Component | Description |
|---|--|
| Mail Recovery Component | |
| Required for all EMS installations. | |
| RecoveryManager™ | <p>Software that restores mail into your primary mail system after an activation of Email Continuity. This process is called <i>recovery</i>. RecoveryManager also restores mail from a Historical Mail archive into your primary mail system.</p> <p>The RecoveryManager is installed in your environment. See "About RecoveryManager" on page 7.</p> |
| Optional Email Continuity Subcomponents | |
| Required only to use optional features of Email Continuity. | |
| Windows Authentication Manager | <p>Allows end users to log in to the Email Continuity portal using their Windows user name and password.</p> <p>Windows Authentication Manager is installed in your environment only if you use the optional Windows Authentication service. See "About Windows Authentication Manager" on page 12.</p> |
| Outlook® Extension | <p>Software that provides access to certain Email Management Services features through a user's Outlook application.</p> <p>The Outlook Extension is installed on end user desktops only if you want to offer the optional Outlook Extension component. See "About the Outlook Extension" on page 13.</p> |
| RIM Agent | <p>A lightweight, Java-based agent that enables users to access messages on their BlackBerry devices during an activation of Email Continuity.</p> <p>The agent is installed on the BlackBerry device of any user who wants to use the optional Wireless Continuity for BlackBerry service. See "About Wireless Continuity for BlackBerry" on page 15.</p> |

1.3.1. About SyncManager

The **SyncManager** component synchronizes your local directory, calendar and contact information with the data center.

SyncManager is required for all EMS installations and is installed using in the Email Management Services service software package. You can configure synchronizations to occur on a regular schedule, or you can launch SyncManager to run synchronizations at unscheduled times. See ["Configure the SyncManager" on page 82](#) for more information.

1.3.2. About Redirector Components

Redirector components are installed on your Exchange servers to enable dynamic rerouting of messages. Redirector components are required only if your organization will use optional partial activation or mail archiving features. Redirector components are installed along with other components in the Email Management Services service software package. See ["Redirector Component Prerequisites" on page 57](#) for more information.

For Email Continuity users, Redirector components are necessary for *partial activation* (a process where some users remain on the primary mail system while others use Email Continuity).

For users of *stored mail/archive components*, Redirector components are necessary to transfer copies of mail to the VaultBox for processing.

Redirector components include the following:

- **RedirectorSinks** are SMTP Event Sinks installed on your Exchange servers that enable the dynamic rerouting of messages. RedirectorSinks redirect messages in your Exchange environment for active Email Continuity users to the data center using the routing information they receive from RedirectorControllers. You must install RedirectorSinks to use the partial activation feature in Exchange 2003 environments.
- **RedirectorAgents** are used only in Exchange 2007 environments. They are custom transport agents that perform functions similar to the RedirectorSinks to support partial activation. You do not need RedirectorAgents if you are running another version of Exchange, or if you do not use the partial activation feature.
- **RedirectorControllers**, also called EMS Controllers, communicate with the data center and provide updates for the RedirectorSinks and RedirectorAgents.
- **RedirectorManager** is a centralized console that lets you install, upgrade and maintain RedirectorSinks on standalone Exchange servers.

1.3.3. About the VaultBox

The VaultBox component enables your mail users to access archived mail stored at the data center. Installing one or more VaultBoxes is required only for organizations using stored mail/archive features.

For Email Continuity users, the VaultBox enables the *Historical Mail* feature. Historical Mail allows Email Continuity users to access stored email during an activation of Email Continuity. Your organization identifies the messages to be stored by defining a retention policy. To access and search stored mail, users log into the web-based Email Continuity webmail interface.

For Email Archive users, the VaultBox enables user access to archived mail 24/7/365 and storage management features of the full Email Archive product. See ["About Historical Mail/Email Archive" on page 21](#).

NOTE Maximum Archive Message Size

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.

To enable access to archived mail stored at the data center, you must install the VaultBox components described in [Table 1-2](#) below along with the Redirector components described under ["About Redirector Components" on page 5](#). The VaultBox software must be installed on a dedicated server. This dedicated server can be the same one on which SyncManager, RecoveryManager, and other service software is installed.

Table 1-2 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 messages 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 EMS Admin 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 (used for Storage Management only) | A task that finds messages eligible 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 links to the data center. |
| Harvester Service (used for 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 <code>m1harvester</code> service to your list of monitored services. |
| Import from Exchange command (used for 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 1-1](#).

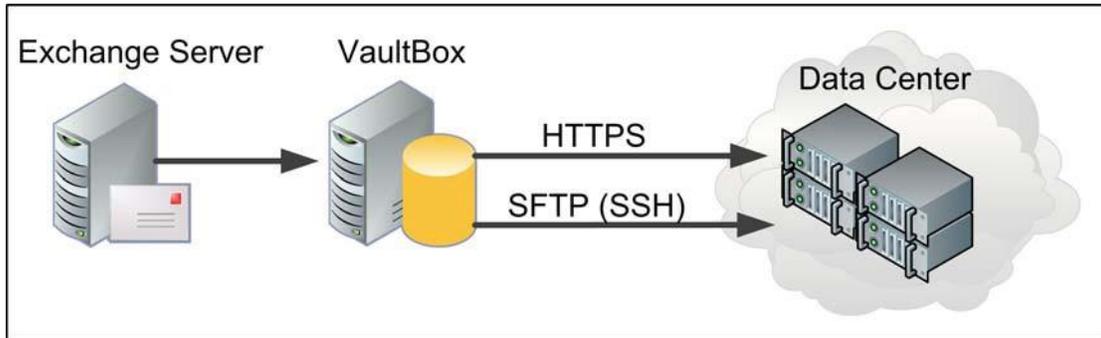


Figure 1-1 Data Transfer for Email Archive

1.3.4. About RecoveryManager

RecoveryManager is required for all EMS installations and is installed using in the Email Management Services service software package. See ["Install Required Service Software" on page 80](#)

RecoveryManager restores mail sent or received during an activation of Email Continuity into your primary mail system after the activation is over. This process is called *recovery*. See ["Recover From an Activation" on page 206](#).

RecoveryManager restores historical mail from data center archives into your primary mail system. See ["Create and Recover Archives" on page 275](#).

1.3.5. Interaction of Components

Figure 1-2 shows the interaction of client-side service software components, your Exchange mail server, and the data center. Port numbers are shown in parentheses.

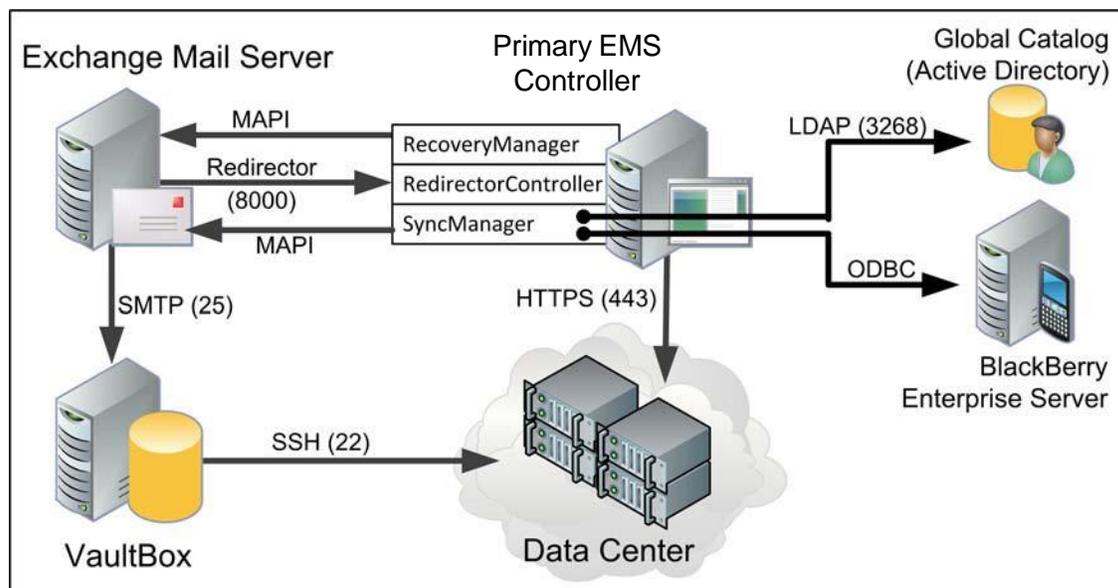


Figure 1-2 Communications Protocols and Port Numbers

To support the partial activation feature of Email Continuity, for Exchange 2003 environments, the Redirector noted in the figure are the RedirectorSinks, see ["Install RedirectorSink on Clustered Exchange Servers" on page 87](#). For Exchange 2007/2010/2013 environments, the system uses RedirectorAgent installed on each Hub Transport server, see ["Install the RedirectorAgent" on page 88](#)

1.4. Current Software Versions

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

Table 1-3 Software Release Versions

| Software | Description | Version | How do I know what version I have? |
|--|--|---------|---|
| Data Center/EMS Admin Console for all components | Software installed in the data center. Changes made to this software may be visible in the EMS Admin Console, or may not be visible at all to administrators or end users. | 6.22 | From the EMS Admin Console, select About . |
| Client-side component software | SyncManager, RecoveryManager, VaultBox, and other software components installed in your organization's environment. | 6.11 | Start one of the client-side components (for example, Start > Programs > MessageOne > SyncManager .) The version number appears |
| Outlook Extension (for Email Continuity only) | Software installed on an end user's machine to support the multiple features of the Outlook Extension. | 6.9 | From the Outlook Extension menu, select Tools > Options > MessageOne EMS > |
| Wireless Continuity for BlackBerry (for Email Continuity only) | Client agent software distributed to user's BlackBerry devices. | 6.2.2 | From the EMS Admin Console, select Blackberry Administration > Export > Export . Sort by Agent Version to see all software versions. |
| Export Manager | Software installed in your organization's environment (not on the same machine that runs the VaultBox), that exports archived messages to PST or EML files. | 6.11 | |
| Import Manager | Software installed in your organization's environment (not on the same machine that runs the VaultBox), that imports messages from PST files into the archive. | 7.1 | From the Import Manager tool, click on the About link. |
| iOS App | Available from Apple iTunes store, entitled <i>MessageOne Email Management</i> or <i>Email</i> | 1.0 | From the app's login page, tap the About link to display the version. |

2. About Email Continuity

Email Continuity is an alternative email service that takes the place of your primary email system during a planned or emergency outage.

This chapter covers the following topics:

- ["Email Continuity Functions" on page 10](#)
- ["Email Continuity Components and Data Transfer" on page 11](#)
- ["Email Continuity States" on page 18](#)
- ["Email Continuity Administration" on page 20](#)

2.1. Email Continuity Functions

Using the **service software** that you install in your organization's mail environment and the software that resides in the Email Management Services **data center**, Email Continuity provides the following functions:

- **Data synchronization.**

Using the **SyncManager** installed in your environment, Email Continuity synchronizes all of your local directory, calendar, and contact information with the data center. For more information about the SyncManager, see ["Install Required Service Software" on page 80](#)

- **Email continuity service during scheduled or emergency outages of your mail system.**

Administrators can choose to activate continuity services for all of the users in your mail environment, for subsets of users, or for specific mail servers.

The Email Continuity Webmail functionality allows users to access their email through a secure browser-based interface. Users can send and receive email messages through this interface until normal service is restored to their primary email system.

You can also allow your mail users to access their mail during an activation by installing the optional **Outlook Extension** client software on user desktops. This allows mail users to access their mail through Outlook during the activation. See ["About the Outlook Extension" on page 13](#) for more information.

If you install the optional **Windows Authentication Manager** into your environment, your mail users can log in to Email Continuity using their existing Windows user names and passwords. See ["About Windows Authentication Manager" on page 12](#) for more information.

- **Email continuity service for wireless devices.**

Included in Email Continuity is Mobile Webmail functionality, which allows users to access their email through a secure, iOS or Android mobile-browser-based interface. Users can send and receive email messages through this interface until normal service is restored to their primary email system.

An iOS app has been created to access Email Continuity. The app must be downloaded by the end-user from the Apple iTunes store. Login access to the iOS app is controlled through the **Mobile Application Enabled Users** list

If your organization chooses to enable the optional **BlackBerry Forwarding** feature, copies of messages can be forwarded to users' RIM devices during an activation of Email Continuity.

Your organization can also choose to implement the full **Wireless Continuity for BlackBerry** subcomponent. This option ensures that messages are delivered to BlackBerry users when Email Continuity is active, and can also deliver messages to BlackBerry users even if your BES fails along with the primary mail system. For more information, see ["About Wireless Continuity for BlackBerry" on page 15](#).

NOTE BlackBerry Forwarding vs. Wireless Continuity for BlackBerry

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

- **Access to stored/archived mail during an activation of Email Continuity.**

The optional Historical Mail upgrade allows your users to access historical email when Email Continuity is active. To use this feature, you must install the optional VaultBox components described in [Table 1-2 on page 6](#) along with the Redirector components described under ["About Redirector Components" on page 5](#).

- **Full range of administration features, audit reports, and system settings using the EMS Admin Console.**

Your organization's authorized administrator users can log into the web-based EMS Admin Console (hosted at the data center) to perform all necessary administration functions. All functions and features of the EMS Admin Console are discussed under ["Administer Email Continuity" on page 204](#).

2.2. Email Continuity Components and Data Transfer

Email Continuity requires you to install and configure at least the following **required** client-side components described under ["Client-Side Software" on page 2](#):

- **SyncManager:** SyncManager is required to keep the directory and contacts information stored in your local mail environment synchronized with the data center. See ["About SyncManager" on page 4.](#)
- **RecoveryManager:** RecoveryManager is required to bring all messages sent or received during an activation back into your mail environment after the outage is ended. See ["About RecoveryManager" on page 7.](#)

You can use extended *optional* features by installing and configuring the following components:

- **Mail Redirector Components:** Redirector components are necessary if your organization wants to enable *partial activation* (a process where some users remain on the primary mail system while others use Email Continuity) or if you want to use the optional stored mail/archive features. See ["About Redirector Components" on page 5.](#)
- **VaultBox:** Install and configure one or more VaultBoxes to use the optional Historical Mail feature. See ["About the VaultBox" on page 5.](#)
- **Windows Authentication Manager:** Install and configure Windows Authentication Manager to allow your users to log into Email Management Services using their existing network user names and passwords. See ["About Windows Authentication Manager" on page 12.](#)
- **Outlook Extension:** Deploy the Outlook Extension to provide your users with a more seamless mail continuity experience. With the Outlook Extension, users continue to use Outlook even when Email Continuity is active and mail is being rerouted. See ["About the Outlook Extension" on page 13.](#)
- **Wireless Continuity for BlackBerry:** Deploy agent software to users' RIM/ BlackBerry devices to enable them to access their mail from their BlackBerry devices during an activation. See ["About Wireless Continuity for BlackBerry" on page 15.](#)

After you have installed and configured client-side components, you can perform most administrative functions using software that resides in the Email Management Services **data center**. Your organization's authorized administrators and users can access these data center features and functions using the web-based **EMS Admin Console**. See ["Administer Email Continuity" on page 204.](#)

2.2.1. About Windows Authentication Manager

The Windows Authentication feature allows your users to log in to the EMS web interface using their existing Windows network user names and passwords. To enable this, you must install Authentication Manager on a local machine in your environment that validates a user's credentials with the local Windows subsystem.

NOTE Passwords are Not Synchronized to the Data Center

When your organization uses Authentication Manager, user passwords are not synchronized from Active Directory to the data center. Authentication Manager validates credentials against the local Windows subsystem.

Depending on whether the credentials are valid, Authentication Manager takes various actions:

- 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 web interface.
- If the Windows subsystem determines that 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 ["Authentication Manager Status" on page 140](#) and ["Windows Authentication Prerequisites" on page 66](#).

2.2.2. About the Outlook Extension

When the Outlook[®] Extension is installed on end-user machines, and when end-users have been authenticated (logged in/registered with Email Management Services), the Outlook Extension periodically polls the data center to see if Email Continuity has been activated. If so, Outlook goes into *offline mode*, and remains offline for the duration of the activation. While Email Continuity is active, messages are routed and delivered to user Inboxes 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 an administrator directs the RecoveryManager to do so.

If Outlook remains open during the activation, the Outlook Extension normally receives a state change signal from the Email Continuity server telling it to reconnect to the Exchange server and return to regular operation when the activation is over. However, if Outlook is closed during the activation and it misses the state change, it may remain offline after the activation is over. If this happens, users can reconnect to Exchange and resume regular operation by right-clicking the **Offline** button.

NOTE Proxy Servers

If your organization uses proxy servers, the Outlook Extension provides basic proxy authentication. The Outlook Extension provides a dialog box for users 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 that polls for the message.

NOTE No Mac Support for Outlook Extension

MessageOne does not provide a version of EMS Outlook Extension for *MS Entourage* or *MS Outlook 2011 for Mac* because those programs do not support Outlook Extensions.

[Table 2-1](#) compares the features and functionality available to users through Email Continuity webmail and the Outlook Extension. A check (✓) means that the feature or function is available. A dash (—) means the feature or function is not available. For more information on limitations of the Outlook Extension, see "[Outlook Extension Limitations](#)" [on page 69](#).

Table 2-1 Outlook Extension/Email Continuity Webmail Feature Comparison

| Outlook Feature | Available in Webmail? | Available in the Outlook Extension? |
|---|-----------------------|-------------------------------------|
| Send and receive email | ✓ | ✓ |
| View or use the message importance feature | ✓ | ✓ |
| Use HTML mail formats | ✓ | ✓ |
| View or use the message sensitivity feature | — | ✓ |
| Use message delivery options | — | — |
| View calendars | ✓ | ✓ |
| Receive appointments | ✓ | ✓ |
| Modify calendars | — | ✓ |

Table 2-1 Outlook Extension/Email Continuity Webmail Feature Comparison

| Outlook Feature | Available in Webmail? | Available in the Outlook Extension? |
|--|-----------------------|-------------------------------------|
| Send appointments | — | ✓ |
| Access free/busy information | — | — |
| View contacts | ✓ | ✓ |
| Modify contacts | — | ✓ |
| View Global Address List | ✓ | ✓ |
| View tasks | — | ✓ |
| Modify tasks | — | ✓ |
| View or use categories | — | ✓ |
| Manage folders | Not applicable | ✓ |
| Access PST folders | Not applicable | ✓ |
| View or use the Reminders window | — | ✓ |
| Access client-side rules (filters) | — | ✓ |
| Access server-side rules and the Out-of-Office feature | — | — |
| Delegate access or view others' mailboxes | — | — |

For more information, see: ["Outlook® Extension Administration" on page 227](#).

2.2.3. About Wireless Continuity for BlackBerry

NOTE BlackBerry Forwarding vs. Wireless Continuity for BlackBerry

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

The Wireless Continuity for BlackBerry feature ensures that 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 mail system.

NOTE BES-Independent Wireless Continuity for BlackBerry

The EMS data center implements a BES-independent continuity model that allows BlackBerry users to compose, send, and receive mail 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 that uses version 6.2.2.3 (or higher) BlackBerry client agent.

Several EMS components work together to enable wireless continuity functionality for BlackBerry devices:

- Prior to an activation, **SyncManager** 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. (See "[Synchronize RIM data:](#)" on page 111)
- The RIM **client agent**, installed on the BlackBerry device for each user, provides seamless email delivery and retrieval during outages. Administrators can deploy the agent by way of the policy management features of BES 4.0+ (deployment *over-the-air*) or through a hyperlink sent to the user through the EMS Admin Console. Users can use the hyperlink to manually download the client agent to their devices.

- 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 2-1](#) shows mail routing flow to BlackBerry devices during and after an activation of Email Continuity.

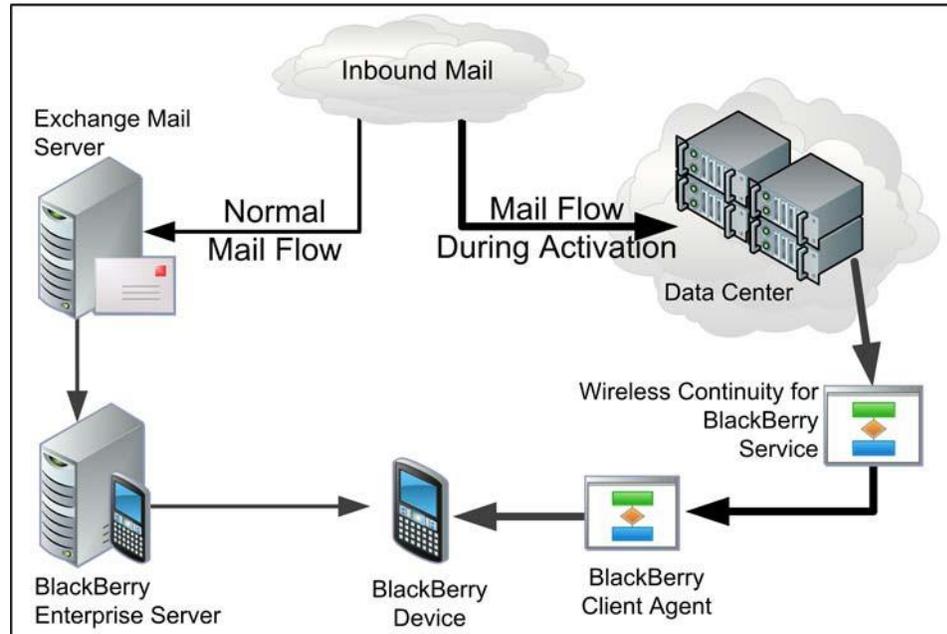


Figure 2-1 Wireless Continuity for BlackBerry Mail Flow

Wireless Continuity for BlackBerry supports:

- Viewing the text of Microsoft Word (.doc), Adobe PDF, and HTML attachments. Special formatting and images in these attachments cannot be displayed on the BlackBerry device.
- Viewing messages no larger than 64 KB in size (because of restrictions in the BlackBerry device software).
- If users 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 the user's Email Continuity webmail account.
- Partial activation of Email Continuity, if your organization has purchased that feature.

For more information on this feature, including limitations, see:

- ["Wireless Continuity for BlackBerry Prerequisites" on page 71](#)
- ["Deploy Wireless Continuity for BlackBerry" on page 111](#)

For more information, see ["Wireless Continuity for BlackBerry Administration" on page 221](#)

2.3. Email Continuity States

After you have installed the necessary components into your environment, using Email Continuity is simple. Email Continuity is always in one of three states: READY, ACTIVE, or RECOVERY. These are shown in [Figure 2-2](#).

- During the READY state, the **SyncManager** automatically sends directory information to the data center on a regular schedule.
- When set to the ACTIVE state by an administrator or Support representative, the system enables users to send and receive their email through the EMS Webmail interface, the Mobile Webmail interface or the Outlook Extension.

- When set to the RECOVERY state by an administrator or Support representative, you can use **RecoveryManager** to import messages sent and received during the activation period into your primary mail system. During recovery, users can access their messages using either the primary mail system or the continuity systems (Webmail, Mobile Webmail or Outlook Extension).

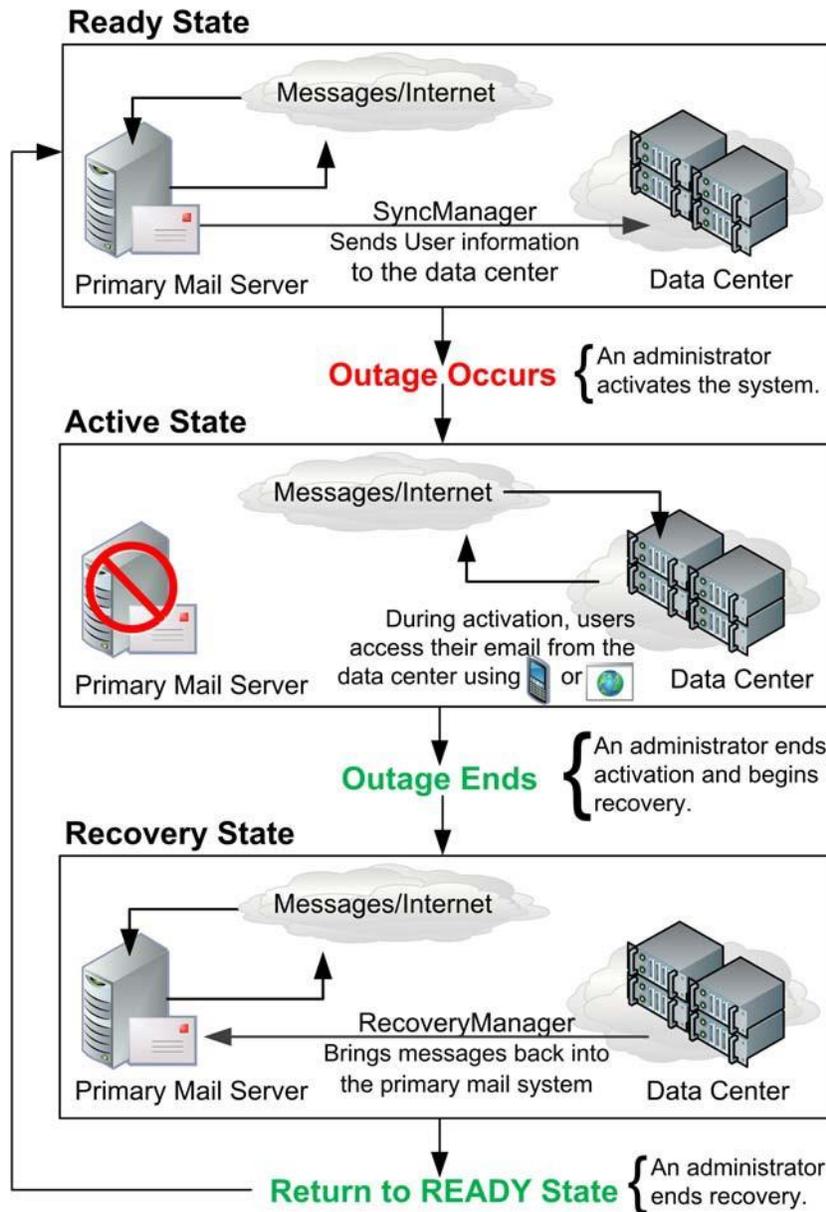


Figure 2-2 Email Continuity States

2.4. Email Continuity Administration

You can find details about all other Email Continuity functions and features in [Chapter 7., "Administer Email Continuity" on page 204](#)

3. About Historical Mail/Email Archive

Historical Mail/Email Archive captures both incoming and outgoing email messages and attachments for your organization and archives them to an off-site data center.

This chapter covers the following topics:

- ["About Historical Mail/Email Archive" on page 21](#)
- ["About Continuity Archive" on page 22](#)
- ["About Enterprise Archive" on page 23](#)
- ["About Storage Management" on page 25](#)
- ["About Import & Export Manager" on page 25](#)
- ["About Email Archive On-Premises Journaling" on page 26](#)
- ["About Failed Message Tracking" on page 27](#)
- ["About Folder Synchronization" on page 28](#)
- ["Email Archive Roles" on page 29](#)
- ["About Retention Policies" on page 30](#)
- ["About Email Recovery & Archives" on page 37](#)
- ["Historical Mail/Email Archive Administration" on page 40](#)

3.1. About Historical Mail/Email Archive

Historical Mail and Email Archive are both inclusive names for two features of the EMS Suite of products.

- Continuity Archive
- Enterprise Archive

Continuity Archive is the portion of the EMS suite that provides the ability to archive messages during an Email Continuity activation, when your normal email environment is unavailable, and to recover these emails back to the email environment. Continuity Archive allows administrators to capture and restore emails, and allows end-users to search captured emails during an Email Continuity activation. See ["About Continuity Archive" on page 22](#) for more information.

The Enterprise Archive portion of the EMS suite of products is independent of Email Continuity. Enterprise Archive allows email messages to be captured from your email environment and archived based on retention policies defined by EMS administrators. Once emails are archived, they can be searched by end-users and reviewers, and several kinds of archives can be created for both export and recovery into the normal email environment. See ["About Enterprise Archive" on page 23](#) for more information.

3.2. About Continuity Archive

Continuity Archive is a feature within Email Continuity.

Continuity Archive allows you to:

- **Capture and archive mail.** Continuity Archive captures and archives incoming and outgoing messages and attachments during Email Continuity activations.
- **Search archived mail.** After messages are available in the archive, they can be acted upon by users, and administrators. See ["Email Archive Roles" on page 29](#).
- **Recover archived mail.** Several types of recovery archives can be created, allowing messages to be recovered back to the Exchange servers. See ["About Email Recovery & Archives" on page 37](#) for more information.
- **Create and manage retention policies.** By configuring retention policies, administrators specify which messages should be archived, under what conditions, and for how long. See ["About Retention Policies" on page 30](#).
- **View storage reports.** Storage reports provide information on the amount of data stored in the archive under various retention policies. See ["Storage Reports" on page 270](#)
- **View audit reports.** Several Audit Reports are available which provide a log of audited events related to Continuity Archive. See ["View Historical Mail Audit Reports" on page 296](#)

During an Email Continuity activation, end-users can access Continuity Archive from:

- Webmail interface or the Email Archive sign-in page on the data center console. See *Email Management Services Email Continuity User Guide* and the *Email Management Services Email Archive User Guide*.
- Mobile Webmail browser-based interface or Mobile App. See *Mobile Access User Guide*
- Or, if the Outlook Extension has been installed, the end-user's Outlook experience is seamless during activation.

3.2.1. Continuity Archive Requirements

To use the Continuity Archive, you must:

- 1) Install and configure the following client-side components described under ["Client-Side Software" on page 2](#):
 - **SyncManager:** SyncManager is required to keep your primary mail environment and the data center synchronized. See ["About SyncManager" on page 4](#).
 - **Mail Redirector Components:** Redirector components are required to ensure that your mail is routed correctly during activation and recovery. See ["About Redirector Components" on page 5](#).

- **RecoveryManager:** RecoveryManager is required to bring all messages contained in an archive back into your mail environment. See ["About RecoveryManager" on page 7](#).
 - **VaultBox:** One or more VaultBoxes must be installed in your mail environment to capture, compress, and transfer messages to the data center. See ["About the VaultBox" on page 5](#).
- 2) Create one or more retention policies in the data center. Retention policies determine which messages are archived, under what conditions, and for how long. See ["About Retention Policies" on page 30](#).

3.3. About Enterprise Archive

Enterprise Archive is independent of Email Continuity and provides a much larger feature set, allowing greater flexibility in storing, searching, exporting and restoring email messages.

Enterprise Archive allows you to:

- **Capture and archive mail.** Enterprise Archive captures and archives incoming and outgoing messages and attachments based on the Retention policies defined.
- **Create and manage Retention policies.** By configuring retention policies, you specify which messages should be archived, under what conditions, and for how long. See ["About Retention Policies" on page 30](#).
- **Search archived mail.** After messages are available in the archive, they can be acted upon by users, and administrators. Enterprise Archive provides an enhanced feature set of search tools. See ["Email Archive Roles" on page 29](#).
- **Recover archived mail.** More types of recovery archives can be created, allowing messages to be recovered back to the Exchange servers. See ["About Email Recovery & Archives" on page 37](#) for more information.
- **Create reviewer groups to manage messages and archives.** Enterprise Archive lets administrators set up Reviewer Groups and designate Reviewers to review archived messages. Reviewers can create Discovery Archives to include all messages matching specific search parameters (such as `date`, `user`, or `keyword`).
- **Track Failed Mail.** Some email messages fail to archive properly. The Failed Message Tracking feature allows Reviewers and Administrators to search and export these emails. See ["About Failed Message Tracking" on page 27](#)
- **Envelope Journaling.** The Envelope Journaling feature allows email messages to be parsed based on the message's envelope, providing more details about the message. See ["About Email Archive On-Premises Journaling" on page 26](#)
- **Office 365 Support.** Environments in rich coexistence can enable archiving for Office 365 users. See ["About EMS Cloud Services" on page 305](#)

- **Synchronization of Outlook Folders.** The Folder Sync feature allows the Outlook folder structure (for their Exchange mailbox) to be preserved when email messages are archive. Allowing end-users to search for messages based on their Outlook folder structure. See ["About Folder Synchronization" on page 28](#)
- **Import and Export of Email.** Email messages can be imported into the archive and exported from the archive using the stand-alone Import Manager and Export Manager tools. See ["About Import & Export Manager" on page 25](#)
- **Storage Management.** Storage Management is a feature of Enterprise Archive that greatly reduces the amount of storage space required for retaining email messages. See ["About Storage Management" on page 25](#)
- **View storage reports.** More storage reports provide information on the amount of data stored in the archive under various retention policies. See ["Storage Reports" on page 270](#)
- **View audit reports.** More Audit Reports are available which provide a log of audited events related to Enterprise Archive. See ["View Historical Mail Audit Reports" on page 296](#)

Reviewers can access Enterprise Archive's *Search Company Archives* feature from:

- The Email Archive sign-in page on the data center console. See the *Email Management Services Email Archive Reviewer Guide*.

End-users and Reviewers can access Enterprise Archive's *Search Personal Mail* feature from:

- The Email Archive sign-in page on the data center console. See *Email Management Services Email Continuity User Guide* and the *Email Management Services Email Archive User Guide* and the *Email Management Services Email Archive Reviewer Guide*.
- Mobile Webmail browser-based interface or Mobile App. See *Mobile Access User Guide*
- Or, if the Outlook Extension has been installed, the end-user's Outlook experience is seamless.

3.3.1. Enterprise Archive Requirements

To use the standard features of Historical Mail, you must:

- 1) Install and configure the following client-side components described under ["Client-Side Software" on page 2](#):
 - **SyncManager:** SyncManager is required to keep your primary mail environment and the data center synchronized. See ["About SyncManager" on page 4](#).

- **Mail Redirector Components:** Redirector components are required to ensure that your mail is routed correctly during activation and recovery. See ["About Redirector Components" on page 5.](#)
 - **RecoveryManager:** RecoveryManager is required to bring all messages contained in an archive back into your mail environment. See ["About RecoveryManager" on page 7.](#)
 - **VaultBox:** One or more VaultBoxes must be installed in your mail environment to capture, compress, and transfer messages to the data center. See ["About the VaultBox" on page 5.](#)
- 2) Create one or more retention policies in the data center. Retention policies determine which messages are archived, under what conditions, and for how long. See ["About Retention Policies" on page 30.](#)
 - 3) If your organization uses Exchange Envelope Journaling, journaling address(es) must be configured to send messages to Email Archive. See ["About Email Archive On-Premises Journaling" on page 26.](#)

3.4. About Storage Management

If your organization purchases additional functions available with Enterprise Archive, your installation of Email Archive may also allow you to:

- **Create and manage storage management policies.** By configuring storage management policies, you can drastically reduce mailbox storage space needed for your organization. When enabled, storage management (also known as *stubbing*), keeps only a single copy of large attachments in storage and replaces all instances of those attachments in messages with HTML links.

To enable Storage Management, you must create one or more storage management policies. See ["Create Storage Management Policies" on page 264.](#)

- **Create and manage user classification retention policies.** User classification policies allow you to designate individual users responsible for identifying messages to store in the archive using designated Outlook folders.

To enable User Classification, you must create one or more User Classification retention policies. See the ["User Classification Retention Policies" on page 34.](#)

3.5. About Import & Export Manager

If your organization purchases additional functions available with Enterprise Archive, your installation of Email Archive may also allow you to:

- **Import older messages from local information stores into the archive.**

To import older messages from local information stores, you must contact Support to install the Import Manager application into your mail environment. See the *Import Manager Administrator Guide* for more information.

- **Export messages from the archive into data files.**

To export messages from the archive to data files which can be imported back into Exchange or into another archive, you must contact Support to install the Export Manager application into your mail environment. See the *Export Manager Administrator Guide* for more information.

3.6. About Email Archive On-Premises Journaling

Once existing EMS Client Servers, SyncManager and VaultBoxes are upgraded to a compatible Client software versions (EMS Client 6.6 or later), Email Archive On-Premises Journaling provides support for Exchange Envelope Journaling. Envelope journaling captures enhanced recipient information from the message envelope, including expanded distribution lists, BCC recipients and alternative recipient information.

Email Archive On-Premises Journaling provides enhanced metadata to Email Archive Reviewers and provides limited additional metadata to Email Archive Users. For example, Reviewers can see BCC recipients for all messages, whereas Users can only see BCC recipients for messages the user sent.

On-Premises Journaling is supported in both hybrid mode (where both journaled and traditional capture through Redirector Agent mailboxes coexist) and journaled-only mode. Envelope journaled messages can be sent directly to the Data Center instead of using a local VaultBox, depending on the configured environment.

- For EMS Email Archive only customers using journaled-only mode, VaultBoxes, Event Sink and Transport agents would no longer be required.
- For EMS Email Continuity customers, the Event Sink and Transport Agents are still required for partial activation.

To support journaling capture, the EMS client includes a Capture Policy Service that queries Active Directory to determine which Exchange users have been enabled for envelope journaling. Once it determines that a user is enabled for envelope journaling, that information is transmitted to the Data Center and EMS removes that user from Event Sink and the Transport Agent replication lists to reduce the possibility of messages being archived twice. Also, the list of envelope-journaling-enabled users is compared to existing retention policies to help ensure that customers who are members of an EMS data retention policy are also enabled for Exchange journaling.

On-Premises Journaling differs from Cloud Journaling (see ["About EMS Cloud Services" on page 305](#)) in that On-Premises Journaling applies to Exchange users and Exchange servers located within the customer's data center (on-premises). Cloud Journaling

applies to Office 365 users whose messages are forwarded to Email Archive from the Office 365 cloud. Customers who have Office 365 users in rich coexistence can use envelope journaling on-premises and within Office 365. These policies are managed within the Exchange management Console and Office 365 Administration Console respectively.

3.7. About Failed Message Tracking

Failed Message Tracking is an optional feature that displays email messages that have failed to be stored in the archive or fully indexed into the database.

Messages may fail because:

- The message cannot be associated with a customer.
- The message is larger than the maximum size limit. (approx. 1 GB)
- The message, either partially or fully, failed to be indexed into the database.

When an email message arrives, EMS normally parses the message for metadata and other information, then stores the message in the archive and sends the metadata to be indexed by the server.

If the message cannot be stored correctly the first time, several more attempts are made to store the message into its archives. If, after repeat attempts, the message cannot be stored into the archives, its metadata is entered into the Failed Message database.

After a message stores correctly, it is sent to be indexed. Again, several attempts are made to index each message. If a message cannot be indexed at all, or can only be partially indexed, its metadata is also placed into the Failed Message database.

EMS administrators whose company has the Failed Message Tracking feature enabled by Support can access the Failed Message Tracking functionality through menu items on the EMS Administration Console.

Email Archive Reviewers can access the feature from both the EMS home page, and from the Email Archive menu.

3.7.1. Failed Message Tracking Additional Information and Limitations

- In the case of the very small minority of messages whose metadata is so corrupt that an association with a Reviewer Group is not possible, that message will not be displayed on the Failed Message Tracking page, unless the scope of the Reviewer Group specified is `All Users`.

- Depending on what time of day a message storage or indexing failure occurs (relative to UTC), the Failed Message Tracking search count (which uses local time) may differ from the Daily Message Volume Failed Message Count chart value (which uses UTC time). The counts are not lost, just rolled into the next day.

3.8. About Folder Synchronization

Folder Synchronization is an optional feature that allows Email Archive users to view their Outlook folder hierarchy (for their Exchange mailbox) in the archive search interface and use the hierarchy when executing searches. If you have users who rely heavily on folders for organizing information, enabling this feature for them can prove beneficial. Many organizations choose to only enable this feature for a subset of users, to minimize bandwidth usage and server load.

Folder Synchronization is not a real-time process, especially when initially enabled. There will be a time delay between a user moving an email to a folder and that change being displayed on the Email Archive search page.

Call Support to enable this feature.

3.8.1. Folder Sync Additional Information and Limitations

- The minimum client software version required to implement folder synchronization is EMS Client 6.9.1.
- Folder Synchronization utilizes Exchange Web Services (EWS), therefore is only applicable to mailboxes that are on Exchange 2007 (SP1+), Exchange 2010, and Exchange 2013.
- When Folder Sync is enabled for a user, it will perform a full sync, which depending on your environment may take a while to complete. Subsequent syncs for that mailbox will update only differential data.
- The default maximum number of items per folder that are synced (per sync run) is 2000 items. If folders contain more items, multiple passes of Folder Sync will retrieve the remaining items.
- By default the folder sync process can run 24x7, but exclusion hours can be configured in the registry. See (reference) for more information.
- Excluded Outlook folders are: [Inbox¹](#), Drafts, Outbox, [Sent Items¹](#), Deleted Items¹, Conflicts, Local Failures, Server Failures, Sync Issues, Contacts, Calendar, Suggested Contacts.
- If a user copies an item from the Sent folder to any other Exchange folder, Folder Sync will not have a record of that message, because the message ID changes when the message is moved.

1. For this folder, the top-level folder itself will not be synced, but email messages in its child folders will be synced by Folder Sync.

- Folder hierarchies may appear in the Email Archive search interface before the contents of the folder have been fully synchronized. These folders are not searchable until the full synchronization has been completed.

3.9. Email Archive Roles

There are three basic roles within Email Archive, each of which have different levels of access and responsibility:

- **Administrators**, who are responsible for:
 - Creating and managing retention policies. See ["About Retention Policies" on page 30](#).
 - Creating and managing storage management policies. See ["Storage Management" on page 261](#).
 - Creating reviewer groups and assigning reviewers to reviewer groups. See ["Reviewer Groups" on page 247](#).
 - Creating Recovery Archives to restore messages processed during specified time periods. See ["Create and Recover Archives" on page 275](#).
 - Recovering archives back to user mailboxes using RecoveryManager. See ["Use RecoveryManager to Restore Archives" on page 280](#).
 - Viewing archive audit reports. See ["View Historical Mail Audit Reports" on page 296](#)
- **Reviewers**, who can:
 - Search through your organization's stored mail
 - Create Discovery Archives
 - Apply Query-Based Retention Holds to messagesSee the *Email Archive Reviewer Guide* and ["Reviewer Groups" on page 247](#).
- **Users**, who can:
 - Search their own message archives and forward a single message at a time from the archive to themselves as an attachment.

See the *Email Archive User Guide*.

3.10. About Retention Policies

Retention policies determine the length of time messages are stored in the archive, for which users, and under what conditions. If no specific 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. The eligibility date is determined by retention policy settings, starting with the date the message was received. Purging is performed in the data center; you may notice a delay between the date a message must no longer be kept according to the governing policy and the date it disappears from the server.

CAUTION Update Retention Policies For Reinstalled VaultBoxes

When updating from 6.4.x to 6.4.4 or higher, no additional steps are required.

For all other updates, when you uninstall and reinstall a VaultBox, you must manually update any retention policies that were associated with that VaultBox using the EMS Admin Console.

Until you reassociate the policies, new VaultBox will be unable to process messages for those policies and no messages from that VaultBox will be sent to the archive.

To do this, log into the EMS Admin Console and select the VaultBox that has been reinstalled. View the list of retention policies for the VaultBox, and for each policy, click **Edit**, then **Save**. You do not have to make any changes to the policies, just manually edit and save them. This step will reassociate the policies with the reinstalled VaultBox and messages will be processed.

You can configure several types of retention policies to meet your organization's message retention needs. See "[Retention Policy Best Practices](#)" on page 31 for information pertinent to all retention policies.

- "[Membership-Based \(Current Membership\) Policies](#)" on page 32
- "[Capture-Based Policies](#)" on page 33
- "[User Classification Retention Policies](#)" on page 34
- "[Query-Based Retention Holds](#)" on page 37

For information on working with retention policies using the EMS Admin Console, see "[Manage Retention Policies](#)" on page 237.

NOTE Retention Policy Based on Received Date

The date used in establishing and managing a message's retention policy behavior is the email message's received date.

3.10.1. Retention Policy Best Practices

Retention policies should be carefully constructed and implemented so as to achieve 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 (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.

- **Email Archive settings do not override mail server settings.**

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

- **Higher priority policies always override lower priority policies, even those of longer 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 the `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.

To avoid unintentional purging of messages intended to be retained for a longer period, ensure that policies with longer durations are prioritized higher than those with shorter durations.

Table 3-1 Example Retention Policies and Priorities

| Retention Policy Name | Retention Period | Priority in EMS Admin Console | Result |
|-----------------------|------------------|-------------------------------|---|
| Executive | 3 years | 1 | Messages tagged under the <code>Executive</code> retention policy are kept for 3 years. |
| Legal | 5 years | 2 | <p>Messages tagged under the <code>Legal</code> retention policy are kept for 5 years.</p> <p>Because this policy has a lower priority than the <code>Executive</code> policy, messages tagged under both policies are kept for only 3 years.</p> <p>To keep messages tagged under both policies for the longer duration, reverse the priority in the EMS Admin Console so that the longer duration policy has a higher priority.</p> |

- **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 (*stubby*) components, there should be at least one week duration overlap to ensure that no items set to be stubbed will be deleted before stubbing. For example, if Storage Management is set to start at 30 days, basic retention duration should be set to at least 37 days. See "[Storage Management](#)" on page 261 for more details.

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

Membership-Based policies are appropriate for retaining messages for retention holds. They are not an adequate substitute for capture-based policies.

3.10.2. Membership-Based (Current Membership) Policies

Under *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 30 days. On the first day that the user is a member of the `Assistant Group`, mail collected during days 31-50 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.

3.10.3. Capture-Based Policies

Under 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 tags all messages received after the user has been added, but does not retroactively associate 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 261.

3.10.4. 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. Your organization's mail administrators create custom folders within the users' 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 the user classification feature.

To configure a user classification retention policy, you must:

- 1) In your mail system, create the user classification directory that email users must use to store the messages to be archived. You can do this manually, before you create the policy in the EMS Admin Console, or you can create it automatically when you create the policy in the EMS Admin Console.
- 2) Using the EMS Admin Console, create the user classification policy, including its priority and duration. See "[Create Retention Policies](#)" on page 237 to create the policy.
- 3) Using the EMS VaultBox Console, set a task schedule for the user classification policy. See "[Configure Manual Retention \(User Classification\) Task schedule settings:](#)" on page 128 for information on setting the task schedule.

In addition to the best practices for all retention policies listed under "[Retention Policy Best Practices](#)" on page 31, adhere to the following best practices for user classification policies:

- **Default retention period:** Retention for user classification retention policies should be set no fewer than 30 days.
- **Folders and subfolders:** When a folder is tagged with a user classification retention policy, all subfolders are included. For example, a policy scanning the folder `Inbox\Legal` will also scan and tag messages in `Inbox\Legal\CaseA` and any other subfolders.
- **Subfolders with different retention periods/priorities:** If a subfolder has a different retention period than its parent folder, messages will be purged according to the priorities assigned to each retention policy as set in the EMS Admin Console.

A best practice is to prioritize retention policies the EMS Admin Console from the longest duration to the shortest, such as in the following example. In this case, messages in the `CaseB` folder are retained for 7 years, those in the `CaseA` folder are retained for 3 years, and those in the top-level `Legal` folder are retained for 2 years.

Table 3-2 Example User Classification Policies and Priorities: Correct

| Folder | Retention Period | Priority in EMS Admin Console | Result |
|--------------------------------|------------------|-------------------------------|---|
| <code>Inbox\Legal\CaseB</code> | 7 years | 1 | Messages in the <code>CaseB</code> folder and its subdirectories will be retained for 7 years. |
| <code>Inbox\Legal\CaseA</code> | 3 years | 2 | Messages in the <code>CaseA</code> folder and its subdirectories will be retained for 3 years. |
| <code>Inbox\Legal\</code> | 2 years | 3 | Messages in the top-level <code>Legal</code> folder and any subdirectories <i>other than</i> <code>CaseA</code> or <code>CaseB</code> will be retained for 2 years. |

However, if you created user classification folders, durations, and priorities as in the example below, *all messages* under `Inbox\Legal\` will be purged after 2 years because of the priority order assigned to each folder, regardless of the longer durations assigned to the subfolder policies.

Table 3-3 Example User Classification Policies and Priorities: Incorrect

| Folder | Retention Period | Priority in EMS Admin Console | Result |
|-------------------|------------------|-------------------------------|--|
| Inbox\Legal\ | 2 years | 1 | Because the <code>Legal</code> policy has the highest priority, all messages under <code>Inbox\Legal\</code> and its subdirectories will be purged after 2 years, regardless of the durations assigned to subdirectory policies. |
| Inbox\Legal\CaseA | 3 years | 2 | |
| Inbox\Legal\CaseB | 7 years | 3 | |

- When a message is tagged under multiple user classification policies (most commonly by being moved from one user classification folder to another), the previous user classification policy tag remains on the message. For example, if a message is moved from the `CaseB` folder (with a 7 year retention period) to the top-level `Legal` folder (with a 2 year retention period), the message retains both tags and will not be purged until the 7 year duration for `CaseB` expires (unless the `CaseB` policy itself is removed).
- Policy tags remain on messages even after they are deleted from a user classification folder. For example, if a message is deleted from the `CaseB` folder, it remains tagged and is not purged until the 7 year duration for `CaseB` expires.
- Versioned policy tags are reapplied to messages any time the policy is changed, such as adding/removing users from the policy or changing policy duration. The Email Archive Harvester component will retag messages that meet the new policy criteria with an updated version of the policy tag.
- If a message needs to be tagged under multiple policies, you can use two methods:
 - a. The preferred method is to leave the message in a folder until the Harvester has had time to scan the folder and pick up the message. The time required for this to happen depends on how your organization's Email Archive administrator has scheduled the Harvester's full and incremental scans. After the Harvester has tagged the message in its original user classification folder, the message can be moved to another folder to be tagged again during the next Harvester scan. The message must remain in each folder until the Harvester has scanned and tagged the message under its new policy.
 - b. A second method is to drop copies of messages in multiple folders to ensure that they are tagged in each location for each user classification policy. Be aware that this creates multiple copies of the message in the archive and may decrease performance and the size of the archive, and is not recommended for most situations.

3.10.5. Query-Based Retention Holds

Administrators who are also Email Archive Reviewers can create query-based retention holds on collections of mail resulting from Archive Searches. Query-based retention holds work similarly to retention policies, except:

- Query-Based Retention Holds are created on the **Review Company Email Archives** screen rather than the EMS Admin Console.
- The Reviewer identifies and selects the messages to be archived under a Retention Hold policy.
- The messages are saved until the Retention Hold is deleted by an Administrator, rather than a set number of days.
- If the Reviewer has checked the **Automatically retain new messages** checkbox when creating the Retention Hold, all new incoming messages that match the criteria for the Retention Hold will be added to the Retention Hold

See ["Query-Based Retention Holds" on page 244](#) and ["Use Retention Policies to Simulate Retention Holds" on page 246](#).

3.11. About Email Recovery & Archives

Email messages can be exported from the archive to satisfy a variety of use cases. Different archive types may be created depending on the use-case, and use different tools depending on the type.

3.11.1. Time-Based Recovery Archives

Email Archive also allows you to create **Time-Based Recovery Archives**, which can be used to recover all mail sent and received during a specified time period. You create Time-Based Recovery Archives in the EMS Admin Console and restore them using RecoveryManager. See ["Time-Based Recovery Archives" on page 275](#).

Example: The mail server crashed last night, wiping out the last 12 hours of email before it could be delivered. An archive administrator logs into the EMS Admin Console and creates a Time-Based Recovery Archive for all mail during that 12 hour period, allowing all mail to be delivered to user mailboxes the next day.

3.11.2. Activation-Based Recovery Archives

Email Archive also allows you to create **Activation-Based Recovery Archives**, which can be used to recover all mail sent and received during a time period prior to the beginning of an activation. Similar to a standard time-based recovery archives, the end

time of an Activation-Based Archive is bounded by the point at which the activation occurred. You create Activation-Based Recovery Archives in the EMS Admin Console and restore them using RecoveryManager. See "[Activation-Based Recovery Archives](#)" on [page 277](#)

Example: The mail server crashed last night, and several hours later, administrators determined it will take a significant amount of time to resolve the problem. At which point, EMS administrator initiated an Activation to re-route users' emails for the duration. While the mail servers are being fixed, an Email Archive administrator can log into the EMS Admin Console and create a Activation-Based Recovery Archive for all mail during the time period between the crash and the beginning of the activation, allowing all mail to be delivered to user mailboxes the next day.

3.11.3. Search-Based Recovery Archives

Email Archive also allows administrators with Reviewer privileges and Super- Admins to create **Search-Based Recovery Archives**, which can be used to recover all mail that meets the search criteria. You create Search-Based Recovery Archives in the Email Archive Reviewer interface and restore them using RecoveryManager. See "[Search-Based Recovery Archives](#)" on [page 279](#) and *Email Archive Reviewer Guide* for more information.

3.11.4. Discovery Archives

Discovery Archives contain email bundled into archives by reviewers using the query features of Email Archive. Using a simple web-based interface, Email Archive Reviewers create Discovery Archives containing messages found during archive searches. Reviewers can search using either a simple query interface or by writing the query directly in the query language. Once they have specified the criteria for the messages to be retained, they save the query results to create the Discovery Archive.

After a Reviewer creates a Discovery Archive, an administrator can recover the messages identified by the archive into a single mailbox or into multiple users' mailboxes using the RecoveryManager application or the messages can be exported to PST or EML files using Export Manager.

When you recover a Discovery Archive, you are not pulling up a static set of email, but rather pulling up all email in the archive that matches reviewer-specified query criteria *when the recovery is run*. For more information on creating a Discovery Archive, see the *Email Archive Reviewer Guide*.

Example 1: Management wants to review old contract discussions in advance of negotiating a contract renewal with Genericorp. A reviewer creates a Discovery Archive of all messages containing the words `Genericorp` and `contract` during the period of time when the original contract was negotiated two years before for management to read.

Example 2: No one can find a schematic that was mailed to a customer by Drafter Bob Smith, who retired six months ago. Since Bob's messages were archived under a retention policy, a reviewer creates a Discovery Archive of all attachments from Bob Smith that have the word `Schematics` in the name so it can be recovered to the mailbox of the new drafter.

Example 3: The hard drive of a CEO has crashed, erasing all his locally stored messages. As he was covered by a 10 year retention policy, a reviewer creates a Discovery Archive of all the CEO's email during the covered period so it can be restored to his new computer.

3.11.5. Failed Message Archive

Email Archive Reviewers can create Discovery Archives based on queries of the Failed Message Tracking database. These archives can be exported using Export Manager, like normal Discovery Archives. These archives can also be imported using Recovery Manager.

Administrators can view a listing of these archives, along with all other Discovery and Recovery Archives on the ***Historical Mail > Email Recovery*** page.

When Email Archive Reviewers no longer need a Failed Message Archive, an administrator can delete the archive like a normal Discovery Archive.

3.11.6. Email Continuity Recovery Archives

Email Continuity Recovery Archives are created during an Email Continuity Activation and contain all the messages sent and received by all activated users during the length of the activation. During the end-of-activation recovery process, RecoveryManager is used to restore the archive's emails to all effected users' mailboxes. See ["Restore Mail to Users' Mailboxes" on page 208](#)

NOTE **Email Continuity Recovery Archives Are Purged After 30 Days**

Email Continuity Recovery archives are available for 30 days after they are created. After that time, they are purged and are no longer available. Be sure that you complete the recovery process within 30 days of creating the recovery archive.

3.12. Historical Mail/Email Archive Administration

You can find details about all other Historical Mail functions and features in [Chapter 8., "Administer Historical Mail/Email Archive" on page 235.](#)

4. EMS Controller and Environment Prerequisites

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

- 1) ["Prerequisites for All Installations" on page 41](#)
 - ["Communications Prerequisites" on page 42](#)
 - ["Hardware Requirements" on page 46](#)
 - ["User Permissions Requirements" on page 47](#)
 - ["Software Requirements" on page 47](#)
 - ["Virtualization" on page 56](#)
- 2) ["Prerequisites for Optional Features" on page 56](#)
 - ["Redirector Component Prerequisites" on page 57](#)
 - ["On-Premises Journaling Prerequisites and Limitations" on page 60](#)
 - ["Stored/Archived Mail Prerequisites" on page 61](#)
 - ["Windows Authentication Prerequisites" on page 66](#)
 - ["Outlook Extension Prerequisites and Limitations" on page 67](#)
 - ["Wireless Continuity for BlackBerry Prerequisites" on page 71](#)
 - ["Folder Sync Prerequisites" on page 77](#)

4.1. Prerequisites for All Installations

Before installing or using Email Management Services, ensure that your operating systems, networks, mail systems, and all other dependencies are updated with the latest patches and updates and working correctly. Email Management Services is not a substitute for a fully functional primary mail system.

All client installations of service software must meet all prerequisites found in the following sections:

- ["Communications Prerequisites" on page 42](#) (including networking, firewall, proxy, gateway, and routing requirements)
- ["Hardware Requirements" on page 46](#)

- ["Software Requirements" on page 47](#) (including operating system, messaging software, and user account requirements)
- ["Virtualization" on page 56](#)

4.1.1. Communications Prerequisites

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

MessageOne 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.

4.1.1.1. Networking Requirements

The networking requirements are:

- 1) The machine on which you install the SyncManager (called the *primary controller* or *EMS server*) must have internet access through secure hypertext transfer protocol (HTTPS), using port 443 outbound.
- 2) Connection to the internet and a browser for performing functions in the EMS Admin Console. (See ["Supported Browser Software" on page 48.](#)) If you are installing on a new machine, run the Microsoft Internet Connectivity Wizard before you install service software.
- 3) For end users accessing the webmail interface, supported browsers are listed at ["Supported Browser Software" on page 48.](#))

4.1.1.2. 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 EMS server to the location-specific IP addresses on port 443.

4.1.1.3. Proxy Requirements

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

4.1.1.4. 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.

4.1.1.5. Mail Routing Requirements — Inbound for Email Continuity

It is vital that a mechanism for routing mail to Email Continuity is included when your primary mail system is unavailable. This mechanism *must* exist outside of your on-site messaging solution, to ensure that mail flow will be maintained even if a complete loss of on-site mail routing capabilities is experienced.

If a third-party gateway is not used to filter email outside of your organization, you must include an alternative mechanism for routing messages to EMS. Please be aware that if you list the EMS failover publicly, you will likely experience a significant level of unwanted mail content as the Email Continuity failover does not filter for spam.

To add this data to your organization's DNS records, add an MX record using the syntax shown in [Table 4-1](#).

Table 4-1 MX Record Syntax

| Domain | MX Preference | Host Name |
|-------------|--------------------|---|
| Syntax | | |
| company.com | MX preference = 5 | mail exchanger = mail11.company.com |
| company.com | MX preference = 10 | mail exchanger = [location-specific MTA from Support] |

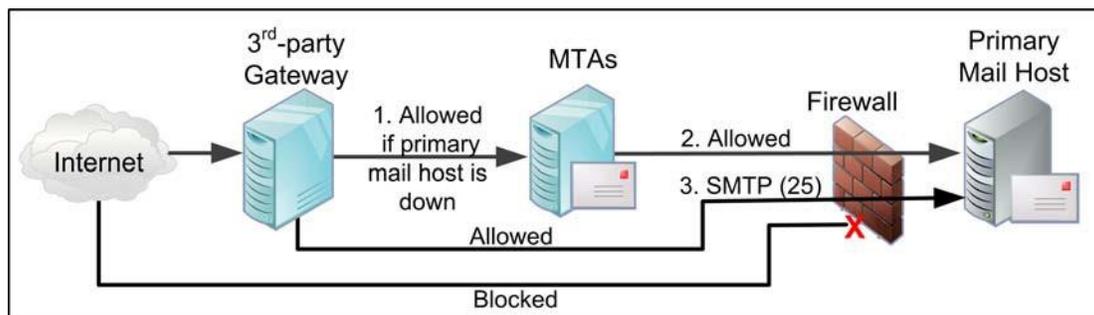
4.1.1.6. Third-party Gateway Requirements

If you use a third-party email gateway, configure it to failover automatically to the location-specific message transfer agent (MTA).

When using a third-party email gateway, configure your corporate mailhost to:

- 1) Accept inbound SMTP connections from the EMS IP addresses provided by Support.
- 2) Configure the EMS IP addresses provided by Support to be a trusted forwarder, but not safe-listed.

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 third-party gateway 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 third-party gateway 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) from the Email Continuity servers. This rule is the same as the firewall rule that allows inbound mail from the third-party gateway.

Figure 4-1 Mail Routing with Third-Party Gateway

4.1.1.7. Mail Routing Inbound — Store and Forward

If your primary mail system has gone down, and your organization has not activated Email Continuity, MessageOne performs a *store and forward* service and attempts to deliver your mail. By default, it tries to deliver mail to your system using the MX records for your organization, in priority order. However, if you use a third party filtering service (or for some other reason your organization's MX records point to an address other than your organization's), the service allows you to configure designated hosts (using hostnames or IP addresses) to which email is sent.

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 Policies for Forwarded Mail" on page 187](#).

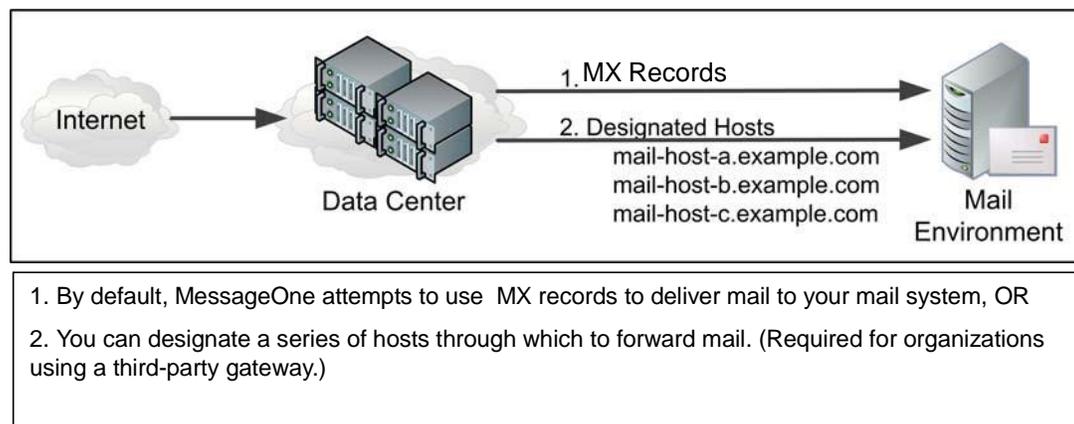


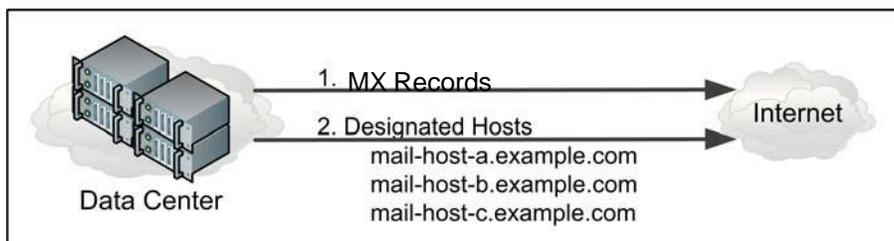
Figure 4-2 Routing for Inbound (Forwarded) Mail

4.1.1.8. Mail Routing — Outbound During Activation

By default, when Email Continuity is active, it uses the MX records of mail recipients to deliver outgoing mail.

However, if your organization uses a third-party provider for security (or other features), or if you want to route outgoing mail through a different host, Email Continuity can be configured to use a designated series of hostnames or IP addresses (*hops*) to determine the path the outgoing email takes while Email Continuity is active. To configure the series of hosts, see "[Routing for Outbound Mail During an Activation](#)" on page 189.

Figure 4-3 Outbound Mail Routing During Activation



4.1.2. Hardware Requirements

Verify that the server you plan to use as the primary controller (the *EMS server*) meets the following minimum hardware requirements:

Table 4-2 Minimum Hardware Requirements, EMS Service Software Host Machines

| Component | Minimum Required |
|------------|---|
| Processor | Speed of 2 GHz or greater |
| Memory | 2 GB or greater |
| Disk Space | 40 GB or more, depending on the number of users |

NOTE Additional Hardware Requirements for Stored Mail/Email Archive Features

If your organization will use any stored mail/archive features, also note the hardware requirements for VaultBox machines listed under "[VaultBox Hardware Requirements](#)" on page 61.

NOTE Software Installation on Dedicated Server Is Recommended

Although a dedicated server is not typically required for the EMS Controller, it is highly recommended that the EMS software be installed on its own physical or virtual server in order to prevent unintended impacts from other applications.

4.1.3. User Permissions Requirements

To perform EMS installation, the user must BE:

- A member of the domain.
- Assigned appropriate send-as and receive-as permissions.
- *Not* a domain administrator (highly recommended)
- A local administrator on the EMS server.

4.1.4. Software Requirements

Both the EMS Server and the VaultBox system require Windows Installer 4.5 or later.

Before you begin an installation, you must install each required software component on the EMS server. Which components you need depend on the email environment you use and which EMS features your organization will use. A Support representative will provide an appropriate software package and walk you through the actual installation process when the preinstallation requirements have been met.

4.1.4.1. Supported Operating Systems

The EMS server must use one of the operating systems described in [Table 4-3](#).

Table 4-3 Supported Operating Systems

| Server | Operating System |
|---|--|
| Email Management Services Server and One or more VaultBox systems | <ul style="list-style-type: none"> • Windows Server 2008, 32-bit or 64-bit • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 |
| One or more VaultBox systems | <ul style="list-style-type: none"> • Windows Server 2008, 32-bit or 64-bit • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 |

4.1.4.2. Supported Messaging Software

The EMS server requires the following versions of Microsoft Exchange Server:

- Microsoft Exchange Server 2003
- Microsoft Exchange Server 2007
- Microsoft Exchange Server 2010
- Microsoft Exchange Server 2013
 - Due to a bug in SP1 for Exchange 2013 that breaks third-party Transport Agents, the following Microsoft hot fix should be installed immediately after installing SP1: <http://www.microsoft.com/en-us/download/details.aspx?id=42065>

And supports the following versions of Microsoft Outlook:

- Microsoft Outlook 2003
- Microsoft Outlook 2007
- Microsoft Outlook 2010
- Microsoft Outlook 2013

4.1.4.3. Supported Browser Software

The following browsers are currently supported:

Table 4-4 Supported Browsers

| EMS Component | Supported Browser |
|---|---|
| EMS Administration Console Classic Email Archive Interface | Internet Explorer 6, 7 and 8 Firefox 8+ |
| New Email Archive Interface | Internet Explorer 8, 9 and 10 Firefox 16+ |
| Email Continuity Webmail | Internet Explorer 8, 9, 10 and 11 Firefox 8+ (latest verified version: 26) Safari 5, 6, 7 Chrome 31+ |

While not specifically supported, access via other browsers and versions is also available.

4.1.4.4. Additional Software Required for the EMS Server

Table 4-5 Software Requirements for Exchange Environments

| Software | Notes |
|---|--|
| Email Management Services Server | |
| .NET Framework v. 4.5 | If not already present on the EMS 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 EMS 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 (08.03.0.8309 or newer) | Download from Microsoft |
| Microsoft Internet Information Server (IIS) and simple mail transfer protocol (SMTP) | To use Historical Mail, you must have IIS services, including SMTP, enabled and configured for anonymous authentication. |
| Microsoft Outlook Messaging and Collaboration client must NOT be installed. | |
| Exchange Server 2013 | |
| Bug introduced in SP1 breaks third-party Transport Agents | The following Microsoft hot fix should be installed immediately after installing SP1: http://www.microsoft.com/en-us/download/details.aspx?id=42065 |
| Exchange Server 2007 & 2010 | |
| If the Exchange 2007/2010 server was not installed with support for pre-Outlook 2007 clients, you must create a Public Folder store | Refer to Microsoft's website for detailed instructions: <ul style="list-style-type: none"> • Exchange 2010 • Exchange 2007 |
| Configure Offline Address Book for Outlook 2003 and earlier clients. | |
| Exchange 2003 Servers | |
| Requires WMI Windows Installer Provider | |

4.1.4.5. Active Directory Service Account Requirements

An *Active Directory Service Account*, an Active Directory user account under which all EMS service processes run. This user account must be created on the EMS server.

This Active Directory Service Account user must be a member of:

- The domain in which the EMS server is installed
- A local administrator group on the EMS server

To insure product reliability and performance, it is our official recommendation that the Active Directory Service Account used be dedicated to EMS and not shared with any other applications.

Further, the Active Directory Service Account requirements may vary between Exchange versions, and between single Exchange configuration environments and coexistent Exchange environments, as detailed in [Table 4-6, "Active Directory Service Account Permission Requirements per Exchange Server version" on page 50](#).

Table 4-6 Active Directory Service Account Permission Requirements per Exchange Server version

| Exchange Version | Permissions/Memberships/Notes |
|------------------|---|
| Exchange 2003 | <p>The EMS Active Directory Service Account must have the following permissions:</p> <ul style="list-style-type: none"> • Exchange Admin permissions at the Organization level. See "Task 4.1." on page 53 • Send As and Receive As permissions on each mailbox store. See "Task 4.2." on page 53 • Local Administrator permissions on the Exchange server is required for remote deployment of RedirectorSinks using the RedirectorManager. You could also deploy RedirectorSinks using a different account that has local administrator permissions. |
| Exchange 2007 | <p>The EMS Active Directory Service Account must be a member of the following Exchange security group:</p> <ul style="list-style-type: none"> • Exchange Organization Administrator <p>The EMS Active Directory Service Account must have the following permissions:</p> <ul style="list-style-type: none"> • Send As and Receive As permissions on each mailbox store. See "Task 4.3." on page 54 |

Table 4-6 Active Directory Service Account Permission Requirements per Exchange Server version

| Exchange Version | Permissions/Memberships/Notes |
|------------------|---|
| Exchange 2010 | <p>The EMS Active Directory Service Account must be a member of the following Exchange security groups:</p> <ul style="list-style-type: none"> • Organization Management • Recipient Management <p>The EMS Active Directory Service Account must have the following permissions:</p> <ul style="list-style-type: none"> • Send As and Receive As permissions on each mailbox store. See "Task 4.3." on page 54 |
| Exchange 2013 | <p>The EMS Active Directory Service Account must be a member of the following Exchange security groups:</p> <ul style="list-style-type: none"> • Organization Management • Recipient Management <p>The EMS Active Directory Service Account must have the following permissions:</p> <ul style="list-style-type: none"> • Send As and Receive As permissions on each mailbox store. See "Task 4.3." on page 54 |

Table 4-6 Active Directory Service Account Permission Requirements per Exchange Server version

| Exchange Version | Permissions/Memberships/Notes |
|---|---|
| Coexistent Exchange 2003/2007/2010 Environments | <p>In Exchange 2003, the <code>Local Administrator</code> permissions on the Exchange server is required 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.</p> <p>In Exchange 2007, the EMS Active Directory Service Account must be a member of the following Exchange security group:</p> <ul style="list-style-type: none"> • <code>Exchange Organization Administrator</code> <p>In Exchange 2010, the EMS Active Directory Service Account must be a member of the following Exchange security groups:</p> <ul style="list-style-type: none"> • <code>Organization Management</code> • <code>Recipient Management</code> <p>The EMS Active Directory Service Account must have the following permissions:</p> <ul style="list-style-type: none"> • <code>Send As</code> and <code>Receive As</code> permissions on each mailbox store. See "Task 4.2." on page 53 and "Task 4.4." on page 54 <p>If you upgrade to Exchange 2010 from Exchange 2003 or 2007 with an existing EMS installation, the EMS Active Directory Service Account permissions should migrate during the upgrade.</p> <p>If you deploy a new Exchange 2010 server without an existing EMS installation, you must grant Administrator permissions to the EMS Active Directory Service Account by using either Active Directory Users and Computers or Exchange Control Panel (ECP) (in the Client Access Server, usually found at <code>https://CASServerName/ecp</code>).</p> |

Table 4-6 Active Directory Service Account Permission Requirements per Exchange Server version

| Exchange Version | Permissions/Memberships/Notes |
|---|---|
| Coexistent Exchange 2007/2010/2013 Environments | <p>In Exchange 2007, the EMS Active Directory Service Account must be a member of the following Exchange security group:</p> <ul style="list-style-type: none"> • Exchange Organization Administrator <p>In Exchange 2010 and 2013, the EMS Active Directory Service Account must be a member of the following Exchange security groups:</p> <ul style="list-style-type: none"> • Organization Management • Recipient Management <p>The EMS Active Directory Service Account must have the following permissions:</p> <ul style="list-style-type: none"> • Send As and Receive As permissions on each mailbox store. See "Task 4.5." on page 55 <p>If you upgrade to Exchange 2010 from Exchange 2003 or 2007 with an existing EMS installation, the EMS Active Directory Service Account permissions should migrate during the upgrade.</p> <p>If you deploy a new Exchange 2010 server without an existing EMS installation, you must grant Administrator permissions to the EMS Active Directory Service Account by using either Active Directory Users and Computers or Exchange Control Panel (ECP) (in the Client Access Server, usually found at https://CASServerName/ecp).</p> |

Task 4.1. Grant Exchange administrator permissions for Exchange 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 EMS 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 EMS Active Directory Service Account displays *inherited*. If, after 15–20 minutes, this is still not displayed, add the EMS account to each administrative group.

Task 4.2. Grant 'Send As' and 'Receive As' permissions for Exchange 2003:

- 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 EMS 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 2003 server.

Task 4.3. Grant 'Send As' and 'Receive As' permissions in Single Environment Exchange 2007, 2010 or 2013 Configurations

- 1) Link to Microsoft's instructions
 - Exchange 2007: [Link to Instructions](#)
 - Exchange 2010/2013: [Link to Instructions](#)
- 2) **Note:** The account used to **set** these permissions must be an Exchange Organizational Administrator or the permissions will not propagate. Not all domain administrators have this right.
- 3) The Shell command to use is:

```
Get-Mailboxdatabase | Add-ADPermission -User [Service Account] -ExtendedRights "Send As","Receive As"
```

Where [Service Account] = display name of EMS Active Directory Service Account.

- 4) Plan at least two hours for permissions to propagate.

Task 4.4. Grant 'Send As' and 'Receive As' permissions in Exchange 2003/2007/2010 Coexistent Configurations

- 1) Link to Microsoft's instructions
 - Exchange 2007: [Link to Instructions](#)
 - Exchange 2010: [Link to Instructions](#)
- 2) **Note:** The account used to **set** these permissions must be an Exchange Organizational Administrator or the permissions will not propagate. Not all domain administrators have this right.
- 3) The Shell commands to use are:

- On the Exchange 2003 Server, follow the steps in ["Task 4.2." on page 53](#)
- On the Exchange 2007 Server:

```
Get-Mailboxdatabase -IncludePreExchange2007 | Add-ADPermission -user [Service Account] -ExtendedRights "Send As","Receive As"
```

- On the Exchange 2010 Server:

```
Get-Mailboxdatabase -IncludePreExchange2010 | Add-ADPermission -user [Service Account] -ExtendedRights "Send As", "Receive As"
```

Where [Service Account] = display name of EMS Active Directory Service Account.

- 4) Plan at least two hours for permissions to propagate.

Task 4.5. Grant 'Send As' and 'Receive As' permissions in Exchange 2007/2010/2013 Coexistent Configurations

- 1) Link to Microsoft's instructions

- Exchange 2007: [Link to Instructions](#)
- Exchange 2010/2013: [Link to Instructions](#)

- 2) **Note:** The account used to **set** these permissions must be an Exchange Organizational Administrator or the permissions will not propagate. Not all domain administrators have this right.

- 3) The Shell commands to use are:

- On the Exchange 2007 Server:

```
Get-Mailboxdatabase -IncludePreExchange2007 | Add-ADPermission -user [Service Account] -ExtendedRights "Send As", "Receive As"
```

- On the Exchange 2010 Server:

```
Get-Mailboxdatabase -IncludePreExchange2010 | Add-ADPermission -user [Service Account] -ExtendedRights "Send As", "Receive As"
```

- On the Exchange 2013 Server:

```
Get-Mailboxdatabase -IncludePreExchange2013 | Add-ADPermission -user [Service Account] -ExtendedRights "Send As", "Receive As"
```

Where [Service Account] = display name of EMS Active Directory Service Account.

- 4) Plan at least two hours for permissions to propagate.

4.1.5. Virtualization

Email Management Services can be virtualized under the following conditions:

- 1) EMS is supported on the VMware Infrastructure virtualization platform. Other platforms may function correctly 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 Prerequisites" on page 42](#)
 - ["Hardware Requirements" on page 46](#)
 - ["Software Requirements" on page 47](#)
- 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 46](#).

4.2. Prerequisites for Optional Features

The following prerequisites must be met depending on the optional features your organization plans to implement:

- To enable partial activation of Email Continuity, you must install Redirector components. See ["Redirector Component Prerequisites" on page 57](#).
- To use any stored or archived mail features, you must install Redirector components and other stored mail components. See ["Redirector Component Prerequisites" on page 57](#) and ["Stored/Archived Mail Prerequisites" on page 61](#).
- To provide Email Archive integration with Exchange Envelope Journaling, see ["On-Premises Journaling Prerequisites and Limitations" on page 60](#)
- To enable Windows Authentication for your users, see ["Windows Authentication Prerequisites" on page 66](#).
- To provide the Outlook Extension to your users, see ["Outlook Extension Prerequisites and Limitations" on page 67](#).
- To enable Wireless Continuity for BlackBerry, see ["Wireless Continuity for BlackBerry Prerequisites" on page 71](#).

4.2.1. Redirector Component Prerequisites

Redirector components are installed on your Exchange servers to enable dynamic rerouting of messages. Redirector components are required only if your organization will use the optional features described below. Redirector components are installed along with other components in the Email Management Services software package.

For Email Continuity users, Redirector components are necessary for *partial activation* (a process where some users remain on the primary mail system while others use Email Continuity).

For users of *stored mail and Email Archive components*, Redirector components are necessary to transfer copies of mail to the VaultBox for processing.

NOTE Email Archive On-Premises Journaling Users

EMS Redirector Sinks or Redirector agents are required only if utilizing EMS Email Continuity services or are using a hybrid approach to message capture (have both journaled and non-journaled messages).

The supported platforms for any machine hosting a Redirector are:

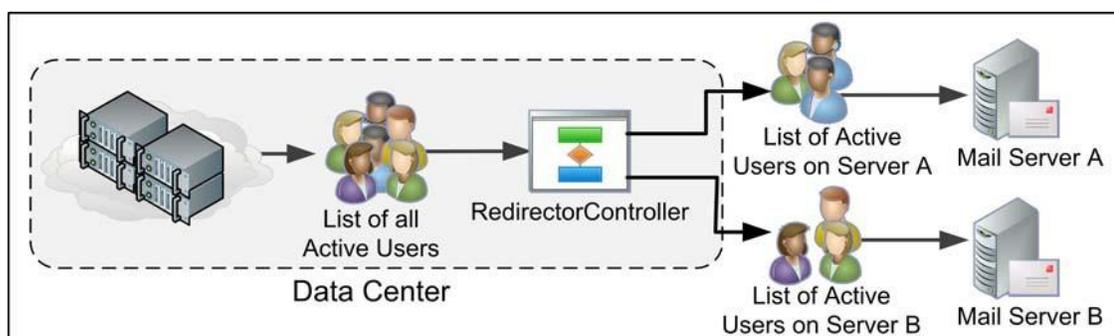
Table 4-7 Supported Platforms, Redirector Components

| Redirector Component | Supported Platforms |
|--|--|
| RedirectorSinks (Exchange 2003 only) | <ul style="list-style-type: none"> Windows Server 2003 with Exchange 2003 |
| Hub Transport Agents (Exchange Server 2007, 2010 and 2013 only) | <ul style="list-style-type: none"> Windows Server 2003 64-bit with Exchange 2007 Windows Server 2008 64-bit with Exchange 2007 Windows Server 2008 64-bit with Exchange 2010 Windows Server 2008 64-bit with Exchange 2013 Windows Server 2008 R2 64-bit with Exchange 2007 Windows Server 2008 R2 64-bit with Exchange 2010 Windows Server 2008 R2 64-bit with Exchange 2013 |

Table 4-8 Exchange Server Software Requirements

| Software | Notes |
|--|--|
| WMI Windows Installer Provider for Windows Server Operating Systems | A Windows component not enabled by default. Only needed for Exchange 2003 if installing the Redirector via Redirector Manager. |
| Exchange 2003/2007/2010: .NET Framework v. 2.0 SP1 or newer Exchange 2013: .NET Framework v. 4.5 or newer | If not already present on the Exchange server, you must manually download and install this software. Download version 4.5 from Microsoft |

Correct 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 mail servers for active users. Without access to RedirectorControllers, messages for active users cannot be redirected. Similarly, without access to the data center, RedirectorControllers cannot obtain updated routing information for your partially activated mail environment.

**Figure 4-4 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 mail servers are available in multiple locations, placing controllers in multiple locations helps protect against catastrophic failure or power outage in a single location.
- **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 Redirector components to obtain updated routing information.

- **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.

In the event of an outage where normally functioning mail 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.

4.2.1.1. Planning RedirectorSink/RedirectorController Placement

To use the partial activation feature in Exchange 2003 environment, RedirectorSinks are required. 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 2007/2010/2013 Environments

The partial activation feature is supported for Exchange Server 2007/2010/2013. Instead of using RedirectorSinks, the service uses a custom Transport Agent installed on the Hub Transport Server. For more information, see ["Install the RedirectorAgent" on page 88](#).

4.2.1.2. 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 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.

4.2.2. On-Premises Journaling Prerequisites and Limitations

4.2.2.1. On-Premises Journaling Supported Environments

Supported Email Management Services environments:

- EMS Client 6.6 or later
- EMS Data Center 6.15 or later

WARNING Upgrade to EMS Client 6.6 **Before** Implementing Email Archive On-Premises Journaling

VaultBoxes prior to EMS Client 6.6 *cannot* parse envelope journaled mail, and mail sent to a VaultBoxes with software earlier than EMS Client 6.6 will be **lost** and **unrecoverable**.

Supported Exchange Server environments:

- Microsoft Exchange Server 2003 SP3
 - See ["On-Premises Journaling Limitations" on page 61](#) for more information.
 - Exchange Server 2003 requires a registry change to enable envelope journaling. For information on enabling this feature please consult your Exchange product documentation or contact Support.

- Microsoft Exchange Server 2007
- Microsoft Exchange Server 2010
- Microsoft Exchange Server 2013

4.2.2.2. On-Premises Journaling Prerequisites

Upgrade all EMS server components (SyncManager, VaultBox, etc) to EMS 6.6 or later.

Review Microsoft Exchange Envelope Journaling documentation for Exchange-specific prerequisites.

4.2.2.3. On-Premises Journaling Limitations

- It is recommended customers review Microsoft's best practices in designing their Exchange envelope journaling deployment strategy.
- In comparison to later versions of Microsoft Exchange, Exchange 2003 provides only limited envelope journaling metadata. As a result, reviewers may notice differences in the amount and types of metadata available depending on the journaling source. This is an expected limitation of the older Exchange journaling format.
- Windows Office 365 users are not supported by the Capture Policy Service. Please verify that Office 365 users included in EMS retention policies are enabled for Exchange journaling within Office 365 manually.

4.2.3. Stored/Archived Mail Prerequisites

To enable stored mail/archive features, you must install Redirector components (see ["Redirector Component Prerequisites" on page 57](#)) and the VaultBox components described in this section. This section applies only if your organization plans to use stored mail/archive features.

4.2.3.1. VaultBox Hardware Requirements

If you plan to use any stored/archived mail features, you must install the VaultBox on 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 Redirector components, ensure that the server hosting the Redirector component meets the requirements as well.

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

Table 4-9 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.

4.2.3.2. VaultBox Planning

CAUTION Read Before Installing VaultBoxes!

Before you install VaultBoxes, 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 archived mail to be stored at the data center, you must do the following:

- 1) Determine how many VaultBoxes you will need for your mail environment. See ["VaultBox Capacity Sizing" on page 64](#).
- 2) Allow port 22 (TCP) as outbound for SSH through the firewall from all VaultBox machines. See the *EMS Network Settings* document provided by Support for specific address information.
- 3) Ensure that all mail servers that use SMTP can communicate with any identified VaultBox systems using port 25 (TCP).
- 4) On the mail server, 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).
- 5) 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 *EMS Network Settings* document provided by Support). See ["VaultBox Mail Routing Requirements" on page 65](#) for more details.

- 6) Assign MX records for VaultBox systems. Contact Support for specific instructions on how to do this for your organization.
- 7) Gather the following information for each machine that will be used as a VaultBox system:
 - The system 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 install the Historical Mail software on a drive with insufficient space, the feature will not work correctly.

NOTE Enable SMTP Logging

Verify that the following logs have been enabled for stored mail audit tracking:

- On the mail 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.
-

NOTE Ensure FIPS Is Disabled

FIPS compliance needs to be disabled in Windows Security Policy Settings for the VaultBox server.

To disable FIPS:

1. In **Control Panel**, double-click **Administrative Tools**.
2. In **Administrative Tools**, double-click **Local Security Policy**.
3. In **Local Security Policy**, expand **Local Policies**, expand **Security Options**, and then double-click **System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing**.
4. In the **System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing Properties** dialog box, click the **Local Security Setting** tab.
5. On the **Local Security Setting** tab, click **Disabled**, and then click **OK**.
6. Close **Local Security Policy**.

EMS uses FIPS-compliant algorithms for secure message transfer, but may use non-compliant algorithms for some internal operations. If you have questions about EMS and FIPS compliance, please contact Support.

4.2.3.3. VaultBox Capacity Sizing

Determining how many VaultBoxes are required to run EMS correctly in your environment depends on three factors:

- Peak message load
- VaultBox hardware specs
- Available bandwidth between your site and the data center

[Table 4-10](#) summarizes VaultBox sizing guidelines, showing the impact of various factors on system throughput. To make this calculation easier and more precise, a sizing calculator has been developed that takes key inputs and gives recommendations on how many VaultBox servers will need to be installed for your organization. Contact your EMS support representative to receive a copy of the EMS VaultBox Sizing Calculator.

Table 4-10 VaultBox Sizing Requirements

| Number of VaultBoxes | RAM | Peak Message Load | Minimum Bandwidth Required |
|----------------------|-------|-------------------|----------------------------|
| 1 | 4 GB | 8 messages/sec | 2 Mbps |
| 2 | 8 GB | 20 messages/sec | 5 Mbps |
| 4 | 16 GB | 40 messages/sec | 10 Mbps |
| 8 | 32 GB | 100 messages/sec | 24 Mbps |

The following considerations apply to both [Table 4-10](#) and the EMS VaultBox Sizing Calculator:

- Each VaultBox server should have a minimum configuration of a 2.4 GHz x86 processor and at least 1 terabyte (TB) of hard drive storage.
- Systems with more than 4 GB of RAM require a 64-bit version of Windows.
- The VaultBox Transfer Service can take advantage of multiple CPUs, and multicore CPUs, thus system performance depends upon, and varies with, the underlying hardware specs.
- The guidelines are based on VaultBoxes handling peak loads and are designed to avoid performance problems. Bandwidth between your site and the data center is one of the most important throughput limiting factors. The numbers listed in [Table 4-10](#) assume the system will encounter no network bottlenecks and specifies the bandwidth required to achieve such capacity. These guidelines allow enough system headroom to process any possible queue build up due to unforeseen circumstances, such as temporary network outages.

4.2.3.4. VaultBox 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 Email Archive implementation requires understanding your organization's mail server routing topology and advanced knowledge of mail server functionality. An analysis of the variables involved leads to the identification of your organization's preferred routing topology, which requires configuration of:

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

Correct implementation of the preferred routing topology not only allows for functional operation of Email Archive, but helps maximize mail system manageability. Variables considered in making this determination include, but are not limited to:

- General network topology
- Mail server 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 Email Archive 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.

Work closely with Support to determine the routing requirements for your organization. Because each network is unique, it is impossible to provide a static requirements list.

4.2.3.5. 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.

4.2.4. Windows Authentication Prerequisites

The Windows Authentication feature allows your users to log in to the EMS web interface using their existing Windows network user names and passwords. To enable this, you must install Authentication Manager a local machine in your environment that validates a user's credentials with the local Windows subsystem using New Technology LAN Manager (NTLM).

4.2.4.1. Windows Authentication Requirements

The following are required to use Windows Authentication:

- 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.

Support for Exchange Resource Forests vary depending on the type of trust between the Exchange and security forests.

- Two-way trust:
 - No changes beyond the normal requirements for deploying auth controllers (redundancy, distributed, etc) should be required.
- One-way trust:
 - Treat one-way trusts as distributed environments, and be sure to deploy a sufficient number of auth controllers for redundancy purposes.

When Support configures Windows Authentication in the data center, they set the parameters described in [Table 4-11](#). To change any of the default values, contact Support.

Table 4-11 Windows Authentication Configuration Parameters

| Parameter | Description | Default Value |
|------------------------|--|---|
| 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 allowed before 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. |

Table 4-11 Windows Authentication Configuration Parameters (Continued)

| Parameter | Description | Default Value |
|---------------------|---|---------------|
| 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 |

4.2.4.2. 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 multidomain 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 the Active Directory password after having logged in and cached the password in Email Continuity, the cached password remains the Email Continuity password until the **Cached Windows Password** time-out expires.

4.2.5. Outlook Extension Prerequisites and Limitations

4.2.5.1. Supported Environments/Prerequisites

For Outlook Extension, the following table identifies the supported Operating Systems and Outlook versions.

Table 4-12 Supported environments for Outlook Extension

| | | Outlook Version | | | | | | |
|------------|------------------------|-----------------|----------------------|----------------------|----------------|----------------|-----------------------------|-----------------------------|
| | | OL 2007 (SP3) | OL 2010 32-bit (SP1) | OL 2010 64-bit (SP1) | OL 2013 32-bit | OL 2013 64-bit | OL 2013 Click-to-Run 32-bit | OL 2013 Click-to-Run 64-bit |
| OS Version | Windows 7 32-bit (SP1) | X | X | NA | X | NA | X | NA |
| | Windows 7 64-bit (SP1) | X | X | X | X | X | X | X |
| | Windows 8.1 32-bit | | X | NA | X | NA | X | NA |
| | Windows 8.1 64-bit | | X | X | X | X | X | X |
| | | | | | | | | X = Supported |

Table 4-13 Supported environments for Outlook Extension Search Feature

| | | Outlook Version | | | | | |
|------------|------------------------|----------------------|----------------------|----------------|----------------|-----------------------------|-----------------------------|
| | | OL 2010 32-bit (SP1) | OL 2010 64-bit (SP1) | OL 2013 32-bit | OL 2013 64-bit | OL 2013 Click-to-Run 32-bit | OL 2013 Click-to-Run 64-bit |
| OS Version | Windows 7 32-bit (SP1) | X | NA | X | NA | X | NA |
| | Windows 7 64-bit (SP1) | X | X | X | X | X | X |
| | Windows 8.1 32-bit | X | NA | X | NA | X | NA |
| | Windows 8.1 64-bit | X | X | X | X | X | X |
| | | | | | | | X = Supported |

4.2.5.2. Outlook Extension Prerequisites

The following are required to use the Outlook Extension:

- Outlook must be in cached mode to use Email Continuity features.

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

- Users must have administrative permissions to install the Outlook Extension. See the article *How to allow users who are not administrators to install MSI packages* (<http://support.microsoft.com/kb/259459>) for additional information.
- For the storage management feature of the Extension to work as described, the administrator must publish two forms to a Library in Exchange, and end users must have access to the forms on Exchange. See "[Install Custom Forms for Storage Management](#)" on page 108.

4.2.5.3. Outlook Extension Limitations

[Table 4-14](#) describes known limitations of the Outlook Extension. To compare Outlook Extension features with those of Email Continuity webmail, see "[About the Outlook Extension](#)" on page 13.

Table 4-14 Outlook Extension Limitations

| Limitation | Status |
|---|---|
| Outlook Extension does not support more than one instance of Outlook on the same machine. | |
| <p>For customers planning to upgrade from 32-bit Outlook to 64-bit Outlook, administrators must <i>uninstall</i> Outlook Extension while still on 32-bit Outlook, and then install Outlook 64-bit, followed by re-installing the Outlook Extension.</p> <p>If the above upgrade procedure is not followed then the user is likely to encounter following error message: "Microsoft Outlook 2003, 2007, or 2010 (x86) is a prerequisite of MessageOne Outlook Addin (x86)" when upgrading or uninstalling Outlook Extension 6.3.</p> | If the user encounters the error message described in the limitation section, the user should <i>downgrade</i> to a 32-bit Outlook version, uninstall Outlook Extension, and then install 64-bit Outlook version, followed by installing Outlook Extension. |
| <p>When an active user (on Outlook 2010) replies to a meeting invitation (from a user on Exchange 2010) and includes text in the body of the response, the recipient (on Exchange 2010) does not receive the response message text.</p> <p>This was confirmed as bug with Exchange 2010.</p> | The recipient user needs to have following installed in order to resolve this issue: Update Rollup 5 for Exchange Server 2010 Service Pack 1 (KB2582113) or Service Pack 2 for Exchange 2010. |
| If two instances of Outlook Extension attempt to access the same mailbox at the same time, each instance will pick up different messages. This can confuse users who will not see all messages in both instances. | <p>Use the workaround: Have only one instance of Outlook Extension running against a mailbox at any time.</p> <p>Use EMS Webmail if you need to access a EMS mailbox from a different machine while Outlook Extension is running.</p> |
| Meeting requests sent using the Outlook Extension in the Active State do not show meeting details when accessed on the Access Email Archive page. Only regular text messages can be rendered on the Access Email Archive page. | Under investigation for a future release. |

Table 4-14 Outlook Extension Limitations

| Limitation | Status |
|--|---|
| During an activation, read/delivery receipts require user to click Send/Receive button in order to be delivered. | During an activation, read receipts are generated and sent when a user clicks the Outlook Send/Receive button. If a 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 a future release. |
| <p>Because of the way Microsoft encodes new lines in the Description field, meetings created using the Outlook Extension sometimes display <code>n</code> characters in the text when they are restored by the RecoveryManager. This is purely a cosmetic issue.</p> <p>For example, instead of Meeting Request for Monday 4/23 - 11:00 -11:30, the invitation reads <code>\nMeeting Request for Monday 4/23 - 11:00 -11:30\n</code>.</p> | Under investigation for a 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. By contrast, Exchange itself would attempt to send the message even if the address did not conform to RFC-822. | This is an expected difference in behavior between the Outlook Extension and Exchange on the primary mail server. |
| If a client-side rule (such as <code>move a message from a user on Exchange to a folder</code>) is based on an Exchange address, the rule may not be processed consistently. Rules must use SMTP addresses to behave as expected. | Under investigation for a future release. |
| Outlook's All Subfolders button does not apply to Outlook Extension Search. Outlook Extension Search searches only the selected folder in the MessageOne Archive Store folder structure. If the currently selected folder happens to be the root MessageOne Archive Store folder, the entire archive is searched. | |
| After enabling a user for Folder Synchronization, archived email messages may not be immediately available in Outlook Extension Search results. Changes to folder structure and message location are synchronized on a schedule established by EMS administrators. Day to day changes to hierarchy or message location may take 24 hours to appear. | |
| In order to minimize impact to the Outlook, mailbox folder hierarchy changes are only made on start-up. Changes to overall folder structure will not be updated in Outlook until Outlook is closed and reopened. | |

4.2.6. Wireless Continuity for BlackBerry Prerequisites

The Wireless Continuity for BlackBerry feature ensures that 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 BlackBerry Enterprise Server (BES) fails along with the primary mail system.

4.2.6.1. Wireless Continuity for BlackBerry Requirements

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

- BlackBerry device software version 4.1 through version 6.0 have been QA-certified for use with Wireless Continuity for BlackBerry. Earlier and later versions may work, but are not supported.
- All BlackBerry devices that will use the client agent must install the agent version 6.2 or later.
- Your organization must be using BES 4.1 through version 5.0. These versions have been QA-certified for use with Wireless Continuity for BlackBerry. Earlier and later versions may work, but are not supported.
- BES High Availability is not a validated configuration for Wireless Continuity for BlackBerry.
- The MDS service must be running on all BES servers.
- The EMS SyncManager must have network access to the BES databases by Window NT authentication.
- If your organization uses MSDE, you must give the EMS Root Account `read` permissions for the directory where the `BESMgmt_data.mdf` and `Besmgmt_log.mdf` reside.
- The RedirectorController must be able to post HTTP requests to the BES systems that have push capability.
- 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 autodetection, the installation process autodetects the correct instance. If your environment does not provide for autodetection, you must set this manually.

4.2.6.2. Wireless Continuity for BlackBerry Supported Configurations

The service supports:

- All configurations of BES 4.1 through 5.0 (other versions may work but have not been QA certified) supported by RIM.
- All devices using OS versions 4.1 through 6.0 (other versions may work but have not been QA certified), 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.
- All messages containing standard UTF-8 and Unicode characters.

4.2.6.3. Wireless Continuity for BlackBerry Limitations

Known limitations for Wireless Continuity for BlackBerry include:

- **GAL lookups unavailable:** During an Email Continuity activation the Wireless Continuity for BlackBerry agent is not capable of Global Address List (GAL) lookups. Wireless Continuity for BlackBerry is limited to using only the contact data that has been stored locally on the BlackBerry device prior to the activation.
- **Unread message counter sometimes incorrect:** 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**.
- **BES-independent model version limitations:** The BES-independent model that allows BlackBerry users to compose, send, and receive mail 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 that uses version 6.2.2.3 (or higher) BlackBerry client agent. Organizations using previous versions of the data center or client agent software will notice no change to their Wireless Continuity for BlackBerry implementations.
- **Cannot send attachments:** 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.
- **Forward/Reply modifies attachments:** Forwarded messages and replies do not include original attachments, but do provide a text rendering of them up to the device limit.
- **Audible/vibration alerts unavailable:** During an activation of Email Continuity, new message notifications will trigger the LED on a device to flash, but no audible or vibration alerts will occur.

4.2.6.4. Wireless Continuity for BlackBerry Known Issues

Known issues for Wireless Continuity for BlackBerry include:

- **Cannot forward/reply messages after activation:** 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 the mail server through the BES.
- **Possible new security prompt:** A possible security prompt: when deploying the RIM Agent, users may see a new security prompt on the device that asks if the agent should be allowed to interact with phone information. Inform users that they should allow these interactions.
- **Outlook folder structure must be visible:** The Outlook folder structure must be visible in the **View Folders** view. This ensures that the device has the user display name, which is required to view received messages.

4.2.6.5. Wireless Continuity for BlackBerry Installation Prerequisites

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 EMS Active Directory Service Account to the Local Administrator Group (see ["Adding the EMS Root Account to the Local Administrator Group" on page 73](#)).
- 2) Enable TCP and Names Pipes Access to the BES database (see ["Enabling TCP and Name Pipes to Access the BES Database for Pre-2005 SQL Servers" on page 74](#)).
- 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 75](#)).
- 4) Verify IT Policy settings (see ["Verifying IT Policy Settings" on page 76](#)).
- 5) Grant `db_datareader` and `public` access to the BES SQL database.

4.2.6.6. Adding the EMS Root Account to the Local Administrator Group

You must add the EMS Root Account (or the valid super administrator account that is running EMS services for your organization) as a local administrator of the BES group.

Task 4.6. Add the EMS 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 EMS Root Account 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 EMS administrator user added to the list.

4.2.6.7. Enabling TCP and Name Pipes to Access the BES Database for Pre-2005 SQL Servers

You must enable TCP and name pipe access to the BES database. To do this, you must run `SVRNETCN.exe` and then stop and restart SQL services.

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.

Task 4.7. 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) Stop and restart the SQL server.
 - a. To stop the MSSQLServer, right-click its icon in the notification area. This launches 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.
 - b. Next, restart the service by right-clicking the icon and selecting **MSSQLServer Start**.

4.2.6.8. 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:

- Configure MDS to act as a push server.
- Configure MDS to listen on a valid port.
- Stop and Restart the MDS services.

Task 4.8. Verify that the MDS server is a push server and has an appropriate listening port configured:

- 1) Select **Start > BlackBerry Enterprise Server > BlackBerry Manager**. The BlackBerry Manager splash screen appears.
- 2) After the BlackBerry Manager starts, 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. When you select a server, settings for that server appear in the **Connection Service** panel.
- 4) 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`.

- 5) Click **Edit Properties** above **Tasks**.
- 6) The **BlackBerry MDS Connection Service** panel appears. Verify that the **Web Service Listen Port** is an available port (usually 8080).
- 7) Stop and restart the service using the buttons in the **Task** panel.

4.2.6.9. Verifying IT Policy Settings

You must verify that your IT policy settings:

- Allow third-party application downloads.
- Allow internal connections.
- Allow external connections.

Task 4.9. Verify 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.

4.2.7. Folder Sync Prerequisites

The following settings need to be configured before the Folder Sync feature can be used.

4.2.7.1. Minimum Client Software Version

The minimum client software version required to implement folder synchronization is EMS Client 6.9.1 for the VaultBox handling the synchronization.

WARNING Upgrade after Folder Sync is enabled by Support

The upgrade to a Folder Sync compatible version of the client software must be performed *after* Support has enabled the Folder Sync feature for your environment, otherwise Folder Sync will not work until the client software is reinstalled.

4.2.7.2. Configure Exchange for Autodiscover

Refer to Microsoft's Exchange configuration documentation for this procedure.

4.2.7.3. Configure Exchange Impersonation

To configure Exchange Impersonation in Exchange 2007, run the following command in Exchange Management Shell:

```
Get-ExchangeServer | where {$_.IsClientAccessServer -eq $TRUE} | ForEach-Object {Add-ADPermission -Identity $_.distinguishedname -User (Get-User -Identity ems-svc | select-object).identity -extendedRight ms-Exch-EPI-Impersonation}
```

Where *ems-svc* is your Active Directory Service Account.

To configure Exchange Impersonation in Exchange 2010/2013, run the following command in Exchange Management Shell:

```
New-ManagementRoleAssignment -  
Name:impersonationAssignmentName -  
Role:ApplicationImpersonation -User:ems-svc
```

Where *ems-svc* is your Active Directory Service Account.

4.2.8. AlertFind Integration Prerequisites

4.2.8.1. AlertFind Integration Requirements

The following are required to support AlertFind Integration:

- 1) One-to-one mailbox-to-user correspondence between products.

AlertFind integration is available only to customers whose Email Continuity and AlertFind user bases are exactly matched; that is, all of the mailboxes synchronized for Email Continuity are also synchronized for AlertFind. AlertFind integration does not work for customers who have all of their users in Email Continuity and only a subset of users in AlertFind, or all of their users in AlertFind and only a subset of users in Email Continuity.

- 2) Active Directory data must be formatted correctly for the AlertFind import to function. Your Support representative can provide you with the correct formatting rules. Incorrectly formatted Active Directory data will not synchronize.

4.2.8.2. AlertFind Integration Limitations

The following are known limitations of AlertFind integration with Email Management Services:

- 1) Although you can synchronize custom data fields from Active Directory and use them as AlertFind groups, PIN fields and time zone data fields are not mapped to AlertFind. Users can create their own PINs and set time zone data through the AlertFind user interface.
- 2) Custom data fields collected from Active Directory and synchronized to AlertFind are not available for use in other features of Email Management Services.
- 3) 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.
- 4) There is currently no mechanism to automatically notify AlertFind users of an activation of Email Continuity. Such notifications must be created by an authorized AlertFind user or administrator.

5. Install and Configure EMS Controller and Environment

Installing and configuring the Email Management Services software involves doing the following:

- 1) ["Install Required Service Software" on page 80](#)
- 2) ["Configure the SyncManager" on page 82](#)
- 3) ["Install and Configure Optional Features" on page 86](#)
 - ["Install Redirector Components" on page 87](#)
 - ["Configure On-Premises Journaling" on page 92](#)
 - ["Configure VaultBoxes" on page 92](#)
 - ["Install Outlook® Extension" on page 96](#)
 - ["Install Custom Forms for Storage Management" on page 108](#)
 - ["Deploy Wireless Continuity for BlackBerry" on page 111](#)
 - ["Mobile App Support Configuration" on page 121](#)
- 4) ["Configure Enterprise Archive Features" on page 123](#)
 - ["Configure Scanning and Data Transfer for Storage Management Policies" on page 123](#)
 - ["Harvester Operation and Data Logging" on page 126](#)
 - ["Configure Scanning and Data Transfer for User Classification Retention Policies" on page 128](#)

Before you start, you will need the service software and a EMS Root Account username and password:

- 1) **Service software** — Download the install package from the location provided by Support.

For full use of stored mail or Email Archive features, your EMS Controller must be running version 6.0 or later of the EMS service software. To see which version of a component you have, select **Start > All Programs > MessageOne > [component name]**, such as **Start > All Programs > MessageOne > RecoveryManager**. 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 6.0 or later of the service software. To see which version you are running of a component, such as the SyncManager, select **Start > All Programs > MessageOne > SyncManager**. The software launches, and the version number appears on the opening screen.

- 2) **EMS Root Account username and password** — You must use the *EMS Root Account* or a valid *super administrator* account (created by your organization's EMS Root Account) for authentication of the SyncManager with the data center servers. If you do not have the EMS Root Account username and password, contact Support.

5.1. Install Required Service Software

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

The installation installs:

- SyncManager
- RecoveryManager, RedirectorController, RedirectorManager, and the Directory Configuration wizard.
- Windows Authentication, if enabled

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

WARNING Upgrading to 6.4.4

If you are upgrading to 6.4.4 from any 6.4.x version, no additional steps are required.

If you are upgrading to 6.4.4 from any pre-6.4.x version of the software, prior to installing the 6.4.4 version, you must first remove (uninstall) all Email Continuity and Historical Mail (ActiveMailbox) software.

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

NOTE RPC over HTTP(S) (Exchange 2013) MAPI Profile Does Not Work with Proxy Server

If Client 6.7+ is used with Exchange 2013 and a proxy server is also used in the environment, EMS Client must be allowed to bypass the proxy server in order to communicate properly with Exchange.

Task 5.1. Install service software:

- 1) On the EMS server, log in using the Active Directory Service Account you created to meet preinstallation requirements under "[Active Directory Service Account Requirements](#)" on page 50.

NOTE Exchange Coexistent Environments with Exchange 2013

If your system is configured in an Exchange Server Coexistent environment with Exchange Server 2013, use the Exchange 2013 Active Directory Service Account to log in to the EMS server.

- 2) Open the installation software folder, and double-click the **ems.msi** file.
- 3) In the **Application Root Username and Password** window, log in with the user name and password of the EMS Root Account or a valid super administrator account, then click **Next**.
- 4) In the **Select Features** window, choose the component to install.
 - a. For a typical installation, click **Complete**. This installs all applicable components.
 - b. 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**.
- 5) In the **Service Credentials** dialog box, identify the Active Directory Service Account that accesses your primary email environment, and assign the account proper domain permissions. Because you logged in with this account, the installation process automatically populates the **Domain** and **Username** fields with the current domain account information. To complete the login process and set necessary domain permissions:
 - a. Verify the information in the **Domain** box or, to log in under a different account, enter the appropriate domain information. MessageOne 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**.

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

- 6) Provide RedirectorController registration information.

To configure the RedirectorController, the software must register the component so that it can communicate with the 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**.
 - e. Click **Install**.
- 7) Email Continuity cannot function until you configure the SyncManager. MessageOne recommends that you configure SyncManager as soon as you complete the installation. To do this, click the **Start SyncManager to configure EMS** check box, then click **Finish**.
 - 8) If the SyncManager has never been run before, a prompt appears requesting your approval to continue. Click **OK**.
 - 9) 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 "[Task 5.2. Launch the SyncManager Setup Wizard manually:](#)" on page 83.

CAUTION Exclude RecoveryManager Temporary File Directory From Antivirus Scanning

In some instances, if the computer's antivirus software is running at the same time as the RecoveryManager runs, the antivirus software removes necessary temporary *.eml files causing errors or the RecoveryManager to close unexpectedly.

Excluding the RecoveryManager temporary file directory from being scanned by your antivirus software will eliminate the conflict.

The directory to exclude is `RecoveryManager` located in the application data directory. The exact location will depend on the computer's operating system and system configuration. For example:

- `C:\Documents and Settings\[user]\Local Settings\Application Data\RecoveryManager`
- `C:\Users\[user]\AppData\Local\MessageOne\RecoveryManager`

Refer to the antivirus software's instructions for how to exclude directories from scans.

5.2. Configure 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 then performs an initial synchronization. After this initial synchronization, 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; "[Resolve User ID Conflicts Manually](#)" on [page 162](#).

Q Why is conflict detection necessary?

- A** Email Management 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.

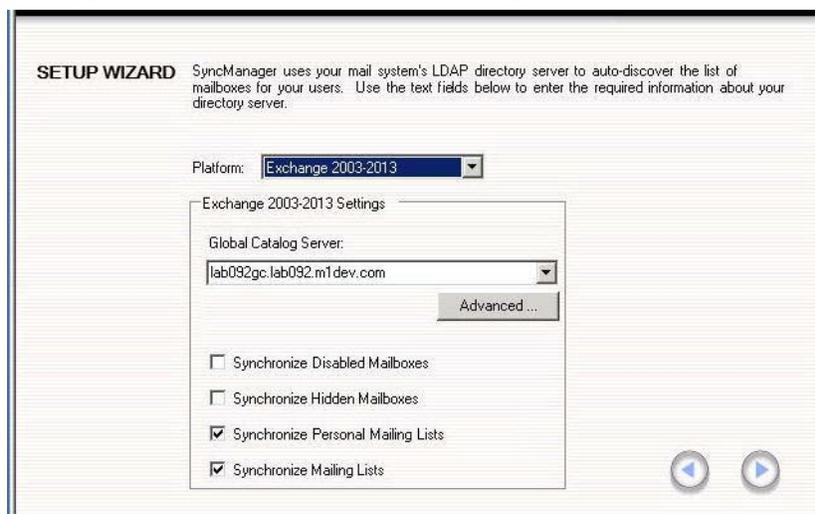
Task 5.2. Launch the SyncManager Setup Wizard manually:

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

Task 5.3. Configure the SyncManager:

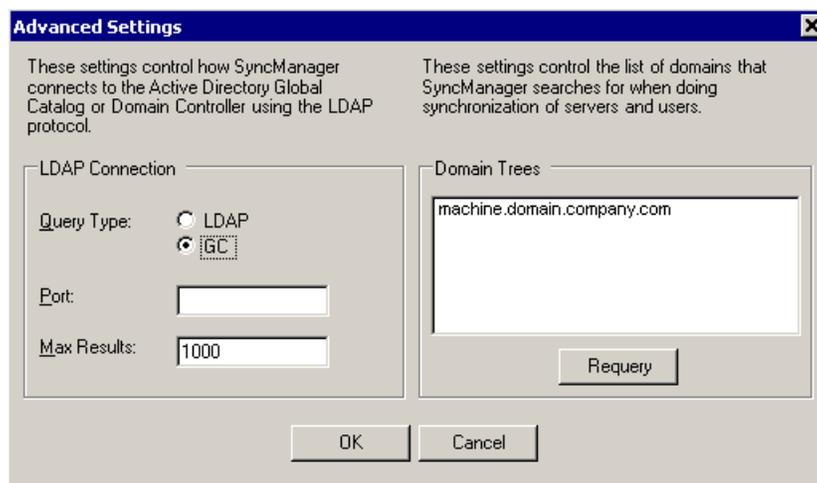
- 1) Log in to the SyncManager Setup Wizard. You must use the user name and password for the EMS Root Account or a valid super administrator account.

2) Identify your version of Microsoft Exchange software.



- a. Select the appropriate email **Platform** and complete the information in the **Settings** portion of the window.
- If you use Exchange 2003/2007/2010/2013 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.



- b. To synchronize disabled and/or hidden mailboxes, check the appropriate box: **Synchronize Disabled Mailboxes**, **Synchronize Hidden Mailboxes**.
- c. 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.
- d. Click the **Next** arrow.

- 3) The Setup Wizard registers the SyncManager instance with the EMS server. Click the **Next** arrow.
- 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.

SETUP WIZARD SyncManager allows you to schedule your directory synchronization runs at whatever intervals are convenient for your organization. You can enable or disable scheduling, and you can set scheduling intervals of every day at a specified hour, every week on a specified day at a specified hour, or every month on a specified day at a specified hour.

Directory Schedule Information

Run Scheduled?

Frequency ? Daily

Day ? Sunday

Start Hour ? 2:00 AM

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 synchronized from Active Directory.

- a. MessageOne 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) To perform the initial Directory data synchronization between SyncManager and the data center, click the **Next** arrow.
 - 6) 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 "[Exclude Users or Mailboxes](#)" on page 160.

Click the **Next** arrow.

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

If other synchronizations are available to you, you can run them at this time. After you have configured the SyncManager, you should set a deletion threshold percentage so that a fault alert message is sent when the set percentage of users or distribution lists is exceeded. See "[Sync Notify Settings](#)" on page 197 for more information.

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

Task 5.4. Configure distributed synchronization with SyncManager:

- 1) On the server that is your primary controller, open SyncManager. From the **Start** menu, select **Programs > MessageOne > 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 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.

5.3. Install and Configure Optional Features

This section contains information useful for installing and configuring the components required for optional features:

- To enable **partial activation** of Email Continuity, you must install Redirector Components. See "[Install Redirector Components](#)" on page 87.
- To enable **stored mail and Email Archive** functions, you must install Redirector Components and at least one VaultBox. See "[Install Redirector Components](#)" on page 87 and "[Configure VaultBoxes](#)" on page 92.

- To allow email users to **access their messages with Outlook** during an activation of Email Continuity, you must install the Outlook Extension. See "[Install Outlook® Extension](#)" on page 96.
- To enable **storage management functions to work with Outlook**, you must install custom forms. See "[Install Custom Forms for Storage Management](#)" on page 108.
- To allow email users to **access their messages on BlackBerry devices** during an activation of Email Continuity, you must configure and deploy the BlackBerry client agent. See "[Deploy Wireless Continuity for BlackBerry](#)" on page 111.

5.3.1. Install Redirector Components

A RedirectorController is installed as part of the basic service software install.

NOTE If Redirector upgrade fails, check rollback status

When upgrading the Exchange Redirectors to Client 6.7+, if the upgrade fails and causes a rollback, check on the status of the Redirector to confirm that it successfully rolled back to the previous version. You may need to manually re-register the transport agent or completely reinstall.

5.3.1.1. Install RedirectorSink on Clustered Exchange Servers

To use the partial activation feature of Email Continuity in an Exchange 2003 environment, you must install RedirectorSink.

Task 5.5. 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 EMS Admin 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.

5.3.1.2. Install the RedirectorAgent

To use the partial activation feature of Email Continuity in Exchange 2007 or 2010 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 2003 environment. 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.

NOTE Exchange 2013 Cumulative Update 1 and 2 can change the priority of 3rd party Transport Agents.

After installing CU1 or CU2, check the priority of our Transport Agent with the `Get-TransportAgent` cmdlet.

If the EMS Redirector is not the lowest priority Transport Agent, then either change the priority with the `Set-TransportAgent` cmdlet or reinstall the Transport Agent.

Task 5.6. 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 Management Services software. Do not enter the values for your Exchange server.

For example, if the name of the server in your environment running EMS 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 EMS 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.

NOTE The Redirector Service Log File

You may see a warning in the **Redirector Service** log file: *Unable to retrieve Installed Redirector Version from registry*. Ignore this warning. There are no functional issues related to this warning and it will eventually be removed from the logs on a subsequent client release.

Task 5.7. 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.

5.3.1.3. Configure 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.

5.3.1.4. Install 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 servers.

Task 5.8. Install RedirectorManager:

- 1) Log in to the RedirectorManager software (**Start > Programs > MessageOne > RedirectorManager**). This verifies the email platform and gathers information from each 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 log in using the EMS 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 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 services and deploy RedirectorSinks.
 - a. Select **Restart Services**.
 - b. Click **Next**.

NOTE Installing Without Stopping Services

You can install RedirectorSinks without stopping and restarting 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 server 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 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 EMS Admin Console do not show the RedirectorSinks as installed on a server, send an email message to any user on that server. This causes the server to load the RedirectorSink. While not typically an issue on production servers under load, this can occur in test environments.

5.3.1.5. Upgrade 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 server to your environment, or when you reinstall an existing server, you must repeat the RedirectorSink installation process to install the RedirectorSink on the new or reinstalled server. When reinstallation is necessary, the EMS Admin Console displays an alert message.

5.3.2. Configure On-Premises Journaling

Please contact Support to discuss the journaling design your organization plans to implement with EMS. Based on that design Support can help ensure the proper journaling configuration within your Exchange environment and help verify the system performs as expected.

Task 5.9. Configure On-Premises Journaling

- 1) Contact Support to enable On-Premises Journaling
- 2) Upgrade to EMS Client 6.6 or newer.
- 3) Create an Active Directory contact for each On-Premises Journaling address you plan to use (See ["Managing On-Premises Journaling Addresses" on page 287](#)). For information on creating an Active Directory contact please review you Exchange product documentation or contact Support.

5.3.2.1. On-Premises Journaling Best Practices

During deployment, test by configuring journaling for 1 or 2 mailboxes to ensure that journaling rules are accurate, otherwise messages may be lost and unrecoverable

Ensure the send connector used for Email Archive does not route through a spam filter or content filter, or messages may be lost. Routing to the EMS Data Center directly is recommended.

5.3.3. Configure VaultBoxes

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

5.3.3.1. Change 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 > MessageOne > 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 "[Configure Scanning and Data Transfer for Storage Management Policies](#)" on page 123 for more information.
- Start and stop User Classification Retention and edit User Classification settings. If your organization uses the user classification retention feature, you must configure additional VaultBox settings. See "[User Classification Retention Policies](#)" on page 34 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

Task 5.10. 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**.

5.3.3.2. Monitor VaultBoxes

Typically, you monitor VaultBox status through the VaultBox Console and EMS Admin 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 5-1 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 5-1 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. | | |
| 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 appears as Simple Mail Transfer Protocol (SMTP) • srtransfersvc, which appears 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 |

Table 5-1 VaultBox Monitoring

| Data Type | Description | Alert When | Troubleshooting Suggestions |
|-----------------------------------|--|-------------------------------------|---|
| 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 EMS Admin Console Readiness check will indicate an error). |
| Messages rejected by a VaultBox | <p>Messages are being rejected by the VaultBox, with error messages in the following form:</p> <pre><xxxxxx.xxx@ems-1.activemailbox.net>: 554 5.7.1 <xxxxxx.xxx@ems-1.activemailbox.net>: Recipient address rejected: Access denied</pre> <p>These are fatal delivery errors most commonly caused by incorrect DNS configuration. Your SMTP server will <i>not</i> attempt to redeliver the messages to the VaultBox. You must take action to get these failed messages into the archive.</p> | Any message of this form is thrown. | <ol style="list-style-type: none"> 1 Contact EMS Support to correct your DNS configuration. 2 Work with EMS Support to schedule a historical import to get the failed messages into the archive. |

5.3.4. Install Outlook[®] Extension

Outlook[®] Extension is provided by Support as an MSI file usable for both GPO and manual installation methods. Outlook Extension conforms to Microsoft-approved Outlook Integration APIs and uses Extended MAPI and Outlook Object Model to interact with Outlook.

Guidelines for installing Outlook Extension:

- You can allow users to use Outlook Extension features without having to log in to Email Management Services. To do this, run the command line utility (**PrepareOutlookAuth**) to create an authentication token *before* you deploy the Outlook Extension to users. See "[Enable User Authentication Through the Command Line](#)" on page 97 for information.
- Ensure that the installation package you receive from Support is configured for your operating system and Outlook version. There are two versions of the installation package. The x86 MSI is for 32-bit Outlook versions. The x64 MSI is for 64-bit Outlook versions.
- MessageOne recommends that Outlook *not be running* during the installation process.
- Outlook Extension can support multiple users running on the same machine in an enterprise environment.

5.3.4.1. Enable User Authentication Through the Command Line

The Outlook Extension uses an authentication token stored at `HKEY_CURRENT_USER\Software\MessageOne\EMS\Profile Info\<profile name>\AuthToken` to allow a user to use the Extension features without having to log in to Email Management Services. The token can be created by a user logging in with a password, or the administrator can use the **PrepareOutlookAuth** tool to create the token. After the authentication token is set, the user will not need to log in again during an activation or while using other Extension features.

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.

PrepareOutlookAuth is installed on the same machine that hosts the SyncManager. You must complete a directory sync before running **PrepareOutlookAuth**. 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 already present. 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**

MessageOne 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.

The following arguments are available.

Table 5-2 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") |
| -primarySMTPAddress <primary email address> | Outlook token update for a single user defined by their primary SMTP email address. Can be shortened to <code>-p <primary email address></code> |
| -inputFile "full_path\filename.txt" | Outlook token update for all users listed in an input file. The input file must be a text file, containing valid primary SMTP addresses, one email address per line. |
| -exchangeServerFile "full_path\filename.txt" | Outlook token update for all users belonging to Exchange servers that are listed in an input file. The input file must be a text file, containing valid Exchange server addresses, one server address per line. |
| -verbose | Enables verbose output |
| -help | Displays usage information |

Task 5.11. 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]\MessageOne EMS\Outlook Addin\`
 - Where `[Program Files]` refers to :
 - `Program Files (x86)`, when installing a 32-bit version of Outlook Extension on a 64-bit Operating System
 - **OR** `Program Files`, when dealing with any other combination of Outlook Extension and Operating System.
- 3) Enter one option:
 - `prepareoutlookauth.exe -user "mailboxdn"`
 - `prepareoutlookauth.exe -all`

- `prepareoutlookauth.exe -primarySMTPAddress test_1@sample.com`
 - `prepareoutlookauth.exe -inputFile "C:\path\OutlookUpdateEmailAddresses.txt"`
 - `prepareoutlookauth.exe -exchangeServerFile "C:\path\ExchangeServerList.txt"`
- 4) Wait for the new mailbox properties to take effect. This may take up to 24 hours.
 - 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.

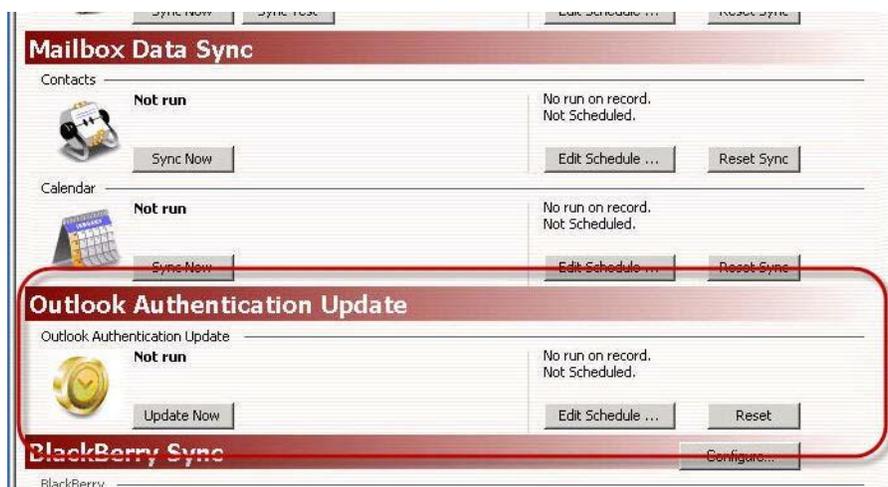
5.3.4.2. Enable User Authentication Through SyncManager

NOTE Functionality Limitations

The following functionality is not applicable if SyncManager is configured in Distributed Sync configuration.

As an alternative to the PrepareOutlookAuth tool described in the previous section, you can manually run and/or schedule the PrepareOutlookAuth update via SyncManager.

When EMS Outlook Extension capability is enabled, the Outlook Authentication Update section is added to the SyncManager main window.



Using SyncManager, user authentication can be set to run for all users on a recurring schedule, or run manually for either a single user or all users. A manual single-user run can be useful when troubleshooting errors that occur when writing the token to a mailbox.

Task 5.12. Create an Outlook Authentication Update schedule for all users

- 1) In the SyncManager main window, click the **Edit Schedule...** button.



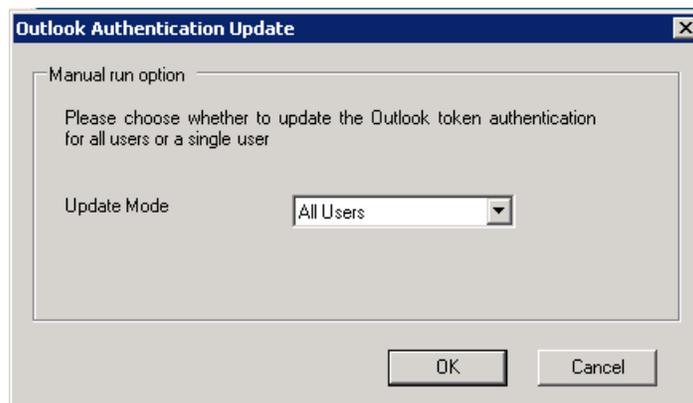
- 2) In the **Edit Outlook Authentication Update Schedule** window, check **Run Scheduled?** checkbox.



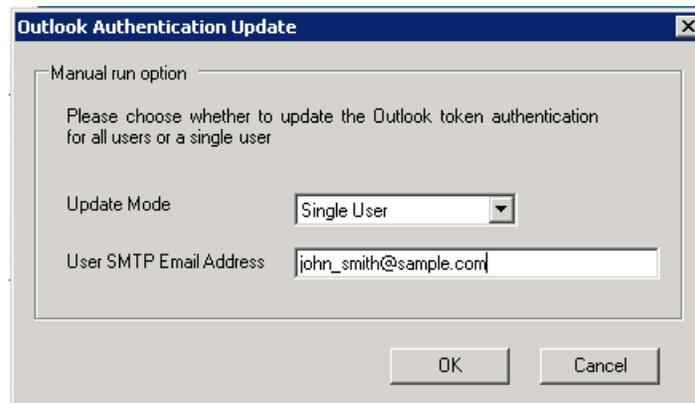
- 3) Choose the day and time to run the update. Then click **Save**.

Task 5.13. Manually run an Outlook Authentication Update.

- 1) From the SyncManager main window, click the **Update Now** button.
- 2) To update all users:
 - a. Select **All Users** from the drop-down



- b. Click **OK**.
- 3) To update a single user:
 - a. Select **Single User** from the drop-down.



- b. Enter the SMTP email address of the user to update.
- c. Click **OK**.

Task 5.14. Overwrite Outlook Authentication token

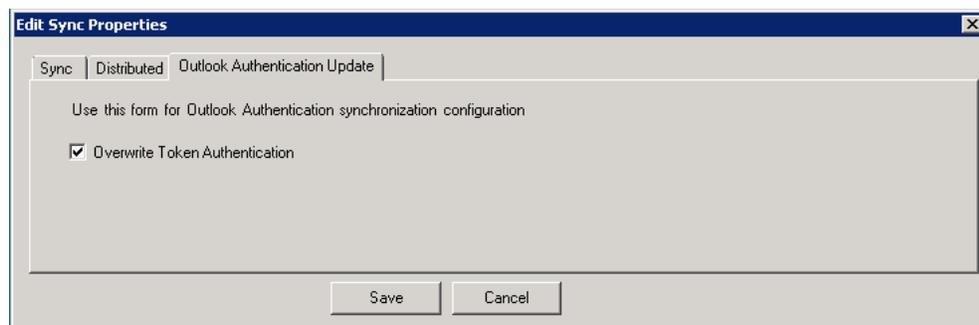
By default, an Outlook Authentication Update run will not overwrite an existing Outlook Authentication token, which means that only users without the token will be updated.

To update all users:

- 1) From the SyncManager main window, click the **Configure ...** button, that is located in the upper-right corner.



- 2) In the **Edit Sync Properties** window, select the **Outlook Authentication Update** tab.



- 3) Check the **Overwrite Token Authentication** box. Then click **Save**.

This setting will remain in effect until it is unset.

5.3.4.3. Install Outlook Extension 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 guidelines:

- 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, MessageOne recommends using the complete version number in the package name (for example, Outlook Extension 6-3-0-8015).

Task 5.15. Install the Outlook Extension using Group Policy:

NOTE GPO Deployment Requires Different Policies for x86 and x64 MSI

There are two versions of the Outlook Extension installer. The x86 MSI is for 32-bit Outlook versions. The x64 MSI is for 64-bit Outlook versions. For GPO deployment, you must create two policies, one for the x86 MSI and one for the x64 MSI.

Create a new GPO package using the Outlook Extension MSI.

- 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 x86 MSI you received from Support, select it, and click **Open**.
- 6) In the **Deploy Software** dialog, select **Assigned**, then click **OK**.
- 7) Link the GPO to the Organizational Unit (OU) that contains the target computers for the x86 MSI.
 - a. Right-click the OU and select **Link an Existing GPO**.
 - b. In the **Group Policy objects:** field, click the GPO.
 - c. Click **OK**.
- 8) Repeat this process to create a policy and select the OU for the x64 MSI.

Task 5.16. Upgrade the Outlook Extension using Group Policy:

Add the new Outlook Extension MSI to the existing policy for the x86 or x64 MSI.

- 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.

Task 5.17. Enable or disable the Outlook Extension using Group Policy:

NOTE **Disabling vs. Removing Outlook Extension**

These instructions allow you to *disable* the Outlook Extension using Group Policy. To *remove* the Outlook Extension from user systems, use the instructions the next section.

- 1) Follow Microsoft instructions and guidelines for distributing registry changes using Group Policy. See <http://technet.microsoft.com/en-us/library/bb727154.aspx> for information.
- 2) To *disable* the Outlook Extension, set the `LoadBehavior` value to 2 under the `HKEY_LOCAL_MACHINE\Software\Microsoft\Office\Outlook\Addins\ACM.Extensibility2` key.
- 3) To *enable* the Outlook Extension, set the `LoadBehavior` value to 3 under the `HKEY_LOCAL_MACHINE\Software\Microsoft\Office\Outlook\Addins\ACM.Extensibility2` key.

Task 5.18. Remove the Outlook Extension using Group Policy:

NOTE Disabling vs. Removing Outlook Extension

These instructions allow you to *remove* the Outlook Extension from user systems using Group Policy. To *disable* the Outlook Extension rather than remove it, use the instructions the previous section.

- 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**.

5.3.4.4. Installing Outlook Extension Manually

Task 5.19. Install the Outlook Extension manually:

- 1) Exit Outlook, if it is open.
- 2) Double-click the MSI file provided to you by Support to launch the InstallShield Wizard and follow the instructions. Installation may take a few minutes.
- 3) Launch Outlook. The Outlook Extension toolbar appears.

In 2007, the **Tools > Options** screen includes a tab for MessageOne EMS. Outlook 2010 and 2013 include the MessageOne EMS section under **File > Options > Add-Ins > Add-in Options**.

Task 5.20. Remove the Outlook Extension manually:

- 1) Exit Outlook, if it is open.
- 2) In Windows 7 and Windows 8, select **Start > Control Panel > Programs and Features**.
- 3) Locate the Outlook Extension and follow the instructions to remove it.

5.3.4.5. Customize Outlook 2010 and 2013 Ribbon

Administrators can customize the Outlook 2010 and 2013 Ribbon behavior for the Outlook Extension tab and group names via registry entries as described in: [Task 5.21., "Customize Outlook Ribbon Tab and Group Names" on page 105](#).

By default, this key and sub-keys are not present in the registry, causing Outlook Extension to use Product Name and a Vendor Name for display names in Ribbon.

NOTE OE Registry-key Customization Feature separate from Outlook 2010 and 2013's "Customize the Ribbon" feature

This registry-key customization feature is separate from Outlook 2010 and 2013's "Customize the Ribbon" feature, *and over-ridden* by Outlook 2010 and 2013's "Customize the Ribbon" settings.

If the end-user chooses to modify a tab or group's name using the Outlook 2010 or 2013 "Customize the Ribbon" feature, the extension's registry customizations will *no longer* apply.

Task 5.21. Customize Outlook Ribbon Tab and Group Names

- 1) Create the following registry entries:

Table 5-3 Outlook Extension Registry Keys

| Location | Key |
|--|--------------------------------------|
| TAB Registry Entry | |
| HKEY_CURRENT_USER\Software\MessageOne\EMS\Ribbon\Tab | ReadFromRegistry Label Visible |
| GROUPS Registry Entries | |
| HKEY_CURRENT_USER\Software\MessageOne\EMS\Ribbon\ArchivesGroup | ReadFromRegistry Label Visible |
| HKEY_CURRENT_USER\Software\MessageOne\EMS\Ribbon\ConfigGroup | ReadFromRegistry Label Visible |
| HKEY_CURRENT_USER\Software\MessageOne\EMS\Ribbon\ContinuityGroup | ReadFromRegistry Label Visible |
| HKEY_CURRENT_USER\Software\MessageOne\EMS\Ribbon\SecurityGroup | ReadFromRegistry Label Visible |

Where:

- ReadFromRegistry is of DWORD type
- Label is of String type
- Visible is of DWORD type

- 2) Set each ReadFromRegistry value to 1, to make OE implement the Label value and Visible status for each of the groups and the tab.

- If `ReadFromRegistry` is set to `0`, the corresponding group or tab is hidden (not displayed in the ribbon).
- 3) Set each `Label` value to the string that will be displayed as the tab or group's label.
 - If the `Label` value contains an empty string, the corresponding element of the Ribbon (tab or group) will not display any text, and this Ribbon element will appear empty. Therefore, it's not advisable to set the `Label` registry entry to an empty string.
 - 4) Set each `Visible` value to `1`, to indicate to Outlook Extension that this tab or group should be visible to the end-user.
 - If `Visible` is `0`, the corresponding group or tab is hidden (not displayed in the ribbon).

5.3.4.6. Troubleshoot Outlook Extension Installation

If the Extension toolbar or Tab does not appear in Outlook:

- 1) Exit Outlook and restart it.
- 2) Verify the Extension-related files are present; `C:\Program Files\MessageOne EMS\Outlook Addin\` and the registry keys listed below.

Table 5-4 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 | |

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:

In **Outlook 2007**: Open **Help > Privacy Options > Add-ins > Manage**, select **COM Add-ins**, and click **Go**.

In **Outlook 2010 and 2013**: Open **File > Options > Add-Ins > Manage**, select **COM Add-ins**, 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:
 - Click on the **Add** button in the **COM Add-Ins** dialog. Browse to the directory where Outlook Extension is installed and select `m1ext.dll`.
 - Once Outlook Extension appears in the list of **COM Add-Ins**, make sure to check the box next to it.
- 4) Ensure that Outlook Extension is not disabled by Outlook.
 - a. **In Outlook 2007:** Open **Help > Privacy Options > Add-ins > Manage**, select **Disabled Items**, and click **Go**.
In Outlook 2010 and 2013: Open **File > Options > Add-Ins > Manage**, select **Disabled Items**, and click **Go**.
 - b. If the Extension is there, select it, and click **Enable**.

5.3.5. Install Custom Forms for Storage Management

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.

Task 5.22. Add a new folder to Exchange Organizational Forms Library in Exchange 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 to add a user account under **Client Permissions** and under **Administrative Rights**. This account is used to publish the forms to this folder. Client Permissions needs to be the **Owner** Role. These permission levels are *required* to publish. The Administrative Rights Permissions must allow **Control Access**. Using a user account with any lower permission levels results in failure to publish.
- 12) Click **OK** to complete creating the new Organizational Forms Library.
- 13) Restart Microsoft Outlook® using the account previously specified with enhanced permissions.

Task 5.23. Create an organizational forms library in Exchange 2007/2010:

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

- 1) Click **Start**, point to **All Programs**.
- 2) Click **Microsoft Exchange 2007/2010 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 2007 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.

Task 5.24. 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>.

5.3.6. Deploy Wireless Continuity for BlackBerry

NOTE Wireless Continuity Installation Prerequisites

Before following the instructions in this section, ensure that all prerequisites listed under "[Wireless Continuity for BlackBerry Prerequisites](#)" on page 71 have been completed.

The deployment process for Wireless Continuity for BlackBerry includes two main steps:

- 1) Synchronizing your RIM data to the data center. See "[Synchronize RIM Data](#)" on page 111.
- 2) Distributing the client agent to your BlackBerry users. See "[Distribute the Client Agent](#)" on page 112.

5.3.6.1. Synchronize RIM Data

Prior to implementing Wireless Continuity for BlackBerry, you must have installed the SyncManager and RedirectorController service. After you have installed these components, you must synchronize data from your BlackBerry Enterprise Server (BES) to the EMS data center.

Task 5.25. Synchronize RIM data:

NOTE Security Settings for BES 4.x

A BES 4.x security setting may interfere with your ability to connect with the data center and synchronize your RIM data. If you are using BES 4.x, navigate within the BES 4.x Admin Console to **BlackBerry Manager > BlackBerry Domain > Servers > [your server] Connection Service tab > Edit Properties > TLS/HTTPS** and set **Allow untrusted HTTPS connections** to `True`.

- 1) Launch the SyncManager. On the SyncManager machine, select **Start > Programs > MessageOne > 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 the Wireless Continuity for BlackBerry feature is enabled for your organization but 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 autodetects and fills needed information in the **Database Instance Name** and **Database Name** columns. If it does not, type `Default` in the **Instance Name** field, then 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 is 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 CANNOT Modify BlackBerry Configuration Information

You cannot modify entries in the **BlackBerry Config** window. Instead, you must remove any incorrect entries 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 the Wireless Continuity for BlackBerry feature, and view information about devices using it. For information on each of these, see ["Wireless Continuity for BlackBerry Administration" on page 221](#).

5.3.6.2. Distribute the Client Agent

The client agent is deployed through the policy management features of BES 4.0+ (deployment *over-the-air*).

NOTE Contact Support for Deployment Best Practices

Because of the variables involved with upgrading software using the over-the-air deployment capabilities within BES, we recommend that you contact Support for the latest best practice deployment information specific to your circumstance when:

- Upgrading the Wireless Continuity for BlackBerry client agent software to a newer release
- Upgrading your BES server from one RIM release to another
- Migrating from one BES server to another
- Adding an additional BES server
- Decommissioning or retiring an existing BES server

See ["Getting Support" on page 339](#) for Support information.

You can push the Wireless Continuity for BlackBerry client agent software over the air to BlackBerry devices, including those that have never had the agent installed before and those that need 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.

NOTE Complete All Preliminaries Before Proceeding

Be sure that you have completed all installation preliminaries listed under ["Wireless Continuity for BlackBerry Prerequisites" on page 71](#), especially the steps for setting IT policies. If you have not completed these steps before you distribute the client agent, the deployment will fail.

5.3.6.3. 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 through 6.0 (other versions may work, but are not supported).

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

- It is vital that your BES has the latest device definitions from RIM, otherwise it may not know how to push out the agent. Use RIM KB13589 to update your BES4 server before proceeding. <http://btsc.webapps.blackberry.com/btsc/search.do?cmd=displayKC&docType=kc&externalId=KB13589>
- Download the agent and prepare the shared application directory. See ["Download the client agent:" on page 114](#).
- Index the Wireless Continuity for BlackBerry agent using RIM's `loader` command.
- Prepare the software configuration (including creating application policies). See ["Configure the agent:" on page 115](#)

- Assign software applications to users. See "[Assign software applications to users:](#)" [on page 116](#).

You can also use the over-the-air method to remove agent software from client devices. See "[Remove the BlackBerry agent for all users:](#)" [on page 116](#) and "[Remove the BlackBerry agent for one user:](#)" [on page 116](#).

Task 5.26. 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 will have one files and three folders: EMS BlackBerryClient.alx and folders labeled 4.1, 4.3, and 4.7. Inside each of these 3 folders are 4 additional files for the EMS Wireless Continuity for BlackBerry Client, each .cod file version to take advantage of APIs available in newer BlackBerry OS versions.
- 3) Copy these files and folders.
- 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 MessageOne.
- 7) Paste the folders and files you copied earlier into the MessageOne 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.

Task 5.27. 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 `MessageOne 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 the **Phone Access** field is set to `Allowed`.
 - 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 Remove`.
 - 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.

Task 5.28. 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.

Task 5.29. 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 take up to four hours, depending on your configuration.

Task 5.30. 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 take 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.

5.3.6.4. Distribution Over-the-Air for BES 5.x

The procedures provided in this section are for BlackBerry Administration Service version 5.1. BlackBerry devices must be version 4.1 through 6.0 (other versions may work, but are not supported).

CAUTION BES High Availability Not Validated

BES High Availability is not a validated configuration for Wireless Continuity for BlackBerry and is currently not supported.

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

- 1) Create and share the application directory. See ["Create and share the application directory:" on page 118.](#)
- 2) Define the application directory in the BlackBerry Administration Service. See ["Define the application directory in the BlackBerry Administration Service:" on page 118.](#)
- 3) Download the client agent. See ["Download the client agent:" on page 119.](#)
- 4) Add and publish the application. See ["Add and publish the application:" on page 119.](#)
- 5) Create and populate the software configuration. See ["Create and populate the software configuration:" on page 120.](#)
- 6) Optionally, you can configure the application deployment schedule to deploy as soon as possible. See ["Configure the application deployment schedule to deploy the application as soon as possible \(optional\):" on page 120.](#)
- 7) Assign the software configuration to users. See ["Assign the software configuration to a user:" on page 120.](#)
- 8) After you have created and assigned a software configuration to a user account (or after an existing software configuration assigned to a user account is changed), the BlackBerry Administration Service creates a job to deliver BlackBerry Device Software, BlackBerry Java® Applications, or application settings to BlackBerry devices. You can view the status of this job by following the instructions under ["View the status of a job:" on page 121.](#)

Task 5.31. Create and share the application directory:

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

NOTE BES Shared Application Directory

The purpose of this share is for storage of OTA applications. The Wireless Continuity Agent zip file does not need to be copied here. Using the process below, your BES will automatically import the files to this directory. Do not manually insert the files yourself.

- 2) Click the **Sharing** tab.
- 3) Click **Share this folder**.
- 4) Click **Permissions**.
- 5) Check **Full Control** (including Change and Read access), and close the Permissions window.

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.

Task 5.32. Define the application directory in the BlackBerry Administration Service:

- 1) Log into the BlackBerry Administration Service (BAS) for BES 5.
- 2) 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.
- 3) On the **Components** page, click the **BlackBerry Administration Service** link listed under the **Component** column.

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).

- 4) 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).
- 5) 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`.

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

Task 5.33. Download the client agent:

- 1) Contact Support to obtain the URL from which you can download the ZIP file containing the latest release of Wireless Continuity for BlackBerry.
- 2) Download and save the ZIP file to a location on your local machine or network.

Task 5.34. Add and publish the application:

- 1) Log into the BlackBerry Administration Service for BES 5.
- 2) From the BAS navigation menu, choose **BlackBerry Solution Management > Software > Applications**.
- 3) Select **Add or Update Applications**.

Browse to the ZIP file containing the client agent, which you should have already successfully downloaded using the instructions under "[Download the client agent:](#)" on page 119.

Click **Next**.

- 4) Click **Publish Application**.
- 5) Click the **More...** link.
- 6) Under **Version Information**, click the version of Wireless Continuity for BlackBerry you would like to deploy.
- 7) Click the **Application control policies** tab, then click **Edit application**.
- 8) Choose **Use custom application control policies** and provide the following information:
 - a. For **Required application name**, enter `Install Email Continuity Agent`
 - b. Set **Are internal network connections allowed** to `Allowed`
 - c. Set **Are external network connections allowed** to `Allowed`
 - d. Set **Is access to the phone API allowed** to `Allowed`
 - e. Set **List of external domains** to `*.messageone.com`
 - f. Click **Save All**.
- 9) Confirm that a new folder exists for the application under the Applications folder, and that `PkgDBCACHE.xml` and `Specification.pkg` exist in this new folder.

Task 5.35. 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) Set the **Disposition** for unlisted Applications to `Optional`, then click **Save**.
- 4) Click **View Software Configuration List** and select the new software configuration you created.
- 5) Click **Edit software configuration**, then click the **Applications** tab.
- 6) Click **Add Applications To Software Configuration**.
- 7) Click **Search**, then check the box beside the name of the new software configuration application. Set the following options:
 - a. Set the **Disposition** to `Required`.
 - b. Set the **Deployment** to `Wireless`.
 - c. Verify that the **Application control policy** is set to `Install Email Continuity Agent`.
- 8) Click **Add to Software Configuration**.
- 9) Click **Save All**.

Task 5.36. Configure the application deployment schedule to deploy the application as soon as possible (optional):

- 1) Log into the BlackBerry Administration Service for BES 5.
- 2) From the BAS navigation menu, choose **Devices > Deployment jobs**.
- 3) Click **Specify Job Schedule Settings**, then click **Edit Job Schedule Settings**.
- 4) Set the **Default Delay** to `1 minute`. (This setting can be left at the default.)
- 5) Click **Save All**. Note that the **Deploy Now** option no longer appears.

Task 5.37. Assign the software configuration to a user:

- 1) Log into the BlackBerry Administration Service for BES 5.
- 2) From the BAS navigation menu, choose **BlackBerry Solution Management > User**.
- 3) Click **Manage Users**.
- 4) Click **Search**, then choose a user account.
- 5) Click the **Software Configuration** tab, then click **Edit User**.

- 6) Under **Available software configurations**, select the software configuration, then click **Add**. The software configuration appears under **Current Software Configurations**.
- 7) Click **Save All**.

Task 5.38. View the status of a job:

- 1) Log into the BlackBerry Administration Service for BES 5.
- 2) From the BAS navigation menu, choose **Devices > Deployment jobs**.
- 3) Click **Manage deployment jobs**.
- 4) Click **Search** to search for a job. In the search results area, the **Status** column displays the status of the job.
- 5) To view more information about a job or to change a job, click the job ID.
- 6) Verify that the client application is installed on a device by choosing **Options > Advanced Options > Applications** on the BlackBerry device.

5.3.6.5. Communicate With Users of the BlackBerry Agent

As part of your deployment, consider informing users of the BlackBerry agent of any relevant information, including:

- ["Wireless Continuity for BlackBerry Prerequisites" on page 71](#)
- ["Wireless Continuity for BlackBerry Supported Configurations" on page 71](#)
- ["Wireless Continuity for BlackBerry Limitations" on page 72](#)

5.3.7. Mobile App Support Configuration

The following settings need to be configured before the Mobile Apps feature can be used.

5.3.7.1. Minimum Software Version

For the iOS App: The end-users must be using iOS 6.1 or later.

5.3.7.2. Enable Mobile Apps

Before the Mobile App service can be used, it must be enabled on the data center by Support. By default, this service should be enabled, but if you experience problems, please contact Support.

5.3.7.3. Configure Enabled Users

To enable end-user access to the Mobile App, users must be added to the Mobile Application Enabled Users list. See ["Mobile App Administration" on page 164](#)

5.4. Configure Enterprise Archive Features

The following features are available only for customers who have purchased the optional Enterprise Archive functions:

- ["Configure Scanning and Data Transfer for Storage Management Policies" on page 123](#)
- ["Harvester Operation and Data Logging" on page 126](#)
- ["Configure Scanning and Data Transfer for User Classification Retention Policies" on page 128](#)

5.4.1. Configure Scanning and Data Transfer for Storage Management Policies

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.

CAUTION Update Retention Policies For Reinstalled VaultBoxes

When updating from 6.4.x to 6.4.4 or higher, no additional steps are required.

For all other updates, when you uninstall and reinstall a VaultBox, you must manually update any retention policies that were associated with that VaultBox using the EMS Admin Console.

Until you reassociate the policies, new VaultBox will be unable to process messages for those policies and no messages from that VaultBox will be sent to the archive.

To do this, log into the EMS Admin Console and select the VaultBox that has been reinstalled. View the list of retention policies for the VaultBox, and for each policy, click **Edit**, then **Save**. You do not have to make any changes to the policies, just manually edit and save them. This step will reassociate the policies with the reinstalled VaultBox and messages will be processed.

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.

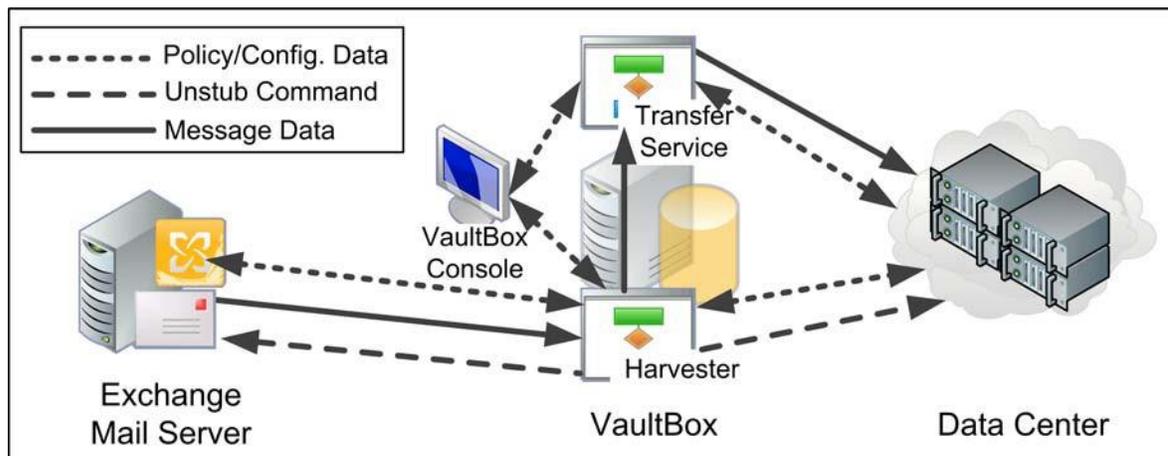


Figure 5-1 Data Transfer for Storage Management

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 > MessageOne > 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

Task 5.39. 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**.

Task 5.40. 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 resynchronize 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.

5.4.2. Harvester Operation and Data Logging

When the Harvester searches mailboxes for attachments 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 5-5](#).

- **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 5-5 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.

5.4.3. Configure Scanning and Data Transfer for 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' 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.

Before user classification retention policies can start archiving mail, you must first create a user classification retention policy in the EMS Admin Console, then set a task schedule for it in the VaultBox Console. See "[User Classification Retention Policies](#)" on page 34 for instructions on creating the policy. Then follow the instructions in this section to set the task schedule.

Task 5.41. 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 > MessageOne > 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 the mail server 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 mail 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 the mail server 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.

6. Administering EMS

This chapter covers the following topics relevant to administering the EMS system. You can find information relevant to administering specific EMS subcomponents in subsequent chapters.

- ["EMS Admin Console" on page 131](#)
- ["User Administration" on page 141](#)
- ["Mobile App Administration" on page 164](#)
- ["Mailboxes and Aliases" on page 165](#)
- ["Mailing Lists" on page 167](#)
- ["Notification" on page 167](#)
- ["View EMS Audit Reports" on page 179](#)
- ["Modify System Settings" on page 184](#)
- ["Help and Downloads" on page 202](#)
- ["Change Your EMS Password" on page 203](#)

6.1. EMS Admin Console

The EMS Admin Console is a web-based interface that allows you to perform most administrative functions for Email Continuity. Obtain the web address (*URL*) for the EMS Admin Console from your Support representative. You can log into the EMS Admin Console with the following types of EMS privileges. Help Desk Users and regular system users cannot log into the EMS Admin Console.

NOTE Restricting Access to the EMS Admin Console

Your organization can enable, partially enable, or disable access to the EMS Admin Console based on a user's IP address. See ["Network Restrictions" on page 191](#).

- **EMS Root Account:** There is only one EMS Root Account. The user name and password for this account are provided to you by Support.
- **Super Administrator:** Users with EMS Root Account permissions or super administrator permissions can create super administrator accounts. Users with super administrator permissions can perform the same EMS functions as the EMS Root Account. See ["Assign Super Administrator Privileges" on page 153](#).
- **EMS Administrator:** Users with EMS Root Account permissions or super administrator permissions can create EMS administrator accounts. EMS administrators can perform all of the functions in the EMS Admin Console except those reserved for super administrators and the EMS Root Account. See ["Assign](#)

["EMS Administrator Privileges" on page 155.](#)

CAUTION Protect the EMS Root Account

The EMS Admin 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 EMS Admin Console to grant Super Administrator privileges and EMS Administrator privileges to appropriate accounts rather than sharing the EMS Root Account.

Task 6.1. Log into the EMS Admin Console:

1) Launch a supported web browser and go to the URL provided by Support. The **Log In** page appears.

2) Enter the EMS account **Username**.

Usernames usually take the form of an email address (such as `user@genericorp.com`). Usernames must contain a total of 64 characters or fewer, including the @ symbol and the full domain name.

3) Enter the EMS account **Password**.

4) Click **Login**.

6.1.1. EMS Admin Console Home

The EMS Admin 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.

NOTE Some Described Features May Not Appear

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

- Admin Console Home
- Historical Mail
- User Administration
- Cloud Services
- Outlook Extension
- Mailboxes and Aliases
- Mailing Lists
- Notification
- Audit Reports
- System Settings
- Help and Downloads
- About
- Exit Admin Console
-
- Your Account
- Change Password

Readiness Check

- Office 365 Journaling Service:** EMS has not received a journaled message in the last 12 hours.
- On-Premises Journaling Service:** EMS has not received a journaled message in the last 12 hours.
- 11 other status checks passed. [▶ Show](#)

User Statistics

- DirectorySync** Retrieved 7 mailboxes. Synchronized 4 mailing lists that have 4 members.
- ContactSync** Retrieved 0 contacts and 0 PDLs, with 0 members from 0 mailboxes.
- CalendarSync** Retrieved 0 entries from 0 mailboxes.
- 43%** of users have not been welcomed. [Welcome Users ...](#)
- [View Synchronization Statistics](#)

Current Email Continuity State

Currently Email Continuity is active for a subset of your users. The inbound SMTP mail should be processed by your internet gateway. Mail for the affected users is rerouted to their Email Continuity mailboxes by the Email Continuity Redirectors. The Email Continuity dropbox is not active at this time.

The table below shows the number of users in each state by group and server

| Group/Server | Active | Recovery | Ready |
|--|--------|----------|-------|
| ▼ Exchange Routing Group (DWBGZMFD01QNBJR) | 1 | | 6 |
| ▶ LAB105EX-1 | 1 | | 6 |

To activate Email Continuity for additional users, click the **Activate** button and the activation wizard will guide you through the steps necessary to activate Email Continuity and notify your users.

[Activate](#)

When servers for active users are back online and receiving mail, click **Start Recovery** to notify these users and generate recovery archive to import their messages from Email Continuity back into the primary mail system.

[Start Recovery](#)

Current Tests

There are currently no Email Continuity tests under way.
You can't start a new Email Continuity test during emergency activation or recovery.

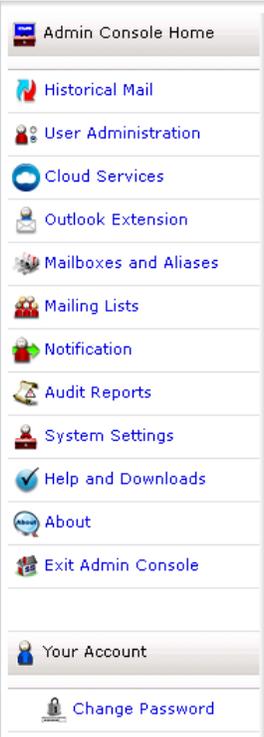
Email Continuity Activity Log

Some processes, such as the sending of large numbers of notification messages or generation of recovery archive files can take a few minutes to complete

The status of all running or recently completed processes is reported below.

| Description | User | Start Date | Progress |
|--|------|------------|----------|
| No processes are in progress currently | | | |

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

| | |
|---|--|
|  | <p>Links to sections describing menu items:</p> <ul style="list-style-type: none"> • "Administer Email Continuity" on page 204 • "Administer Historical Mail/Email Archive" on page 235 • "User Administration" on page 141 • "EMS Cloud Services" on page 305 • "Mobile App Administration" on page 164 • "Outlook® Extension Administration" on page 227 • "Mailboxes and Aliases" on page 165 • "Mailing Lists" on page 167 • "Notification" on page 167 • "View EMS Audit Reports" on page 179 • "Modify System Settings" on page 184 • "Help and Downloads" on page 202 • "Change Your EMS Password" on page 203 |
|---|--|

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 EMS Admin Console home page displays the sections described in [Table 6-1](#).

Table 6-1 EMS Admin Console Home Page Sections

| Section Name | Description |
|-----------------|---|
| System Updates | This section shows data center maintenance alerts from MessageOne. This section will not appear if there is no current alert. |
| Readiness Check | The service monitors the operational readiness of critical components and automatically sends notifications to designated administrators if their components are not working correctly. 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. |

Table 6-1 EMS Admin Console Home Page Sections

| Section Name | Description |
|---------------|--|
| 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. |

6.1.2. EMS 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 Management 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 ["Manage EMS Fault Alerts" on page 176](#) for information on fault notifications.) A readiness check displays indicating if addresses have been populated to the list, or not (See ["Fault Alert Users" on page 138](#))

The Readiness checks are described in the following table.

Table 6-2 Admin Console Readiness Checks

| Readiness Check | Description & Troubleshooting |
|-------------------------------------|--|
| *Default contacts synchronization | <p>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.</p> <p>If this readiness check fails, follow this procedure. After completing each troubleshooting step, please log into the EMS Admin Console to verify whether synchronization issue has been resolved.</p> <ol style="list-style-type: none"> 1 Verify that the machine running the SyncManager software is currently running and has outbound HTTPS (port 443) access to the Internet. HTTPS access can be verified by opening a web browser on the machine running the SyncManager and connecting successfully to the EMS URL provided to you by Support. If you are unable to connect to this URL, verify your proxy/firewall settings with your network administrator. 2 Verify that the Sync Manager Service is running in the Services Control Panel Applet. If the service is already running, restart the Sync Manager Service. 3 Check the Application Event Log for non-informational events from the Sync Manager Service. (Information events can generally be ignored.) 4 Launch the SyncManager (Start > Programs > MessageOne > SyncManager) and execute a manual sync. This may take some time to complete based on the size of your organization. Verify successful operation after the manual run dialog box has been dismissed. 5 If none of the steps above resolves the synchronization issue, contact Support for assistance. |
| *Default calendar synchronization | <p>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.</p> <p>If this readiness check fails, follow the procedure for troubleshooting Sync Manager issues under Default contacts synchronization above. After completing each troubleshooting step, please log into the EMS Admin Console to verify whether synchronization issue has been resolved.</p> |
| *Default directory synchronizations | <p>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.</p> <p>If this readiness check fails, follow the procedure for troubleshooting Sync Manager issues under Default contacts synchronization above. After completing each troubleshooting step, please log into the EMS Admin Console to verify whether synchronization issue has been resolved.</p> |

Table 6-2 Admin Console Readiness Checks

| Readiness Check | Description & Troubleshooting |
|---|--|
| *MX Record (per domain) | <p>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).</p> <p>If this readiness check fails, contact Support immediately for assistance.</p> |
| Default RIM Synchronization (for Wireless Continuity for BlackBerry only) | <p>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.</p> <p>If this readiness check fails, follow the procedure for troubleshooting Sync Manager issues under Default contacts synchronization above. After completing each troubleshooting step, please log into the EMS Admin Console to verify whether synchronization issue has been resolved.</p> |
| BlackberryContinuity Unsupported Version (for Wireless Continuity for BlackBerry only) | <p>If any BlackBerry devices are running unsupported versions of the Wireless Continuity for BlackBerry Agent, the following readiness check will display: <code>BlackBerry Continuity: 2 devices are running unsupported versions of the BlackBerry Continuity Agent.</code></p> <p>Refer to "Wireless Continuity for BlackBerry Requirements" on page 71 and the BlackBerry Administration > BlackBerry Device Information console page to ensure that all users and devices are using supported versions of the Agent.</p> |
| Authentication Manager (per server) (for Windows Authentication only) | <p>Reports the last time a particular Authentication Manager connected to the data center.</p> <p>If this readiness check fails, verify that the Authentication Manager service is running on the specified computer and that it can access the data center over port 443. If this does not resolve the issue, contact Support.</p> |
| Controller Status (per server) | <p>Reports the last time a particular RedirectorController connected to the data center.</p> <p>If this readiness check fails, verify that the Controller service is running on the specified computer and that it can access the data center over port 443. If this does not resolve the issue, contact Support.</p> |
| Redirector Status (per server) | <p>Reports Exchange servers that have a Redirector installed, as well as servers that have a Redirector installed, but are not currently in communication with at least one RedirectorController.</p> <p>The best practice recommendation is that all Exchange 2003 servers have the RedirectorSink installed, all Exchange 2007 Hub Transport servers have the RedirectorAgent installed, and that each of these be in communication with at least two RedirectorControllers.</p> <p>If this readiness check fails:</p> <ol style="list-style-type: none"> 1 Verify that the Controller service is running on the specified computer and that it can access the data center over port 443. 2 Verify that you are following the best practice above and all RedirectorSinks and Hub Transport servers are communicating with RedirectorControllers. 3 If these steps do not resolve the issue, contact Support. |

Table 6-2 Admin Console Readiness Checks

| Readiness Check | Description & Troubleshooting |
|--|---|
| *User Directory Status | <p>Reports user ID conflicts detected by the SyncManager using primary email address.</p> <p>If this readiness check fails, follow the instructions under "Resolve User ID Conflicts Manually" on page 162. If this does not resolve the issue, contact Support.</p> |
| VaultBox (for Historical Mail only) | <p>Reports the last time a VaultBox connected to the data center.</p> <p>If this readiness check fails, 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. If this does not resolve the issue, contact Support.</p> |
| Server Assigned to Replication Zone (for Historical Mail only) | <p>Reports any servers that are currently not assigned to a replication zone. All servers must be assigned to a replication zone.</p> <p>If this readiness check fails, follow the instructions under "Replication Zones" on page 236 to ensure that the reported servers are assigned to replication zones. If this does not resolve the issue, contact Support.</p> |
| Fault Alert Users | <p>A readiness check to determine if there are users assigned to receive fault alert notifications. If no users are assigned to receive alerts, then the following message is displayed: Fault Alert Users: No users have been configured to receive fault alerts.</p> <p>If users have been assigned, then the following message is displayed: Fault Alert Users: At least one user has been configured to receive fault alerts</p> <p>At least one user should be assigned to receive fault alerts to ensure error messages are not lost.</p> |
| Office 365 Journaling Service: Not Received Journalled Message | <p>This check is to verify whether or not a journaled message has been received in the last 12 hours. If it hasn't, this warning will display.</p> <p>Office 365 Journaling Service: EMS has not received a journaled message in the last 12 hours. This error message could also mean there is a misconfiguration, like an improper journaling address.</p> <p>If this readiness check is displayed, verify your Office 365 environment is set to send journaled messages. Contact Support if further assistance is required</p> |
| Office 365 Journaling Service: TLS Warning | <p>If a message is sent from Office 365 without using Transport Layer Security (TLS) a readiness check warning will appear.</p> <p>Office 365 Journaling Service: EMS received a journal message without Transport Layer Security (TLS).</p> <p>If this readiness check is displayed, verify your Office 365 environment is set to send secure messages. Contact Support if further assistance is required.</p> |

Table 6-2 Admin Console Readiness Checks

| Readiness Check | Description & Troubleshooting |
|---|---|
| Next Hop Status | <p>This check is a test over port 25 from the EMS to whatever next hop destinations are configured in "Email Routing: Configure Mail Routing" on page 186, to confirm they are capable of receiving messages from EMS.</p> <p>The status message: Next Hop Status: 2 of 4 next hops passed. Details... indicates the number of ports which passed the test, with the Details link showing a table detailing the test results. See "Next Hops Readiness Check" on page 188.</p> |
| On-Premises Journaling Service: Journaled Message Retention | <p>If EMS detects an Exchange mailbox that is enabled for Exchange Envelope Journaling, but is not in an Email Archive retention policy, a readiness check will display: Journaled Message Retention: 22 journaled mailboxes are not included in a retention policy. Show List... Click on Show List to see the mailboxes (first 50 are shown, remainder can be downloaded into CSV file).</p> |
| On-Premises Journaling Service: Non-Journaled Message Retention | <p>If EMS detects an Exchange mailbox that is in an Email Archive retention policy, but not enabled for Exchange Envelope Journaling, a readiness check will display: Non-Journaled Message Retention: 2 non-journaled mailboxes are included in a retention policy. Show List... Click on Show List to see the mailboxes (first 50 are shown, remainder can be downloaded into CSV file).</p> |
| On-Premises Journaling Service: Hidden Journaled Mailboxes | <p>If a mailbox or distribution list is hidden or disabled, but is enabled for Exchange Envelope Journaling, a readiness check will display: Hidden Journaled Mailboxes: 1 hidden/deleted, journaled mailboxes are not included in a retention policy. Show list... Click on Show List to see the mailboxes (first 50 are shown, remainder can be downloaded into CSV file).</p> |
| On-Premises Journaling Service: Not Received Journaled Message | <p>This check is to verify whether or not a journaled message has been received in the last 12 hours. If it hasn't, this warning will display. On-Premises Journaling Service: EMS has not received a journaled message in the last 12 hours.</p> <p>This error message could also mean there is a misconfiguration, like an improper journaling address.</p> <p>If this readiness check is displayed, verify your Exchange environment is set to send journaled messages to EMS. Contact Support if further assistance is required.</p> |

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 EMS Admin Console. During this waiting period, `Updating Mail Routing Configuration` appears as a pending task in the Activity Log section.

6.1.3. 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 Management Services Authentication Manager readiness check entry.

Table 6-3 Authentication Manager Status icons

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

6.1.4. 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 Management Services RedirectorController/RedirectorSink status screen click the **Details** link in the Email Management Services RedirectorSink readiness check entry.

Table 6-4 Redirector Status Icons

| Icon | Definition |
|---|--|
|  | Connected to the Email Management Services server. |
|  | Disconnected from the Email Management Services server. |
|  | 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. |

6.2. User Administration

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

NOTE EMS Usernames

Usernames are generally in the form of email addresses (such as `user@genericcorp.com`). Usernames must contain a total of 64 characters or fewer, including the @ symbol and the full domain name.

6.2.1. Search 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.

Task 6.2. Search user information:

- 1) From the EMS Admin 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.
 - The **State** column indicates the user's readiness for activation.
 - The **Journaling Service** column is displayed if Cloud services or On-premises journaling services are enabled. Displays three values: [[words here]]
 - **N/A**: Non-journaled on-premises Exchange user.
 - **Office 365**: Office 365 journaling service user. See ["About EMS Cloud Services" on page 305](#).
 - **On-Premises**: On-premises Exchange Envelope Journal service user. See ["About Email Archive On-Premises Journaling" on page 26](#)
 - 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.

6.2.2. Reset 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:

- ["Reset an Individual User's Password" on page 143](#)
- ["Reset Multiple Passwords By Template" on page 144](#)
- ["Reset Multiple Passwords by CSV Import" on page 146](#)

NOTE Password Change Confirmation SMS Not Sent During Ready or Recovery State

If a user's password is changed when Email Continuity is in the *Ready* or *Recovery* states, and the user's notification setting is to receive text notifications via SMS, the user will **not** receive a password change confirmation SMS message. The password change notification is sent to the user's primary email address.

However, if the user's password is changed when Email Continuity is in the *Active* state, and the user's notification setting is to receive text notifications via SMS, the user **will** receive a password change confirmation SMS message.

6.2.2.1. Reset 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.

Task 6.3. 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 appears.
- 3) In the **New Password** box, type a new password.
- 4) In the **Confirm Password** box, retype the new password.
- 5) Click **Submit**.

6.2.2.2. Reset 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.

Task 6.4. Change multiple users' passwords:

- 1) From the EMS Admin 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@genericcorp.com`, the resulting new password would be `!Lilajones_Aug-2010%`.
 - If you applied this pattern in November 2009 for user `samuels.JK@genericcorp.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@genericcorp.com`, the resulting new password would be `john_doe`.
 - If you applied this pattern for user `lilajones@genericcorp.com`, the resulting new password would be `lilajones`.
 - If you applied this pattern for user `samuels.JK@genericcorp.com`, the resulting new password would be `samuels.jk`.
- c. Choose **Username** to reset the passwords for all selected users to each user's EMS 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 EMS 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.

6.2.2.3. Reset Multiple Passwords by CSV Import

You can use the EMS Admin Console to import passwords in bulk using a CSV (comma separated values) file with UTF-8 encoding. This feature works only for users already in the system. You cannot create users using this import file.

Task 6.5. 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 EMS Admin 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 6-5 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. **Required.**

- **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. **Optional.**
- **Welcomed** flag: A flag indicating whether the user has already been welcomed to the system. **Optional.**
 - 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. **Optional.**
 - 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 with UTF-8 encoding.

NOTE Use UTF-8 Encoding for Password Import File

The CSV file you use for importing passwords must use UTF-8 encoding. Otherwise, passwords containing non-ASCII characters will be imported incorrectly, and users will be unable to log in.

Task 6.6. Import passwords by CSV file:

- 1) From the EMS Admin 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 "[Create a password import CSV file:](#)" on page 146.

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.

6.2.3. Change 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 "[Exclude Users or Mailboxes](#)" on page 160. 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`.

Task 6.7. Change status flags for users:

- 1) From the EMS Admin Console, click **User Administration**.
- 2) Click **User Information**. The **User Account Information** screen appears.
- 3) Click **Bulk Reset Flags**. The **Select Users** screen appears.
- 4) Click the appropriate tab to identify the users to change status for. You can select by:
 - Predefined **User Sets**:
 - All Users
 - Users who have never logged in
 - Users not yet welcomed
 - Users who have been sent a welcome message
 - Excluded users
 - Users who have opted out of providing notification dataClick the button next to the appropriate set.
 - **Mailing Lists**: Search by Email or by Name, using % as a wildcard.
 - **Servers**: Click the check box by the appropriate server.
 - Individual **Users**: Search by Email or by Name, using % as a wildcard.
- 5) Click the check box to select a user or group from the left list.
- 6) Click **Add**. The selected users move to the **Change status of these users** list.
- 7) Click **Next**.
- 8) For each of the status settings, select one:
 - **Do not change** (Default)
 - **Set flag**
 - **Clear flag**
- 9) Click **Next**.
- 10) To see a list of all users affected by the change, click **Show Affected Users**. If the list is incomplete, or you want to make other changes, click **Back**. If you are satisfied with the list of users, click **Submit**.

6.2.4. Update a User's Contact Information

NOTE Integration with AlertFind

If your Email Continuity application is integrated with AlertFind, changes to user's notification options must be managed from within AlertFind. Consequently, some of the functionality described in this chapter may not appear in your EMS Admin Console.

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.

Task 6.8. 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 appears.
- 2) Update any information as necessary. When finished, click **Submit**.

6.2.5. Define 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.

Task 6.9. Create a user set:

- 1) From the EMS Admin Console, click **User Administration**.
- 2) Click **User Sets**. The **User Sets** page appears.
- 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 6-6 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**.

6.2.6. User Permission Levels

EMS provides different levels of user permissions depending on the user's role. [Table 6-7](#) shows the different levels of EMS user permission roles, and which functions each role can perform.

Table 6-7 User Permissions Matrix

| Action | EMS Root Account | SuperAdmin Account | Administrator | Help Desk User | User |
|---|------------------|--------------------|---------------|----------------|------|
| Change EMS Root Account Password | X | | | | |
| Change Authentication Method | X | | | | |
| Install EMS Software | X | X | | | |
| Create Super Administrators | X | X | | | |
| Create EMS Administrators | X | X | | | |
| Create Help Desk Users | X | X | | | |
| Change Imported User Attributes | X | X | | | |
| Change Global Address List Attributes | X | X | | | |
| Configure Email Routing | X | X | | | |
| Modify Email Disclaimer | X | X | | | |
| Change AlertFind Mapping Settings | X | X | | | |
| Configure User ID Conflict Resolution | X | X | | | |
| Set User Deletion Notification Thresholds | X | X | | | |
| Customize Home Page | X | X | | | |
| Customize Welcome Wizard | X | X | | | |
| View Undeliverable Mail | X | X | | | |
| Create Reviewer Groups | X | X | | | |
| Manage Journaling Services | X | X | | | |
| Activate Email Continuity | X | X | X | | |
| Install/Configure RedirectorManager | X | X | X | | |
| Install BlackBerry Agent | X | X | X | | |
| Create User Authentication Tokens | X | X | X | | |
| Install/Configure VaultBox | X | X | X | | |
| View Audit Reports | X | X | X | | |
| Create New Mailboxes | X | X | X | | |
| Add/Manage Users | X | X | X | | |
| Create Incoming Mail Aliases | X | X | X | | |
| Send Custom Notifications | X | X | X | | |
| View User Information | X | X | X | X | |
| Reset User Passwords | X | X | X | X | |
| Log In to EMS | X | X | X | X | X |
| Access Personal Mailbox | | X | X | X | X |
| Change Personal Password | | X | X | X | X |

6.2.7. Assign Super Administrator Privileges

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

EMS Super Administrators can perform more actions than regular EMS Administrators. The table below summarizes functions available to Super Administrators and the EMS Root Account that are not available to regular EMS Administrators.

Table 6-8 Features Limited to Super Administrators or EMS Root Account

| Feature | See Also |
|--|--|
| Creating Super Administrators | This section |
| Creating EMS Administrators | "Assign EMS Administrator Privileges" on page 155 |
| Creating Help Desk Users | "Assign Help Desk Privileges" on page 156 |
| Changing the user attributes imported from Active Directory | "User Import: Change User Attributes Imported from Active Directory" on page 184 |
| Changing the Global Address List attributes displayed in the webmail interface | "Address List Display: Display Global Address List (GAL) Attributes" on page 185 |
| Configuring email routing | "Email Routing: Configure Mail Routing" on page 186 |
| Modifying the organization's email disclaimer | "Email Disclaimer" on page 194 |
| Changing AlertFind mapping settings | "AlertFind Mapping" on page 195 |
| Configuring automatic resolution of conflicting user IDs | "Resolve User ID Conflicts Automatically" on page 162 |
| Setting user deletion notification thresholds for SyncManager | "Sync Notify Settings" on page 197 |
| Customizing the Home Page | "End User Pages Settings" on page 198 |
| Changing the EMS Root Account password (EMS Root Account only) | "Change Your EMS Password" on page 203 |
| Installing RedirectorSinks using the RedirectorManager | "Install RedirectorManager on a Standalone Server" on page 90 |
| Creating Reviewer Groups for Email Archive | "Reviewer Groups" on page 247 |

Task 6.10. Create a super administrator:

- 1) Log into the EMS Admin Console using an existing *super administrator* account or the *EMS Root Account* provided by Support. See ["EMS Admin Console" on page 131](#) for more information.

NOTE Log in Using a Super Administrator or EMS Root Account

You can only access the Super Administrator features by logging into the EMS Admin Console with the EMS Root Account or another super administrator account.

- 2) From the EMS Admin 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 Administrator role. You can assign this role to any existing EMS account. If you need to create a new account, see ["Add Mailboxes \(Users\) Manually" on page 165](#) 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.

Task 6.11. Remove super administrator privileges:

- 1) Log into the EMS Admin Console using an existing *super administrator* account or the *EMS Root Account* provided by Support. See ["EMS Admin Console" on page 131](#) for more information.

NOTE Log in Using a Super Administrator or EMS Root Account

You can only access the Super Administrator features by logging into the EMS Admin Console with the EMS Root Account or another super administrator account.

- 2) From the EMS Admin 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 EMS user privileges.

6.2.8. Assign EMS Administrator Privileges

EMS Administrators can use all the features of the EMS Admin Console except those explicitly limited to Super Administrators and the EMS Root Account. (These exceptions are listed under ["Assign Super Administrator Privileges" on page 153.](#)) Creating EMS administrators helps you track actions taken in the system more accurately.

Task 6.12. Assign administrative privileges to an account:

- 1) Log into the EMS Admin Console using an existing *super administrator* account or the *EMS Root Account* provided by Support. See ["EMS Admin Console" on page 131](#) for more information.
- 2) From the EMS Admin Console, click **User Administration**.
- 3) Click **Administrators**. The **Administrators** page appears.
- 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 appears near the top of the page.

Task 6.13. Remove administrative privileges from an account:

- 1) Log into the EMS Admin Console using an existing *super administrator* account or the *EMS Root Account* provided by Support. See ["EMS Admin Console" on page 131](#) for more information.
- 2) Click **Administrators**. The **Administrators** page appears.
- 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.

6.2.9. Assign 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 EMS users by Super Administrators or by the EMS Root Account. EMS Administrators can view the list of Help Desk users, but cannot grant or remove Help Desk privileges.

Task 6.14. Grant a user Help Desk privileges:

- 1) Log into the EMS Admin Console using an existing *super administrator* account or the *EMS Root Account* provided by Support. See "[EMS Admin Console](#)" on [page 131](#) for more information.
- 2) Click **User Administration**.
- 3) Click **Help Desk Users**. The **Help Desk Users** page appears.
- 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 appears near the top of the page. When the Help Desk user logs in to the service during an activation, a help desk icon appears along with a link to the **User Information** screen in the EMS Admin Console. From the **User Information** screen, the Help Desk user can reset users' passwords.

Task 6.15. Remove Help Desk privileges from an account:

- 1) Log into the EMS Admin Console using an existing *super administrator* account or the *EMS Root Account* provided by Support. See "[EMS Admin Console](#)" on [page 131](#) for more information.
- 2) Click **Help Desk Users**. The **Help Desk Users** page appears.
- 3) Locate the appropriate user and click the **Remove** check box next to the name. Click **Remove**.

6.2.10. Review Login Status

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

Task 6.16. Review login status:

- 1) From the EMS Admin Console, click **User Administration**.
- 2) Click **Login Status**. The **Login Status** screen appears.
The **Login History** section shows how many users are in the system.

NOTE Login Status Includes Webmail Logins Only

If the Outlook® Extension has been installed, users may be using Outlook during the activation. These users are not counted in the Login History.

- 3) To see the login status for a user, click **Show last login**. The **Login Report** screen appears.
- 4) To find the most recent login for a particular user:
 - a. In the **Search for Users** field, type the name or email address (or a partial value with % as a wildcard).
 - b. 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:
 - a. In the **Login Status** screen **Previous Activations** section, select a past activation from the drop-down list.
 - b. Click **Show last logon**. 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.

6.2.11. Export 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 6-9, "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 ["User Import: Change User Attributes Imported from Active Directory" on page 184](#).

Table 6-9 Exported User Data

| Category | Data |
|--|-------------------------------------|
| User Account | Primary Email |
| | Display Name |
| | Journaling Service |
| | System ID |
| | Last Login |
| | Welcome Message Sent status |
| | Excluded (status) |
| | Has permanent password (status) |
| | Opted Out of Notifications (status) |
| Contact Information: Field requires manual entry by end user into their EMS Profile | Street Line 1 |
| | Street Line 2 |
| | City |
| | State/Province |
| | Zip/Postal Code |
| | Country |
| | Home Number |
| | Work Number |
| Notification Email Addresses to be used by automated EMS Alerting systems: | Cell Number |
| | Wireless Forwarding Address |
| | Email Address 1 |
| | Email Address 2 |
| | Email Address 3 |

Table 6-9 Exported User Data (Continued)

| Category | Data |
|--|--------------------|
| End User's Emergency Contacts: Field requires manual entry by end user into their EMS Profile | 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 |
| Additional data Automatically synchronized from your organization's Active Directory: | Country/Region |
| | Comment |
| | Company |
| | Department |
| | Fax |
| | First Name |
| | Home Phone |
| | Address-Home |
| | City |
| | Cell Phone |
| | Phone-Mobile-Other |
| | Pager |
| | Office |
| | Street Address |
| | Zip Code |
| | Last Name |
| | State |
| | Street-Address |
| Street Address | |
| Phone Number | |
| Title | |

Task 6.17. Generate a CSV spreadsheet of emergency contact data for all users:

- 1) From the EMS Admin 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.

6.2.12. Exclude Users or Mailboxes

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 ["Change Status for Multiple Users" on page 148](#).

Task 6.18. Exclude a user:

- 1) From the EMS Admin 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**.

Task 6.19. Remove individual users from the Excluded list (reinstate them in the system):

- 1) From the EMS Admin 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.

Task 6.20. Remove multiple users from the Excluded list (reinstate them in the system):

- 1) From the EMS Admin 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**.

6.2.13. Resolve User ID Conflicts

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 ["Resolve User ID Conflicts Automatically" on page 162](#)) and Super Administrators and EMS Administrators can resolve conflicts manually using the processes described under ["Resolve User ID Conflicts Manually" on page 162](#).

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.

6.2.13.1. Resolve User ID Conflicts Automatically

In some situations, such as when you are transitioning from one server version to another where only one Administrator category is permitted, SyncManager may detect high numbers of user ID conflicts. (See ["Configure the SyncManager" on page 82](#) 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 EMS administrator. See ["Resolve User ID Conflicts Manually" on page 162](#) 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.

This attribute can be set from the System Settings menu, see ["Task 6.54. Configure the system-wide method for resolving user ID conflicts:" on page 197](#)

6.2.13.2. Resolve User ID Conflicts Manually

Super Administrators and EMS Administrators can resolve conflicts manually using the processes described in this section.

Task 6.21. 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 6-10](#).
- 2) From the EMS Admin 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 6-10 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 |

Task 6.22. 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**.

6.3. Mobile App Administration

The EMS Mobile Apps provide the ability for end-users to access Email Continuity and Email Archive functionality through a native application interface. The features available in the mobile applications depend upon which EMS services have been purchased by the organization.

Before the Mobile App service can be used, it must be configured. See "[Mobile App Support Configuration](#)" on page 121

6.3.1. Enable Mobile App End-User Access

To enable end-user access to the Mobile App, the users must be added to the **Mobile Application Enabled Users** list.

To establish a dynamic list of enabled users, create a Mailing List or User Set populated with desired users, or assign users to specific server(s), then select that Mailing List, Users Set, or Server(s) to be the Mobile Application Users. When users are added to or removed from the dynamic lists, that change is automatically reflected in the Mobile Application Users list.

Task 6.23. Enable End-User Mobile App Access

- 1) In left-hand navigation menu, click **Mobile App Administration** button.
The **Mobile Application Enabled Users** page appears.
- 2) Click the **Select Users** link.
- 3) In the user-picker, select the appropriate tab: **Users Sets**, **Mailing Lists**, **Servers**, or **Users**.
- 4) Check the box next to the desired item(s) and click the **Add** button to copy the item to the right-hand pane.
- 5) When all users have been copied to the right-hand pane, click **Next**.
- 6) On the confirmation page, verify that the correct users have been enabled. If so, click **Submit**. Otherwise, click **Back** to return to the user-picker and revise the selection.

6.3.2. Users Download & Access Mobile App

After enabled, the end-users need to install the iOS App from the iTunes store.

The iOS app's name is `MessageOne Email Management`, with a short name of `Email Mgmt`. The app's logo is displayed on the right.

The user initially authenticates with their EMS username and password.

Once authenticated, users are asked to enter a PIN, which is used to unlock the app for future use.

For more information, end-users can see the *Mobile Access User Guide*.



6.4. 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.

NOTE Requirements for EMS Usernames and Mailing Lists (Distribution Lists)

Whether you import users and mailing lists from your primary mail system or you create them manually using the EMS Admin Console, the usernames and mailing list aliases you use must adhere to the following requirements:

- Usernames and distribution list names must not start with the pound character (#). EMS will disregard any mailing list or user name that begins with the pound character.
- Usernames are generally in the form of email addresses (such as `user@genericorp.com`). Usernames must contain a total of 64 characters or fewer, including the @ symbol and the full domain name.
- EMS requires that distribution list names contain 128 characters or fewer. Distribution lists with names larger than 128 characters will not receive messages through EMS. Messages sent to these distribution lists will not archive correctly and can prevent messages from being received by other users during an activation. Ensure that the names of all distribution lists and mailing lists in EMS contain 128 characters or fewer.

NOTE Excluding Mailboxes

See ["Exclude Users or Mailboxes" on page 160](#) for instructions on excluding resource mailboxes from EMS.

6.4.1. Add Mailboxes (Users) Manually

Usually, users and mailboxes are added to the system during regular synchronization of your primary mail system with the EMS data center. However, EMS root users, Super Administrators, and Administrators can also add mailboxes to the system manually.

Task 6.24. Add a mailbox (user) to EMS:

- 1) From the EMS Admin Console, click **Mailboxes and Aliases**. The **Additional Mailboxes and Aliases** screen appears.
- 2) Click **Create Mailbox**. The **Create Mailbox** screen appears.
- 3) In the **Display Name** field, type a name.
- 4) In the **Email Address** field, type an email address, which will become the user's EMS username.

NOTE EMS Usernames

Usernames are generally in the form of email addresses (such as `user@genericorp.com`). Usernames must contain a total of 64 characters or fewer, including the @ symbol and the full domain name.

- 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.

6.4.2. Create Aliases

EMS root users, Super Administrators, and Administrators can create aliases within EMS.

Task 6.25. Create an alias:

- 1) From the EMS Admin 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.

6.5. Mailing Lists

EMS synchronizes your existing distribution 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 distribution lists as activation or recovery units. For example, it might be best to activate the members of a building-specific distribution list or to recover a small set of users before a full-scale recovery.

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

NOTE EMS Mailing Lists

EMS requires that distribution list names contain 128 characters or fewer. Distribution lists with names larger than 128 characters will not receive messages through EMS. Messages sent to these distribution lists will not archive correctly and can prevent messages from being received by other users during an activation. Ensure that the names of all distribution lists and mailing lists in EMS contain 128 characters or fewer.

Task 6.26. View mailing lists and members of each list:

- 1) In the EMS Admin 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.

6.6. Notification

The **Notification** screens in EMS 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.

6.6.1. Welcome 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. As part of sending the welcome message, temporary passwords are set automatically for the message recipients, 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 email address 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.
- 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 is considered *responded* when they have logged in to the service and provided notification data.
- 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.

Further information on the welcome process:

- 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 ["Change Status for Multiple Users" on page 148](#).

- Audit Report Available For Manual Welcome Process Actions
See ["Notification Reports" on page 181](#) for audit information on changes to notification settings and users welcomed. These reports show changes made from the EMS Admin Console.

6.6.1.1. Best Practices for Welcoming for 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`.

6.6.1.2. Welcome Message Variables

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.

6.6.1.3. Send Welcome Message to New Users

This option sends a Welcome Message to users who have not yet received a welcome message.

The user-picker in the steps includes only users who have not received a message. If a mailing list is selected, the welcome message will be sent to users within that mailing list who have not yet received a welcome message.

To re-send a message to any user, see ["Re-send Welcome Message to Any User\(s\)" on page 171](#)

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

Task 6.27. Send a welcome message to users not yet welcomed:

- 1) In the EMS Admin Console, click **Notification**.
- 2) Click **Welcome New Users**.
- 3) Click **Welcome users who have not been sent an initial welcome message...**
 - To see a list of the users who have not yet been welcomed, click the **Show users...** link above the **Welcome users who have not been sent an initial welcome message...** link.

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 **Message 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, Mailing List, Server, or individually by User.

This user-picker in the steps includes only users who have not received a message. If a larger grouping is selected, such as a mailing list, the welcome message will be sent to users within that mailing list who have not yet received a welcome message.

- a. If you select the **Mailing Lists** or **Users** tab, in the **Search** box type an email address or name (or part using % as a wildcard) and search for the results. Then click the listed mailing list or user to select.
 - b. If you select the **User Sets** or **Servers** tab, click a checkbox to select it.
- 9) Click **Add** to copy the selected items to the right-hand pane.

- 10) Continue selecting users until all intended recipients are listed in the selected users list.
- 11) Click **Next**. The **Confirm** screen appears.
- 12) To see a list of recipients, click **Show Affected Users**. Review the message text.
- 13) Click **Send**.

6.6.1.4. Re-send Welcome Message to Any User(s)

This option re-sends a Welcome Message to the user(s) selected.

To re-send a message to users who have not yet received a welcome message, see ["Send Welcome Message to New Users" on page 170](#)

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

Task 6.28. Re-send a welcome message to any user:

- 1) In the EMS Admin Console, click **Notification**.
- 2) Click **Welcome New Users**.
- 3) Click **Re-send welcome message to any user(s)...**
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 **Message 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 Sets, Servers, Mailing Lists, or individually by User.
This user-picker contains all users in the system.
 - a. If you select the **Mailing Lists** or **Users** tab, in the **Search** box type an email address or name (or part using % as a wildcard) and search for the results. Then click the listed mailing list or user to select.
 - b. If you select the **User Sets** or **Servers** tab, click a checkbox to select it.
- 9) Click **Add** to copy the selected items to the right-hand pane.
- 10) Continue selecting users until all intended recipients are listed in the selected users list.

- 11) Click **Next**. The **Confirm** screen appears.
- 12) To see a list of recipients, click **Show Affected Users**. Review the message text.
- 13) Click **Send**.

6.6.1.5. Re-send Welcome Message to Users Who Have Not Responded

Users are considered to have *responded* to the welcome message when they have:

- Logged in, thereby requiring they create a new password for themselves
- Provided notification information.

This option re-sends a Welcome Message to users who have logged in, but not provided notification information.

The user-picker in the task below includes only users who have not responded. If a mailing list is selected, the welcome message will be sent to users within that mailing list who have not yet responded to the welcome message.

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

Task 6.29. Re-send welcome message to users who have not responded:

- 1) In the EMS Admin Console, click **Notification**.
- 2) Click **Welcome New Users**.
- 3) Click **Re-send welcome messages to users who have not responded...**
 - This link will appear grayed out if all users who have been sent a welcome message have logged in and entered notification information.
 - To see a list of the users who have not responded, click the **Show users...** link above the **Re-send welcome messages to users who have not responded...** link.

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 **Message 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, Mailing List, Server, or individually by User.

This user-picker in the steps includes only users who have not responded to the welcome message. If a larger grouping is selected, such as a mailing list, the welcome message will be sent to users within that mailing list who have not yet responded.

- a. If you select the **Mailing Lists** or **Users** tab, in the **Search** box type an email address or name (or part using % as a wildcard) and search for the results. Then click the listed mailing list or user to select.
 - b. If you select the **User Sets** or **Servers** tab, click a checkbox to select it.
- 9) Click **Add** to copy the selected items to the right-hand pane.
 - 10) Continue selecting users until all intended recipients are listed in the selected users list.
 - 11) Click **Next**. The **Confirm** screen appears.
 - 12) To see a list of recipients, click **Show Affected Users**. Review the message text.
 - 13) Click **Send**.

6.6.1.6. Re-send Welcome Message to Users Who Have Not Set a Permanent Password

This option sends a Welcome Message to users who have not set a permanent password.

The user-picker in the task below includes only users who have not set a permanent password. If a mailing list is selected, the welcome message will be sent to users within that mailing list who have not yet set a permanent password.

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

Task 6.30. Send welcome message to users who have not set a permanent password:

- 1) In the EMS Admin Console, click **Notification**.
- 2) Click **Welcome New Users**.
- 3) Click **Send welcome messages to users who do not have a permanent password...**

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 **Message 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, Mailing List, Server, or individually by User.
This user-picker in the steps includes only users who have not set a permanent password. If a larger grouping is selected, such as a mailing list, the welcome message will be sent to users within that mailing list who have not yet set a permanent password.
 - a. If you select the **Mailing Lists** or **Users** tab, in the **Search** box type an email address or name (or part using % as a wildcard) and search for the results. Then click the listed mailing list or user to select.
 - b. If you select the **User Sets** or **Servers** tab, click a checkbox to select it.
- 9) Click **Add** to copy the selected items to the right-hand pane.
- 10) Continue selecting users until all intended recipients are listed in the selected users list.
- 11) Click **Next**. The **Confirm** screen appears.
- 12) To see a list of recipients, click **Show Affected Users**. Review the message text.
- 13) Click **Send**.

6.6.1.7. Enable/Disable Automatic Welcome Messages

This option enables the ability for the EMS system to automatically send a welcome message to any new users who have not been sent one.

The automatic welcome message is sent once per week.

By default, the automatic welcome feature is turned off.

Task 6.31. Automatically send welcome messages to new users:

- 1) In the EMS Admin Console, click **Notification**.
- 2) Click **Welcome New Users**.

- 3) Click ***Automatically welcome new users...***
The **Automate Welcome Message** page appears.
- 4) Click the ***Enable automated welcome message*** checkbox.
- 5) In the **Subject** box, make any necessary changes to the default text.
- 6) In the **Message Text** box, make any necessary changes to the default text.
- 7) Click ***Submit***.

6.6.2. Send Reminders

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

- Those who have not responded to the welcome message.
A user is considered to have *not* responded when they have logged in to the system and created a permanent password, but not entered notification information.
- 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.

Task 6.32. Send a reminder:

- 1) In the EMS Admin Console, click ***Notification***.
- 2) Click ***Reminders***. The **Reminders** screen appears.
- 3) Select the reminder to send by clicking one of the following:
 - ***Send a reminder to welcomed users who have not responded,***
 - ***Send a reminder to users 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 Lists** or **Users** 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 **User Sets** or **Servers** tab, click a checkbox 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**.

6.6.3. Manage EMS 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 ["EMS Readiness Checks" on page 135](#)).
- The percentage of users or mailing list members exceeds the configured threshold (see ["Sync Notify Settings" on page 197](#)).

Task 6.33. Add a user to the fault alerts list:

- 1) In the EMS Admin Console, click **Notification**.
- 2) Click **Fault Alerts**. The **Fault Notification** page appears.
- 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 appears near the top of the page.

Task 6.34. Remove a user from the fault alerts list:

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

6.6.4. Manage Email Continuity Transition Alerts

The transition alert list identifies users who should automatically receive notifications whenever Email Continuity changes state: 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 "[View Email Continuity Audit Reports](#)" on page 229.

Task 6.35. Add users to the transition alerts list:

- 1) In the EMS Admin Console, click **Notification**.
- 2) Click **Transition Alerts**. The **Transition Notification** page appears.
- 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 appears near the top of the page.

Task 6.36. Remove a user from the transition alerts list:

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

6.6.5. Send Custom Notifications

Administrators can use the service to send email messages to users. You can send custom notifications to both primary email addresses and/or alternate email addresses.

Task 6.37. Send a custom message:

- 1) In the EMS Admin Console, click **Notification**.
- 2) Click **Custom Notification**.
- 3) Click **Send a custom message**. The **Edit Message** page 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, 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**.

6.7. View EMS Audit Reports

The service provides an audit trail of actions taken within the system. Audit reports are accessible by administrators, super administrators, and the EMS Root Account. Help desk users and regular system users cannot access audit reports.

There are several categories of EMS audit reports available:

- **User administration reports** provide audit information on actions taken on EMS user accounts, such as password resets, permission changes, user ID conflict resolution, and exports. See ["User Administration Reports" on page 179](#).
- **Notification reports** provide audit information on changes to notification lists and users welcomed. See ["Notification Reports" on page 181](#).
- **System settings reports** provide audit information on network restriction settings and customizations to the home page and email disclaimer text. See ["System Settings Reports" on page 182](#).

In addition, other specific audit reports for EMS components are available under the following sections

- ["View Email Continuity Audit Reports" on page 229](#)
- ["View Historical Mail Audit Reports" on page 296](#)

6.7.1. User Administration Reports

User administration reports provide audit information on actions taken on EMS user accounts. These reports show changes made from the EMS Admin Console, including the following data:

Table 6-11 User Administration Reports Fields

| Column | Description | Notes |
|--------|--|---|
| Event | The action taken | <ul style="list-style-type: none"> • For example, user passwords or flags were reset using a bulk reset function. • User permissions were changed, or memberships in user sets were altered. • User ID conflicts were resolved, or accounts were added to the excluded list. |
| Actor | The EMS username of the person responsible for the event | |

Table 6-11 User Administration Reports Fields

| Column | Description | Notes |
|----------------|---|--|
| 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 | |

Task 6.38. View any of the user administration reports:

- 1) From the EMS Admin Console, click **Audit Reports**.
- 2) Under the **User Administration** section, click the name of the report you want to view. The following user administration reports are available:

Table 6-12 User Administration Reports

| Report | How to View | Provides audit information for |
|---|--|---|
| Bulk Password Updates History Report | Audit Reports > Bulk Password Updates | Bulk password resets using the User Administration > User Information function |
| Bulk Flag Resets History Report | Audit Reports > Bulk Flag Resets | Bulk user flag resets using the User Administration > User Information function |
| User Conflicts History Report | Audit Reports > User Conflicts | Resolution of user ID conflicts using the User Administration > User Conflicts function |
| Excluded Users History Report | Audit Reports > Excluded Users | Exclusion or inclusion of EMS users using the User Administration > Excluded Users function |
| User Information Exports History Report | Audit Reports > User Information Exports | Exports of user information to CSV using the User Administration > Export function |
| User Permissions History Report | Audit Reports > User Permissions | Changes to user permissions using the User Administration > [user permission] function, such as User Administration > Help Desk Users |
| User Sets History Report | Audit Reports > User Sets | Creation or deletion of user sets using the User Administration > User Sets function |

- 3) On the report search page, you can narrow the report to include only events logged for specific users by entering the user name or email address in the search field and clicking **Search**. The filtered list of events appears.

You can use % as a wildcard for any search. To search for events logged by EMS Support users, enter `eparoot` in the search box.
- 4) To export all logged events to a CSV file, click **Export**. A **File Download** dialog box appears.

NOTE All Logged Events Are Exported

When you export an audit report to CSV, all logged events are exported. The export file does not limit events based on any filter or search you may have applied to the displayed report.

- 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. You can provide a custom name for the file, but do not change the file suffix or file type.
- d. Click **Save**.

6.7.2. Notification Reports

Notification reports provide audit information on changes to notification settings and users welcomed. These reports show changes made from the EMS Admin Console, including the following data:

Table 6-13 Notification Reports Fields

| Column | Description | Notes |
|----------------|--|--|
| Event | The action taken | <ul style="list-style-type: none"> • For example, fault or transition notifications are enabled or disabled. • User welcome messages are sent. |
| Actor | The EMS username of the person responsible for the event | <ul style="list-style-type: none"> • Time is shown using <code>hh:mm:ss AM/PM</code> format, based on a 12-hour clock and your time zone. • Date is shown in <code>MM-DD-YYYY</code> format. |
| Date | The time and date the event was initiated | |
| Originating IP | The IP address of the system used for the event | |

Notification reports can only show data collected since the deployment of EMS data center version 6.6. Data from earlier EMS versions is not available.

Task 6.39. View notification reports:

- 1) From the EMS Admin Console, click **Audit Reports**.
- 2) Under the **Notification** section, click the name of the report you want to view. The following notification reports are available:

Table 6-14 Notification Reports

| Report | How to View | Provides audit information for |
|--|--|---|
| Fault and Transition Alerts History Report | <i>Audit Reports > Fault and Transition Alerts</i> | Fault or transition notifications being enabled or disabled using the <i>Notification > Fault Alerts</i> or <i>Notification > Transition Alerts</i> function |
| Users Welcomed History Report | <i>Audit Reports > Users Welcomed</i> | User welcome messages are sent using the manual <i>Notification > Welcome New Users</i> function. Note that if your organization uses automated, scheduled welcome messages using the <i>Notification > Welcome New Users > Automatically welcome new users</i> function, these automated welcome messages are not logged in this report. |

- 3) On the report search page, you can narrow the report to include only events logged for specific users by entering the user name or email address in the search field and clicking **Search**. The filtered list of events appears.

You can use % as a wildcard for any search. To search for events logged by EMS Support users, enter `eparoot` in the search box.

- 4) To export all logged events to a CSV file, click **Export**. A **File Download** dialog box appears.

NOTE All Logged Events Are Exported

When you export an audit report to CSV, all logged events are exported. The export file does not limit events based on any filter or search you may have applied to the displayed report.

- 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. You can provide a custom name for the file, but do not change the file suffix or file type.
- d. Click **Save**.

6.7.3. System Settings Reports

System settings reports provide audit information on network restriction settings and customizations to the home page and email disclaimer text. These reports show changes made from the EMS Admin Console, including the following data:

Table 6-15 System Settings Reports Fields

| Column | Description | Notes |
|----------------|--|---|
| Event | The action taken | <ul style="list-style-type: none"> For example, text appearing on the EMS home page or in the standard email disclaimer is changed. Networks are allowed to connect or are restricted from connecting to specific EMS features. |
| Actor | The EMS username of the person responsible for the event | |
| Date | The time and date the event was initiated | <ul style="list-style-type: none"> Time is shown using <code>hh:mm:ss AM/PM</code> format, based on a 12-hour clock and your time zone. Date is shown in <code>MM-DD-YYYY</code> format. |
| Originating IP | The IP address of the system used for the event | |

System settings reports can only show data collected since the deployment of EMS data center version 6.6. Data from earlier EMS versions is not available.

Task 6.40. View system settings reports:

- 1) From the EMS Admin Console, click **Audit Reports**.
- 2) Under the **System Settings** section, click the name of the report you want to view. The following system settings reports are available:

Table 6-16 System Settings Reports

| Report | How to View | Provides audit information for |
|-------------------------------------|--|---|
| Home Page History Report | Audit Reports > Home Page | Changes made to the EMS home page using the System Settings > Home Page Settings function |
| Email Disclaimer History Report | Audit Reports > Email Disclaimer | Changes made to the email disclaimer text using the System Settings > Email Disclaimer function |
| Network Restrictions History Report | Audit Reports > Network Restrictions | Networks allowed or restricted using the System Settings > Network Restrictions function |

- 3) On the report search page, you can narrow the report to include only events logged for specific users by entering the user name or email address in the search field and clicking **Search**. The filtered list of events appears.

You can use `%` as a wildcard for any search. To search for events logged by EMS Support users, enter `eparoot` in the search box.

- 4) To export all logged events to a CSV file, click **Export**. A **File Download** dialog box appears.

NOTE All Logged Events Are Exported

When you export an audit report to CSV, all logged events are exported. The export file does not limit events based on any filter or search you may have applied to the displayed report.

- 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. You can provide a custom name for the file, but do not change the file suffix or file type.
- d. Click **Save**.

6.8. Modify System Settings

NOTE System Settings Are Available to the EMS Root & SuperAdmin Accounts

The System Settings menu and its options are only available to administrators logged in using the EMS Root Account or given Super Admins privileges.

6.8.1. User Import: Change User Attributes Imported from Active Directory

Administrators using the EMS Root Account can change which data fields are synchronized from Active Directory. Certain attributes are required; these are listed in [Table 6-17](#).

Table 6-17 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 |

Table 6-17 Required Attributes

| Attribute Name | Attribute Display Value |
|----------------------------|---------------------------------|
| 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 |

Task 6.41. Change the attributes imported from Active Directory:

- 1) From the EMS Admin 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**.

6.8.2. Address List Display: Display 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 EMS 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.

Task 6.42. Change the attributes displayed in Global Address List:

- 1) From the EMS Admin 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**.

Task 6.43. Restore an attribute that has been removed:

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

6.8.3. Email Routing: Configure Mail 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 mail during an activation of Email Continuity. Before changing these settings, see the sections on mail routing: ["Mail Routing Requirements — Inbound for Email Continuity" on page 43](#) and ["Mail Routing — Outbound During Activation" on page 45](#). Note that an audit trail is provided for all changes made to mail routing, including event, actor and day/time information.

By default, EMS will resolve the email it receives using public MX records. However, if your organization would like to have EMS send the email it receives to specific destination MTAs, you can specify those MTAs within the EMS Admin Console. Additionally, if your organization uses a third-party gateway to filter your email prior to being relayed to your primary mail system, it is required that you identify specific destination MTAs within your onsite messaging solution in order to prevent mail looping.

If the destination MTA defined within the EMS Admin Console is unavailable to accept email from EMS, our systems are designed to hold and retry delivery for up to 30 days, or until the defined host resume accepting email.

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.

6.8.3.1. Routing Policies for Forwarded Mail

Task 6.44. Configure the routing path for forwarded mail:

- 1) From the EMS Admin Console, as a Super Admin user, click the **System Settings** menu item.
- 2) Click the **Email Routing** menu item.
The Email Routing Rules page appears.
- 3) The **Forwarding of Inbound Email to Your Mail System** section displays the current forwarding setting, which is either:
 - Forward email using MX records for your email domains.
 - Forward email via mail routing policies.
- 4) To change the routing, click the **Edit** under the current forwarding setting.
The **Mail Routing Policies** page appears.
- 5) The **Routing Policy** table lists all the mail routing policies currently in use.
The `Default Policy` can be edited, but not renamed. It defines routing policy for all customer domains not defined in other policies.
- 6) Click **Edit** beside the policy to change it.
Or click **Create Mail Routing Policy** to create a new policy.
This brings up the **Inbound Mail Routing Policy** page.
- 7) Enter, or edit, the **Policy Name**.
The `Default Policy` cannot be renamed.
- 8) Check the **Customer Domain(s)** for which is policy will apply.
Changing, adding or removing customer domains requires Support's assistance. Please, contact Support if the listed domains are incorrect.
If a domain is in use by another mail routing policy (**Current Policy** column), checking the **Include In This Policy** box and submitting the form will reassign the domain to this policy.

- 9) The Next Hops section of the form defines the ordered list of mail servers that messages will be routed to.

If this section is left blank, the MX Records will be used for next hops.

To enter next hop hosts, enter a fully-qualified domain name in the text-entry field and click **Add**.

The hostname appears in the **Next Hops in priority order** box above.

Repeat to add all required hostnames. Click the **Up** or **Down** buttons to specify the order of the hops.

To remove a Next Hop domain, click the domain in the list to highlight it, then click **Remove**. This change is not saved until the form is submitted.

WARNING Improper configuration can result in lost mail

Hosts configured here must *not* send mail back to Email Management Services as a fail-over. Improper configuration can result in bounced or undelivered mail. If you are unsure of which hosts to specify, please contact Support.

- 10) In the **Next Hop Transport Layer Security** box, the **Use Opportunistic TLS** option is checked by default, which means EMS delivers messages via TLS, unless the recipient is not capable of receiving messages via TLS, in which case, EMS will deliver the messages via SMTP.

Unchecking the **Use Opportunistic TLS** checkbox forces TLS to be used in all communication with hosts. If the message recipient is unable to receive email via TLS, the message may not be delivered to that recipient.

Support suggests this checkbox remain checked for most efficient communication between hosts.

- 11) To periodically test communication with next hops or MX records, check the **Enable Readiness Checks** box. See ["Next Hops Readiness Check" on page 188](#)
- 12) Click **Submit** to save the changes.

The new setting appears in the **Forwarding of Inbound Email to Your Mail System** section.

6.8.3.2. Next Hops Readiness Check

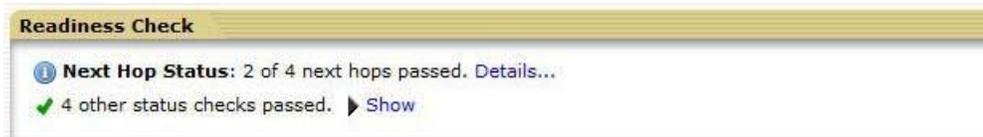
If the target specified within the EMS Next Hop Routing section (see ["Email Routing: Configure Mail Routing" on page 186](#)) is not configured to accept email from the EMS Data Center (over port 25/SMTP) it is possible that critical emails may not be delivered.

Examples of potentially affected content includes:

- Mail sent from activated users to non-activated users during Email Continuity activations
- End-user welcome messages

- Password reset email confirmations
- Readiness Check Fault Notification Alerts to your EMS administrators
- Other Data Center initiated communications

Given how critical it is that the EMS Data Center be able to successfully communicate with the destination mail systems you have specified, a Readiness Check attempts to establish connection at least once per day over port 25 to each destination mail system specified. If EMS is unable to establish a successful connection an error like the one shown below will be displayed within the **Readiness Check** section of the EMS Admin Console.



Clicking on the **Details...** link presents the Next Hop Status table, which shows the individual test results.

| Next Hop Status | | | |
|--|-----------------------|----------------------------|---------------|
| This table shows the status of next hop servers. | | | |
| Next Hop | Domain | Time | Status |
| anothercompany@company.com | anycompany@domain.com | 05:19:52 GMT on 08-29-2012 | Connected |
| www.yahoo.com | anycompany@domain.com | 05:22:32 GMT on 08-29-2012 | Not Connected |
| anothercompany@company.com | anycompany@domain.com | 05:22:32 GMT on 08-29-2012 | Connected |
| www.yahoo.com | anycompany@domain.com | 05:25:12 GMT on 08-29-2012 | Not Connected |

Refresh

If Not Connected statuses are displayed, insure that your firewall has been configured to always allow connection attempts sent over port 25 from the IP addresses specified within the *EMS Network Settings Guide* documentation. (If you require a new copy of the *EMS Network Settings Guide* documentation contact Support.)

Contact Support if further assistance is required.

6.8.3.3. Routing for Outbound Mail During an Activation

Task 6.45. Configure the path for outbound mail during an activation:

- 1) From the EMS Admin Console, as `emsroot` user or a Super Admin user, 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 record(s)** (default) or
 - **Send via specific hosts**. A dialog box appears.
- c. If you selected specific hosts, enter the host name in the text-entry 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.

6.8.3.4. Enable/Disable Store and Forward

Checking the box, **Reject mail (421) while inactive (do not store and forward)**, will disable **Store and Forward** functionality.

If checked (disabled) no email will be accepted for your organization unless you activate Email Continuity.

Checking this option causes the EMS MTAs to soft reject messages with a 421 error unless you perform a full activation.

Spammers often target the lower priority public MX records. Therefore, if the EMS MTAs are listed as a lowest priority public MX record for your organization, you may wish to check this option (disable store and forward) so that the EMS MTAs do not accept mail unless you have activated Email Continuity for your entire organization.

For customers who utilize a 3rd-party mail gateway, and/or who do not list the EMS Email Continuity MTAs in their public DNS, it is generally not recommended that this option be checked. If you have a use case where you still want to disable store and forward in this configuration, please contact Support to discuss the possible impacts of this configuration change.

Task 6.46. Disable Store and Forward

- 1) As `emsroot` user or a Super Admin user, click on **System Settings**, then **Email Routing**.
- 2) In the **Enable/Disable Store and Forward** section, check **Reject mail (421) while inactive (do not store and forward)**.
- 3) To save the updates, click **Submit** at the bottom of the page.

6.8.3.5. Enable/Disable 3rd-Party External Archive Support

NOTE This Section Does NOT Apply to Exchange Journaling For Email Archive

This section does not apply to on-premises Exchange Envelope Journaling when used in conjunction with Email Archive. See ["About Email Archive On-Premises Journaling" on page 26](#)

For EMS users who use a 3rd-party external archive support, this field provides the means of entering the target address of the external archive provider.

It is advised that you contact Support before enabling this functionality.

Task 6.47. Enable 3rd-party external archive support

- 1) As `emsroot` user or a Super Admin user, click on **System Settings**, then **Email Routing**.
- 2) In the **Enable/Disable 3rd Party External Archive Support** section, check **Enable 3rd party external archive support for active users**. This brings up a text-entry field.
- 3) Enter the target address of your external archive.
- 4) To save the updates, click **Submit** at the bottom of the page.

6.8.4. Network Restrictions

EMS allows you to enable, partially enable, or disable access to EMS functions based on a user's IP address. You can choose the following access levels:

- **No access restrictions:** With no restrictions in place, EMS users can log into EMS and access the full range of features available to your organization from any IP address. This is the default setting in place until you choose another option.
- **Full restrictions:** With full restrictions configured, users are allowed to log into EMS only from explicitly allowed IP addresses. Users attempting to log into EMS from disallowed IP addresses will be unable to log in.
- **Partial restrictions:** With partial restrictions configured, administrators can restrict access to specific features, which will be available only to users logging into EMS from approved IP addresses. Features left unrestricted can be accessed by authenticated users logging in from any IP address.

Task 6.48. Configure network restrictions:

- 1) From the EMS Admin Console, click **System Settings**, then click **Network Restrictions**. The **Network Restrictions** page appears.

NOTE Contact Support to Enable This Feature

Before you can configure network restrictions, you must contact Support to enable the feature for your organization. If you do not see the **Network Restrictions** menu item under **System Settings** in the EMS Admin Console, the feature has not been enabled. After Support enables the feature, you can configure network restrictions as described in this section. Otherwise, there are no access restrictions in place.

- 2) Choose the **Protection Status**:

- **Disabled:** If you choose **Disabled**, no network restrictions will be configured, and any existing restrictions will be removed. This option allows authenticated users to log in and access the full range of EMS features available to your organization from any IP address.

After you choose **Disabled**, click **Submit**. You do not need to continue with any other steps in this section.

- **Enabled:** If you choose **Enabled**, users will be allowed to log into EMS only from IP addresses you list in the **Allowed Networks** list that appears. Continue to [step 3](#).
- **Partially Enabled:** If you choose **Partially Enabled**, users will be allowed access to the features you choose only when they log into EMS from IP addresses you list in the **Allowed Networks** list that appears. Continue to [step 3](#).

- 3) In the **Allowed Networks** field, enter the IP addresses from which users are allowed access to EMS or its features. You can specify addresses or an IP range using CIDR notation, with the following restrictions:

- *You must include your own IP address in the **Allowed Networks** field.* Because EMS will not allow you to lock yourself out, the IP address for the computer you are using must be included among those in the **Allowed Networks** field. EMS displays your IP address so that you can include it in the list.
- *You must provide your **external** IP addresses.* Private network host ranges (such as 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16) cannot be used to implement network restrictions.

To check whether a specific host is within the range you specified, you can enter its IP address in the **Host IP Address** field and click **OK**.

NOTE Client Components Not Restricted

EMS client software components (such as SyncManager and RecoveryManager) are never restricted from connecting to the data center. You do not have to include the IP addresses for these components in the **Allowed Networks** field.

- 4) For *full restriction*, click **Submit**. You do not need to continue with the next step. For *partial restriction*, continue to the next step.
- 5) For *partial restriction* only, check the boxes in the **Protected Features** list to restrict features. Users will be allowed to access features you check only from allowed IP addresses. Any features you leave unchecked will be available to authenticated EMS users logging in from any IP address.

NOTE Protected Features Available Only For the Partially Enabled Option

The **Protected Features** list appears only after you select the **Partially Enabled** option. The Protected Features list does not appear if you select **Enabled** or **Disabled**

For example, you could check **Administrative Console** to restrict access to the EMS Admin Console to a limited set of IP addresses, but leave **Webmail** unchecked to allow users to access Webmail from any IP address.

For example, you could check **Reviewer Search** to restrict access to reviewer features to a limited set of IP addresses, but leave **User Search** unchecked to allow users to search their own archived messages from any IP address.

Click **Submit** to configure the network restrictions for the features you have selected.

6.8.5. Password Policy

Administrators can set password policy in the Admin Console. You can:

- Set Authentication Method
- Set Lock Out Policy
- Set Password Constraints

Task 6.49. Set authentication method

- 1) From the EMS Admin Console, click **System Settings**.
- 2) Click **Password Policy**. The **Password Policy** page appears.
- 3) Select **Use EMS-managed passwords for all users** to use EMS authentication, or **Use Authentication Controller** for Windows authentication.

- 4) Select how many hours to **Cache Passwords For**. This value should never be less than 1, and a value of 8–24 is more typical.

NOTE Root Access Needed To Set Authentication Method

Note that root access is required to change between Windows authentication and EMS authentication.

Task 6.50. Set password lock out policy:

- 1) From the EMS Admin Console, click **System Settings**.
- 2) Click **Password Policy**. The **Password Policy** page appears.
- 3) Set **Maximum Attempts**. This determines how many attempts a user will be allowed to attempt to log into EMS until they are locked out.
- 4) Set the minutes after which to **Reset Attempts After**. After this period of time, a user that has exceeded the maximum number will have their failed attempts purged.
- 5) Set the **Lockout Period**. This setting determines how long the system will lock a user out after they have exceeded the number of failed **Maximum Attempts**.

Task 6.51. Set password constraints:

- 1) From the EMS Admin Console, click **System Settings**.
- 2) Click **Password Policy**. The **Password Policy** page appears.
- 3) Set the **Minimum Length** for a password.
- 4) Set the number of months **and** changes for the password to remain **Unique Within**. This prevents users from reusing old passwords within the specified iterations and period of time.

6.8.6. Email Disclaimer

Only administrators logged in using the EMS Root Account can change the email disclaimer.

Task 6.52. Add disclaimer text to the end of each message sent by the service:

- 1) From the EMS Admin 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**.

6.8.7. AlertFind Mapping

Using the AlertFind mapping feature, you can:

- Choose to identify users by First name, Last name rather than the Active Directory display name, which often contains more information than the person's name, or is formatted Last name, First name. When using the voice messaging features of AlertFind, a First name, Last name designation is often preferable.
- Add more devices to AlertFind by taking advantage of those stored in Active Directory
- Select attributes to be captured from Active Directory and displayed in the AlertFind Description field, and
- Automatically create AlertFind groups using Active Directory Attributes

NOTE AlertFind Data Synchronization Schedule

Synchronization of data to AlertFind takes place once per day. Depending on your SyncManager processing schedule, you may experience a delay of 48 hours or more before new or changed Active Directory information available in Email Continuity appears in AlertFind.

NOTE Full AlertFind Integration Required

This feature is available only to customers whose Email Continuity and AlertFind products are fully integrated; 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. There must be a one-to-one correlation between users in both Email Continuity and AlertFind.

Task 6.53. Configure AlertFind mapping:

- 1) From the EMS Admin Console, click **System Settings**.
- 2) Click **AlertFind Mapping**.
- 3) In the **Display Name** section, select the identification method by clicking either:
 - **Use display name**
 - **Use first and last name**
- 4) In the Device Synchronization section, identify which data for additional devices you want to import from Active Directory to AlertFind.

- a. From the **Device Type** drop-down list, select Phone, Email, SMS, or Fax.
- b. From the **Select Attribute** drop-down list, choose the attribute to synchronize.

NOTE Use Only Appropriate Attributes for the Device Type

The interface allows you to pair any attribute with any device type. Setting inappropriate attributes (such as Display name for a phone, for example) can cause errors in the import process. Select attributes with care.

- c. Click **Add**. The Device type and attribute appear in the **Attributes mapped to devices** field.
- 5) In the **Description Mapping** section, select Active Directory attributes to be imported to the description field in AlertFind.

NOTE Data Size Limitation

Because of an AlertFind limitation, data displayed in these attributes is limited to 128 characters. Longer data strings will be truncated.

- a. In the **Select Attribute** drop-down list, select an attribute.
 - b. Click **Add**. The attribute appears in **Attributes mapped to the description field**.
- 6) Automatically create AlertFind groups using Active Directory attributes. You can also use topology attributes (such as servers, sites and stores) to identify groups. You can create as many groups as you need.
- a. From the **Select Attribute** drop-down list, select an attribute.
 - b. Click **Add**. The attribute appears in the **Attributes used to create AlertFind groups** field.
- 7) Click **Submit**.

6.8.8. User ID Resolution

This User ID Resolution menu item changes the method used for User ID restitution. See ["Resolve User ID Conflicts" on page 161](#) for the processes to resolve conflicts.

The system uses the Microsoft Exchange LegacyDN as a unique user identifier when processing mail. When moving users between Administrative Groups or Exchange Organizations the Exchange Legacy DN may change. To ensure that retained mail remains associated with a user as the LegacyDN changes, the SyncManager checks for multiple instances of the same primary email address on each directory sync. If multiple instances are found, a "User ID conflict" is identified and reported. You can configure the

system to handle these conflicts in a variety of ways. In many cases, the multiple instances of the primary address refer to the same user, and you "resolve" the conflict so that all the mail for the user is stored together in the system.

These four methods are available to configure, on a system level, how User ID conflicts should be handled:

- **Manual:** Each User ID conflict must be addressed manually by an administrator through the Admin Console. This is the default setting. See ["Resolve User ID Conflicts Manually" on page 162](#) for more information.
- **Primary Email:** All multiple instances of a primary email address are presumed to be the same end user, and all mail is associated with that user automatically without administrator intervention.
- **All Aliases:** If all aliases in the mailbox of the first instance of the primary email address are present in the second, the primary email addresses are presumed to be the same user, and the conflict is resolved automatically. The second may have additional aliases as well, but each of the primary aliases must appear. If only some or most of the primary ones are present, the action fails and an administrator must address the conflict manually in the Admin Console.
- **Active Directory Attribute:** Choose a custom or default attribute from the ones synced from Active Directory. If the attribute values match, the primary email addresses are presumed to be the same user, and the conflict is resolved automatically. Some examples might be Employee Number, User ID, phone number, or cell number.

Task 6.54. Configure the system-wide method for resolving user ID conflicts:

- 1) From the EMS Admin 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.

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

- 4) Click **Submit**.

6.8.9. 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 ["Manage EMS Fault Alerts" on page 176](#).

Task 6.55. Configure the user/mailling list deletion percentage at which a warning message is sent:

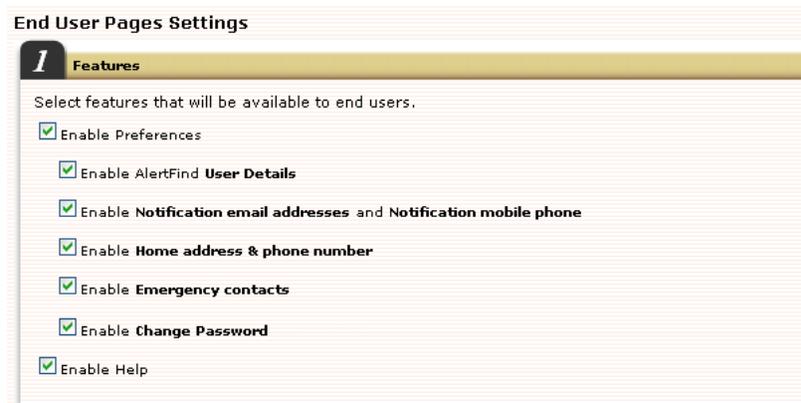
- 1) From the EMS Admin Console, click **System Settings**.
- 2) Click **Sync Notify Settings**.
- 3) In the **Sync Notification Settings** section, **Deletion Threshold** field, enter the percentage of deleted users or distribution lists above which the system should send a warning message.
- 4) Click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

6.8.10. End User Pages Settings

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

6.8.10.1. Enable/Disable End User Preferences

Select which links appear in the **Preferences** section on the Home page, or hide the Preferences section entirely.



Information about the settings is provided below.

- **Enable AlertFind **User Details****
 - *Enabled Page:* Configure Notification & Contact Settings
 - *Applicable Section Title:* User Details
 - *User Prompt Text:* Notifications are sent to you automatically when important events occur. To configure your notification settings, click the link below.
 - *User Action:* End users are prompted to provide information required by AlertFind.
- **Enable **Notification email addresses** and **Notification mobile phone****

- *Enables Page:* Configure Notification & Contact Settings
- *Applicable Section Title:* Notification email addresses
- *User Prompt Text:* Notifications are sent to you automatically when important events occur. To receive notifications via email, configure any number of email addresses below. This may include your personal email accounts. Your primary email address will always be sent notifications.
- *User Action:* Users are prompted to enter an email address.

More email addresses can be added by clicking the link again. Each address will display with a `Remove` link beside it, Users click the `Remove` link to delete the address. Primary email address cannot be deleted.
- *Applicable Section Title:* Notification mobile phone
- *User Prompt Text:* Notifications are sent to you automatically when important events occur. To receive notifications via SMS, configure your mobile phone below.
- *User Action:* Users are prompted to enter their carrier, country and mobile phone number.
- **Enable Home address & phone number**
 - *Enables Page:* Configure Notification & Contact Settings
 - *Applicable Section Title:* Home address & phone number
 - *User Prompt Text:* In case of an emergency, your organization may need to contact you at home. Configure your home address and telephone number below.
 - *User Action:* Users are prompted to enter street address, city, state/province, zip/postal code, country and home phone number.
- **Enable Emergency contacts**
 - *Enables Page:* Configure Notification & Contact Settings
 - *Applicable Section Title:* Emergency contacts
 - *User Prompt Text:* In case of an emergency, your organization may need to contact people who are close to you. Configure at least one, and up to three, emergency contacts.
 - *User Action:* Users are prompted to enter the contact's name, relationship, address, and phone number.

Up to three contacts can be entered. To remove a contact clear the information.
- **Enable Change Password**
 - *Enables Page:* Change Password
 - *User Action:* Allows end users to change their service password.

Not available for organizations using Windows Authentication.

- Enable Help
 - *Enables Page:* Help
 - *Purpose:* Displays online help for end users.

Task 6.56. Display/hide all the Preferences or Help prompts from the end-user's Home page:

- 1) In the EMS Admin Console, click **System Settings**.
- 2) Click **End User Pages Settings**.
- 3) In the **Features** section:
 - To hide the entire **Configure Notifications & Contact Settings** page, deselect the **Enable Preference** check box.
 - To hide the **Online Help** page, deselect the **Enable Help** check box.
- 4) Click the **Submit** button at the bottom of the page.

Task 6.57. Enable/disable individual links in the Preferences section of the Home page:

- 1) In the EMS Admin Console, click **System Settings**.
- 2) Click **End User Pages Settings**.
- 3) In the **Features** 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.

6.8.10.2. Add Additional Text to Home Page

Text can be added to the top of the End User Home page to give additional information to your users. In addition, if Email Continuity is enabled for your organization, you can add messages to be displayed to users during each of the Email Continuity states.

Task 6.58. Change the text displayed to end users on the Home Page:

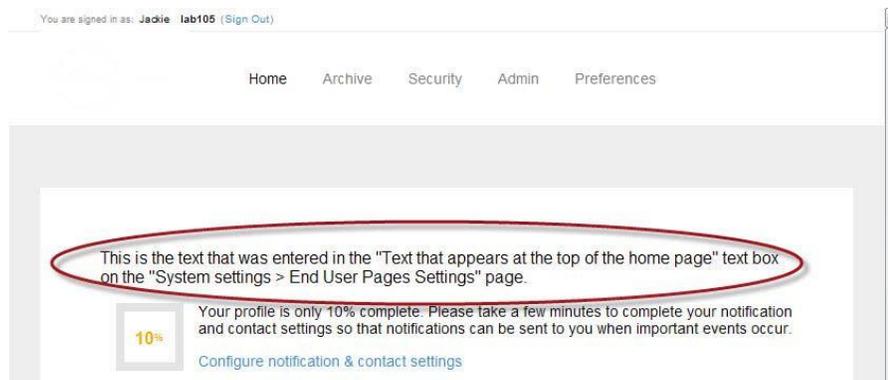
- 1) In the EMS Admin Console, click **System Settings** menu item.
- 2) Click **End Users Pages Settings** menu item.

3) In the **Home Page Textual Content** section enter text as desired.

To not display additional text in a particular context, leave the text box empty.

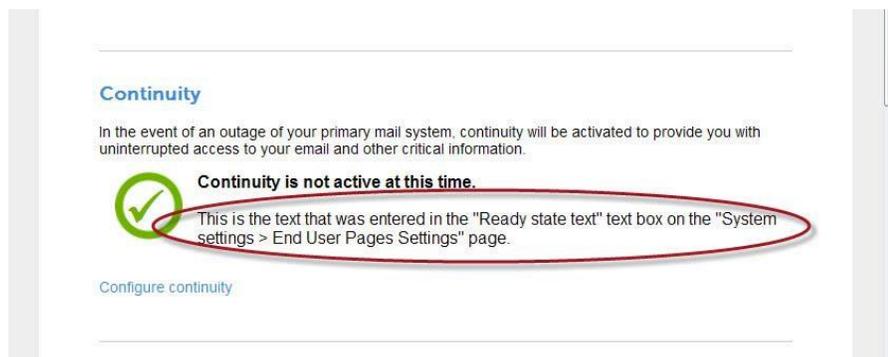
If you want to include images or links in your message, you can do so using Bulletin Board (BB) code. For example, to add an image, include a link to the image between `IMG` tags, for example `[IMG]link to image[/IMG]`. To add a link, include the link between `URL` tags, such as `[URL]link[/URL]`.

- *Top of the Home Page Text:* This text is displayed at the top of the page, under the headers and before the rest of the Home Page content. This text is displayed all the time, and is not related to Email Continuity state.



- *Active State Text:* This text displays when Email Continuity is in an **active** state.

Active, Ready, and Recovery State Text entries are displayed in the same place on the Home Page, and the text displayed varies by Email Continuity's state. To not display text for a state, leave that state's text box empty.



- *Ready State Text:* This text displays when Email Continuity is in a **ready** state.
- *Recovery State Text:* This text displays when Email Continuity is in a **recovery** state.

4) Click the **Submit** button at the bottom of the page.

6.8.11. Change Logo Image

EMS allows you to set your own organization's logo.

Task 6.59. Set your own logo:

- 1) In the EMS Admin Console, click **System Settings**.
- 2) Click **Change Logo Image**. The **Change Logo Image** page appears.
- 3) Click **Browse** to locate the .gif image you wish to upload. MessageOne requires using a logo no larger than 400 pixels wide by 55 pixels high so as to avoid having the logo overlap the display area.
- 4) Click **Submit** to upload the logo.

6.8.12. Archive Search UI

EMS allows you to re-enable the Classic Email Archive User Interface which was disabled in April 2014. This option will be available only until October 2014.

Selecting this option will display the options to access the classic interface beside the options for the new interface.

Task 6.60. Enable Classic Email Archive Interface

- 1) In the EMS Admin Console, click **System Settings**.
- 2) Click **Archive Search UI**.

The **Archive User Interface** page appears.

- 3) Check the **Enable the legacy archive user interface** box.
- 4) Click **Submit** to enable the classic Email Archive user interface.

The options to access the classic interface will appear beside the new Email Archive interface access links.

6.9. Help and Downloads

The **Help and Downloads** menu item opens a page with links to PDFs of the most current EMS documentation and ZIP files of the most current software downloads.

If you need additional tools or information, please contact Support.

6.10. Change Your EMS Password

You can change your password directly from the EMS Admin 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 the EMS Root Account, this feature changes the root-level password.

CAUTION Changing EMS Root Account Password

If you are logged in using the EMS 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 EMS Root Account password to others who must use it.

Task 6.61. Change your password:

- 1) From the EMS Admin Console, in the **Your Account** section of the left-hand menu, click **Change Password**.
The **Change Password** screen appears.
- 2) In the **New Password** field, type the new password.
- 3) In the **Confirm Password** field, retype the new password.
- 4) Click **OK**.

7. Administer Email Continuity

This chapter covers the following topics:

- ["Log Into the Email Continuity Admin Console" on page 204](#)
- ["Activate Email Continuity" on page 204](#)
- ["Recover From an Activation" on page 206](#)
- ["Configure BlackBerry Forwarding" on page 219](#)
- ["Wireless Continuity for BlackBerry Administration" on page 221](#)
- ["Outlook® Extension Administration" on page 227](#)
- ["View Email Continuity Audit Reports" on page 229](#)
- ["Access Email Continuity Mailboxes" on page 231](#)
- ["Test Email Continuity" on page 232](#)

7.1. Log Into the Email Continuity Admin Console

The administration functions described in this chapter are available to you by logging into the EMS Admin Console. See ["EMS Admin Console" on page 131](#) for additional information.

NOTE Some Described Features May Not Appear

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

7.2. Activate Email Continuity

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 your organization has deployed the Outlook® Extension, your mail 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 13](#).

Task 7.1. Activate Email Continuity:

NOTE Preparing for an Activation

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 *EMS 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 mail via the service.

- 1) Log in to the EMS Admin Console with an Administrator, Super Administrator, or EMS Root Account.
- 2) Review the **Readiness Check** section to ensure that all components are functioning correctly. All items should display a green check mark. If any components do not appear ready, contact Support.
- 3) In the **Current EMS State** section, 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. This may cause user statistics to appear out of sync in the SyncManager summary.

- 4) If your implementation includes the partial activation feature, the **Selecting the Scope of the Activation** page appears. To activate your *whole environment*, select `Activate for the Whole Email Environment`.

To activate for a *subset of users*, select `Activate EMS 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 appears empty.
 - (2) In the **Search** box, type a name or email address, (or part of the name or address, with % 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**.
- 5) Choose whether to notify users that Email Continuity is being activated. Either:
 - a. Edit the **Subject** or **Text** of the message.

If you choose to send a notification, notification messages will be sent to the contact addresses listed in the Email Continuity user profiles for the users you selected for the activation. When users receive this notification message, they can log in to the webmail interface to send and receive email. The message composition page containing the default message appears.
 - b. Select **Don't send a notification message**.
 - c. Click **Next**.

TIP Inform Users About Webmail Limitations

In your notification message, you should inform users that from 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) The **Confirmation** page appears. Review the summary of the activation steps, then click **Activate** to begin activation.

Note that the EMS Admin 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 or another EMS Administrator ends activation and begins recovery. See ["Email Continuity States" on page 18](#), and ["Recover From an Activation" on page 206](#).

7.3. Recover 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 and reintegrates messages sent or received during an activation into your primary mail system. See [Figure 2-2, "Email Continuity States" on page 19](#) for a diagram. *Recovery Archives* can contain:

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

See the following sections for procedures relevant to Recovery Archives:

- ["Create an Activation-Based Recovery Archive" on page 218](#)
- ["Start Recovery from an Activation" on page 207](#)
- ["Restore Mail to Users' Mailboxes" on page 208](#)
- ["Complete Recovery from an Activation" on page 217](#)

7.3.1. Start Recovery from an Activation

For partial activations, you can recover on a server-by-server, group-by-group, or mailbox-by-mailbox basis.

Task 7.2. Initiate recovery:

- 1) Log in to the EMS Admin Console.
- 2) In the **Current EMS State** section, 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) To recover your entire environment, select `Start Recovery for All Users`. Otherwise, select `Start recovery for some users`, leave others in the `Active` state then identify the users to recover:
 - a. Select the **User Sets**, **Mailing Lists**, **Servers**, or **Users** tab, then select an item to recover from the list displayed.
 - 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, then click **Next**.
- 4) Notify users entering the recovery process that the service is no longer active and that they can resume using the primary mail system. Remind them 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 of this in the notification message.

- 5) Click **Next**. The message composition page containing the default message appears.
- 6) Edit the **Subject** or **Text** of the message as needed, then click **Next**.
- 7) The **Confirmation** page appears. Click **Next**.
- 8) In the **Archive Name** box, type a name for the archive file (for example, `Archive_10_12_06`), then click **Next**. The RecoveryManager uses the recovery archive to deliver to end users' mailboxes the email data sent or received during the activation period. Use a name that helps you identify it.

NOTE Recovery Archives Are Purged After 30 Days

Recovery archives are available for 30 days after they are created. After that time, they are purged and are no longer available. Be sure that you complete the recovery process within 30 days of creating the recovery archive.

- 9) The EMS Admin Console displays a summary of all recovery steps to be taken. Review the recovery steps summary.
- 10) Click **Start Recovery**. The recovery process begins.

The EMS Admin 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.

7.3.2. Restore 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.

Create the recovery archive using the instructions under "[Start Recovery from an Activation](#)" on page 207 before launching the RecoveryManager.

NOTE Attachment Filenames May Be Renamed Upon Recovery

Email sent and received by Webmail and Mobile Webmail during an activation implements RFC-2231-encoded fields, the industry standard.

EMS Client software, such as Outlook Extension and Recovery Manager, rely on Microsoft Technology which does not properly decode RFC-2231-encoded fields.

Therefore, upon recovery, some attachment's filenames may be replaced with a temporary filename, such as `ATT00112.txt`. No information or attachments are lost; the attachment is only renamed.

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 an archive that was created by Email Archive, see ["Use RecoveryManager to Restore Archives" on page 280](#)

Task 7.3. Recover mail from an activation:

- 1) On the EMS server that hosts the RecoveryManager component, select **Start > Programs > MessageOne > RecoveryManager**. The RecoveryManager login page appears.
- 2) Log into the RecoveryManager using an Administrator, Super Administrator, or EMS Root Account.

Username:

Password:

Click the link below to begin the mailbox recovery process.

RecoveryManager runs under the credentials of the currently logged in user. Please make sure the account you are logged into Windows with has sufficient permissions to access the mailboxes being imported (e.g. The Service Account).

[Start Recovery](#)

3) Click **Start Recovery**.

A list of available recovery archives appears. If you see no archives available, make sure you have created a recovery archive using the EMS Admin Console before launching the RecoveryManager.

4) Select the working directory for RecoveryManager to use as a temporary data store during the import process. You can choose to:

- Use the default directory.
- Click **Browse** to select any directory with plenty of space.
- Type a directory path directly into the **Working Directory** field.

The screenshot shows a web interface for selecting a working directory. At the top, there is a text input field labeled 'Working directory:' containing the path 'C:\Recovery' and a 'Browse ...' button to its right. Below this, there are two radio buttons: 'Activation Recovery' (which is selected) and 'Active Recovery'. Underneath the radio buttons is a table with three columns: 'Name', 'Mailboxes', and 'Messages'. The table contains three rows: 'temp_archive 3' (1 mailbox, 2 messages), 'Activation - 2014-01-23' (8 mailboxes, 9 messages), and 'Open local archive ...'. At the bottom left of the interface is a 'Refresh List' link, and at the bottom right is a 'Continue' link.

| Name | Mailboxes | Messages |
|-------------------------|-----------|----------|
| temp_archive 3 | 1 | 2 |
| Activation - 2014-01-23 | 8 | 9 |
| Open local archive ... | | |

5) Choose **Activation Recovery** to recover from an activation of Email Continuity.

To recover archives generated by Email Archive, use the **Active Recovery** radio button. See ["Use RecoveryManager to Restore Archives" on page 280](#) for this procedure.

6) Click to select the appropriate archive from the list.

To refresh the list click **Refresh List**.

7) Click **Continue**.

If the directory chosen doesn't exist, a pop-up asks if you want to create it. Click **Yes** to continue.

Metadata about the archive is downloaded into the working directory you specified. Actual mail data is downloaded for each user later in the process.

- 8) The platform and settings information displayed as default in fields on the top part of this page reflects settings pulled from SyncManager and allows RecoveryManager to access the primary mail system. Typically, these settings are not changed as part of recovering archives.

Platform: Exchange 2003-2013

Directory Settings

Global Catalog Server:
sample@company.com
Advanced ...

Mailbox Access Settings
Configure

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](#)

- 9) 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.

10) Click **Continue**.

- 11) 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**.

- 12) The next RecoveryManager page controls how the archive is recovered. Status indicators are displayed in the left column of the page.

Recovery Progress

Mailboxes in Archive: 1
Recovered: 0

[User Status ...](#)
[View Recovery Log](#)

Analysis Results

Matched to a user: 1
Unmatched mailboxes: 0

[Analyze Again](#)

- **Mailboxes in Archive** — The total number of mailboxes in the archive.
- **Recovered** — The number of mailboxes for which mail has been recovered.
- **User Status** — Displays the status of each individual user, including 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.

- **Matched to a user** — Displays the number of user accounts that 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.
- Click the **Analyze Again** link to repeat the analysis done in [step 11](#) above.

13) 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, follow the directions below.

Skip this step if your organization does not use a third-party journaling product.

- 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 at the bottom of the window.

[Figure 7-1](#) 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 To: BCC: | User A Mail Recovered to User A Mailbox To: Undisclosed BCC: |
| User A Mail Recovered to Journal Mailbox for A To: BCC: | User A Mail Recovered to Journal Mailbox for A To: Undisclosed BCC: User A |
| ----- | |
| User A Mail Recovered to Alternate Mailbox X To: BCC: | User A Mail Recovered to Alternate Mailbox X To: Undisclosed BCC: |
| User A Mail Recovered to Journal for Alternate Mailbox X To: BCC: | User A Mail Recovered to Journal for Alternate Mailbox X To: Undisclosed BCC: User A, User X |
| ----- | |
| User B Mail Recovered to User B Mailbox To: BCC: | User B Mail Recovered to User B Mailbox To: Undisclosed BCC: |
| User B Mail Recovered to Journal Mailbox for B To: BCC: | User B Mail Recovered to Journal Mailbox for B To: Undisclosed BCC: User B |
| ----- | |
| User B Mail Recovered to Alternate Mailbox X To: BCC: | User B Mail Recovered to Alternate Mailbox X To: Undisclosed BCC: |
| User B Mail Recovered to Journal for Alternate Mailbox X To: BCC: | User B Mail Recovered to Journal for Alternate Mailbox X To: Undisclosed BCC: User B, User X |

Figure 7-1 BCC Journaling Results

- c. Click on the group, server, or store you want to configure to highlight it.
- d. Click **Change**.
- e. Using the radio buttons, select whether to:
 - Use the same setting as parent item.
 - Do not save a copy of recovered messages.
 - Store a copy of all recovered messages to the selected mailbox. If you choose this option, use the drop-down lists to select the server and mailbox for the recovered mail.
- f. Click **OK**.

- 14) The RecoveryManager **User Selection** page reappears. Select the set of users to recover from the right column.



- **All Users** — This 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** — This 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** — This 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** to copy them to the user list in the right-hand column.

- (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 appears 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** — This option recovers users based on 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** which will copy the group to the right-hand column. Continue to add groups until all you desire are copied to the right.

(2) Click **Continue**.

- **EMS Dropbox** — This 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.

15) Once you've completed the required information and clicked **Continue**, you are taken to the summary screen which lists the users identified for recovery.

16) Choose how to restore the mail.

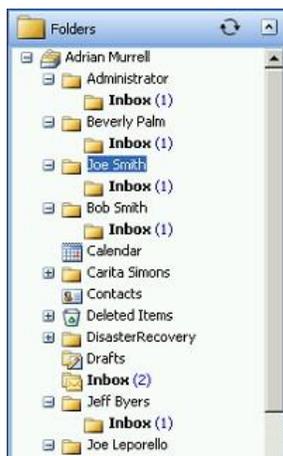
- Leave both the **Recover to alternate folder** and the **Recover all messages to single mailbox** options unchecked to import the messages into a folder labeled with the reviewer's user name with sub-folders **Inbox** and **Sent Items**.
- To recover all mail from the activation to a designated folder within users' mailboxes, click the **Recover to alternate folder** check box and type a name for the folder in the field.

After recovery is completed, messages recovered using this option will appear in users' mailboxes like this:



- c. 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 recovered using this option will appear in the mailbox you chose.



- d. 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 recovered using both options will appear in the single mailbox you designated, with the alternate folder listed, like this:



- 17) 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.
- 18) Click **Start Recovery** to begin importing data for selected users.
- 19) The RecoveryManager downloads mail data from the EMS server and imports it to the appropriate mailboxes and mailbox folders. The **Progress** page displays the number of items that successfully imported, failed to import, or were skipped. To see the recovery status for each mailbox, click **View Log**.



NOTE Cancelling Recovery

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

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

- 22) After all mail is successfully restored to users' mailboxes, return to the EMS Admin Console and finalize the recovery process. This returns mailboxes to the READY state and deletes email from the webmail interface.

See "[Recover From an Activation](#)" on page 206 instructions for completing recovery from an activation.

7.3.3. Complete Recovery from an Activation

After you have successfully restored messages to users' mailboxes using the RecoveryManager, return to the EMS Admin Console and finalize the recovery process. This returns mailboxes to the READY state and 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 ending recovery. You can download recovery archives for up to 30 days after they are created or until you end recovery. After you end recovery in the EMS Admin Console, the recovery archive no longer exists and you can no longer access it.

Task 7.4. Complete recovery from an activation:

- 1) In the EMS Admin Console **Current EMS State** section, click **End Recovery**. The Recovery Wizard launches.

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

- 2) Using the radio buttons, select the scope of the recovery. Choose *End recovery for all users in the Recovery state* or *End recovery for some users, leave others in the Recovery state*. Click **Next**.
- 3) On the **Confirmation** page, click **End Recovery**. This purges the recovery archive from the data center and returns all activated mailboxes to the READY state.

7.3.4. Create an Activation-Based Recovery Archive

An **activation-based recovery archive** allows 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.

Task 7.5. 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, type an email address or name in the **Search** box and search for the results. Then click the listed mailing list or user to select it.
 - b. If you select the **Server** tab, click a server to select it.
- 8) Click **Add**. Repeat until all are listed in the correct section.
- 9) Click **Next**. A summary screen describing the Email Recovery Archive you've defined appears.
- 10) Click **OK**. The activation-based recovery archive is created. Follow the instructions under "[Restore Mail to Users' Mailboxes](#)" on page 208 to recover the messages.

7.4. Configure 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. The full Wireless Continuity for BlackBerry subcomponent is a separate optional product. To prevent receiving duplicate messages on the device during activation, your organization should use only one of these services. For information, contact Support.

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 Email Continuity is ACTIVE 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 Email Continuity is ACTIVE 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.

Task 7.6. Configure a BlackBerry device for BlackBerry forwarding:

Before your users can enable forwarding for their BlackBerry devices, they need three pieces of information.

- The name of their 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.

Have your BlackBerry users follow the instructions below to configure their devices for BlackBerry forwarding:

- 1) Follow the account setup process for your carrier.
 - a. Log in to <http://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.
 - d. 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. 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, then BlackBerry forwarding is not enabled for your organization.

- 4) During an activation, you must change Message Services to be able to send email from your BlackBerry. To change message services during an activation:
 - 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 activation is ended and your 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.

7.5. 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 EMS Admin Console to manage the Wireless Continuity for BlackBerry feature.

7.5.1. Configuration Parameters

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.

7.5.2. Manage Users and Devices

The EMS Admin Console provides you with information on BlackBerry users and their devices. You can view overview or detailed information about each device.

A data logging interface is installed on each device as part of the client agent version 6.2 and higher. This agent interface allows you to send diagnostic information to Support.

Task 7.7. View BlackBerry user and device information:

- 1) From the EMS Admin 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 7-1](#).

Table 7-1 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. |

Table 7-1 Mailbox Information Page

| Field | Description |
|--------------------------------------|--|
| BlackBerry PIN | The device PIN. |
| BlackBerry Enterprise Server | The BES to which the device is attached. |
| EMS 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. |

Task 7.8. Export BlackBerry device details:

- 1) From the EMS Admin 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 7-1](#).
- 3) To export device information for all BlackBerry users synced with your Email Continuity environment to a comma-separated values (CSV) file, click **Export**. The CSV file includes all information shown on the **Mailbox Information** page, except for login history data. These fields are described in [Table 7-1](#).

Task 7.9. Reset a BlackBerry device:

- 1) From the EMS Admin 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 7-1](#).
- 3) To reset a device, click **Reset**. The reset process pushes all contact information out to the device. This is useful when a device misses a device check-in interval or experiences other issues.

Task 7.10. Send BlackBerry device logs/diagnostics to Support:

- 1) From the EMS Admin 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 7-1](#).
- 3) 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 appear for version 6.1 and older agents.

7.5.3. View Information on the BlackBerry Device

Your BlackBerry users can access information about their devices and client agents using the instructions in this section.

Task 7.11. View information about a device using the interface installed with the device agent:

- 1) The BlackBerry must be on and the Wireless Continuity for BlackBerry client agent must be installed. Contact your Email Continuity administrator if you need the client agent.
- 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.

7.5.3.1. Device Menu Options: Standard Display Mode

Your BlackBerry users can access menu options by clicking the scroll button. Menu options that appear on the Standard Display are:

Table 7-2 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 | Closes the agent interface and returns you to the BlackBerry main menu. (Applies only to agents version 6.1 and earlier.) |

7.5.3.2. Device Menu Options: Advanced Display Mode

Your BlackBerry users can access menu options by clicking the scroll button. Menu options that appear on the Advanced Display are:

Table 7-3 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. |
| Close | Closes the agent interface and returns you to the BlackBerry main menu. |

7.5.3.3. Advanced Display Information

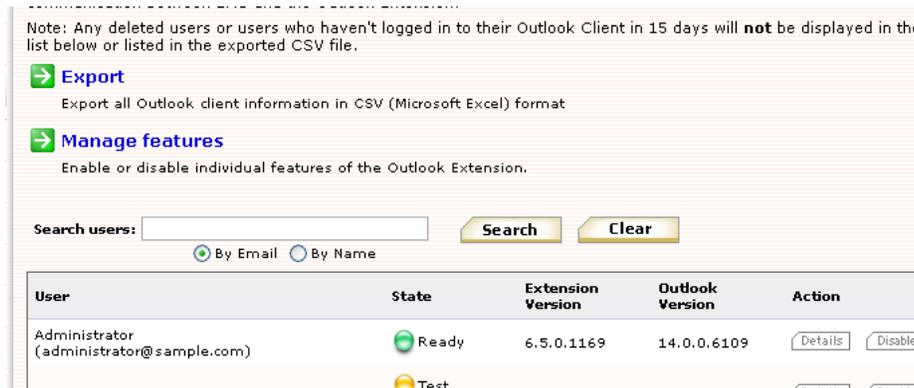
Your BlackBerry users can use the Advanced Display to view read-only information about the agent and the BlackBerry device on which it is running. When users are viewing the Advanced Display, the pop-up menu displays an option to return to the Standard Display.

Table 7-4 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 EMS 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. |

7.6. 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 EMS Admin Console and click the **Outlook Extension** menu button. The **Outlook Client Information** screen appears.

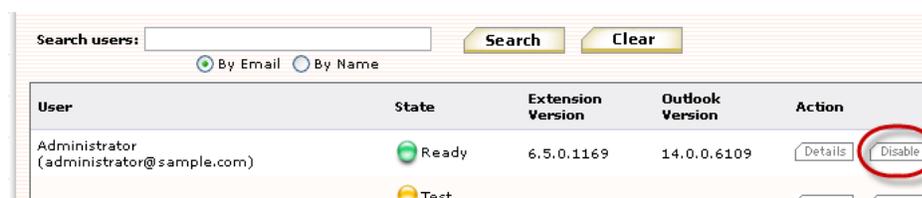


The Outlook Client Information screen provides a list of users, and indicates whether they have installed the extension and polled the data center. You can search for a specific user, then click the **Details** button to display:

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

Task 7.12. Enable or disable the Extension:

- 1) Click the **Outlook Extension** menu button.
- 2) To disable an individual user so that the Extension cannot be used, click the **Disable** button adjacent to the user's name.



A confirmation box appears. Click **OK**.

- 3) To enable or disable Outlook Extension features for all users:

- a. On the **Outlook Client Information** screen, click **Manage Features**.

Note: Any deleted users or users who haven't logged in to their Outlook Client in 15 days will **not** be displayed in the list below or listed in the exported CSV file.

→ **Export**
Export all Outlook client information in CSV (Microsoft Excel) format

→ **Manage features**
Enable or disable individual features of the Outlook Extension.

Search users:

By Email By Name

| User | State | Extension Version | Outlook Version | Action |
|---------------|-------|-------------------|-----------------|--------|
| Administrator | ... | ... | ... | ... |

- 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.

Outlook Extension Features

1 Extension Features

Choose which features should be available to users of the Outlook Extension. Any changes will take effect the next time the Outlook client is started.

Email Continuity

Email Archive

Storage Management (always enabled)

- c. Click **Submit**.

Task 7.13. Export the list of users:

- 1) Click **Export**.

Note: Any deleted users or users who haven't logged in to their Outlook Client in 15 days will **not** be displayed in the list below or listed in the exported CSV file.

→ **Export**
Export all Outlook client information in CSV (Microsoft Excel) format

→ **Manage features**
Enable or disable individual features of the Outlook Extension.

Search users:

By Email By Name

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

7.7. View Email Continuity Audit Reports

The service provides an audit trail of actions taken within the system. Audit reports are accessible by administrators, super administrators, and the EMS Root Account. Help desk users and regular system users cannot access audit reports.

Email Continuity audit reports provide the history of activations and tests and can be exported to CSV files. The reports provide the name of the user who initiated each state transition along with the time and date of the transition, the logon status of users during an activation, and, if a recovery archive has been generated for the activation, the name and size of the archive.

Email Continuity audit reports show all available historical data collected for your organization.

See the following sections for more information:

- ["Activation History Reports" on page 229](#)
- ["Test History Reports" on page 230](#)

7.7.1. Activation History Reports

Activation History Reports provide a report on state transitions (such as ACTIVE, RECOVERY, or READY), and a list of user logins during an activation.

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.

Task 7.14. View an Activation History Report:

- 1) From the EMS Admin Console navigation menu, click **Audit Reports**.
- 2) Under the **Email Continuity** section, **Activation History Report**. The **Activation History Report** page appears, showing all events logged.
- 3) Click the **State Transitions** arrow for an activation to display the date, time, and responsible party.

- 4) Click **View logon records during this activation** to see active users or identify who logged in to the service during an activation. (See also "[Review Login Status on page 157.](#)")

You can narrow the records displayed to include only specific users by entering the user name or email address in the search field and clicking **Search**. The filtered list of users appears.

You can use % as a wildcard for any search. You can exclude users from this report by clicking **Exclude** in the **Action** column for a user.

- 5) Click **Export** to export all logged events to a CSV file. A **File Download** dialog box appears.

NOTE All Logged Events Are Exported

When you export an audit report to CSV, all logged events are exported. The export file does not limit events based on any filter or search you may have applied to the displayed report.

-
- 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. You can provide a custom name for the file, but do not change the file suffix or file type.
 - d. Click **Save**.

7.7.2. Test History Reports

The Test History Report gives you an easy way to provide disaster recovery or business continuity auditors with data proving that your organization conducts regular tests.

Task 7.15. View a Test History Report:

- 1) From the EMS Admin Console navigation menu, click **Audit Reports**.
- 2) Under the **Email Continuity** section, **Test History Report**. The **Test History Report** page appears, showing all events logged.
- 3) Click the **State Transitions** arrow for an activation to display the date, time, and responsible party.

- 4) Click **View logon records during this activation** to see active users or identify who logged in to the service during a test. (See also ["Review Login Status" on page 157.](#))

You can narrow the records displayed to include only specific users by entering the user name or email address in the search field and clicking **Search**. The filtered list of users appears.

You can use % as a wildcard for any search. You can exclude users from this report by clicking **Exclude** in the **Action** column for a user.

- 5) Click **Export** to export all logged events to a CSV file. A **File Download** dialog box appears.

NOTE All Logged Events Are Exported

When you export an audit report to CSV, all logged events are exported. The export file does not limit events based on any filter or search you may have applied to the displayed report.

- 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. You can provide a custom name for the file, but do not change the file suffix or file type.
- d. Click **Save**.

7.8. Access Email Continuity Mailboxes

This section explains how to access various Email Continuity mailboxes, including:

- ["Access Your Mailbox" on page 231](#)
- ["View Undeliverable Mail in the Dropbox" on page 232](#)

7.8.1. Access Your Mailbox

When Email Continuity is active, you can access your webmail account directly from the EMS Admin 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. Users without access to the EMS Admin Console can access their mailboxes using the web address provided to your organization by Support.

Task 7.16. Access your webmail account during an activation:

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

NOTE Legacy Active Mail Older than 1970 Not Available in Webmail

If your organization has imported legacy active mail dated prior to 1970, these messages are not available through the Webmail interface.

7.8.2. View 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 EMS Admin Console.

Task 7.17. View undeliverable mail during an activation:

- 1) From the EMS Admin Console, click **Your Account**.
- 2) Click **Access EMS Dropbox**. The webmail inbox for the Dropbox appears.

7.9. Test Email Continuity

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

Task 7.18. Start a test of Email Continuity:

- 1) In the EMS Admin 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 appears. 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 "[Manage Email Continuity Transition Alerts](#)" on page 177.) 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 appears in the EMS Admin 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.

Task 7.19. Start recovery from a test:

- 1) In the **Current Tests** section of the EMS Admin Console, click **Start Recovery**.
- 2) Select the recovery type and click **Next**. A notification message composition page appears. 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 appears when you use the RecoveryManager to restore messages to the primary mail system.
- 4) Click **Next**.
- 5) Click **Start Recovery**.

8. Administer Historical Mail/Email Archive

Depending on the level of service purchased by your organization, EMS can provide users access to historical mail 24/7/365.

This chapter covers the following topics:

- ["Historical Mail/Email Archive Admin Console" on page 235](#)
- ["Replication Zones" on page 236](#)
- ["Manage Retention Policies" on page 237](#)
- ["Reviewer Groups" on page 247](#)
- ["Storage Management" on page 261](#)
- ["Storage Reports" on page 270](#)
- ["Create and Recover Archives" on page 275](#)
- ["On-Premises Journaling Administration" on page 287](#)
- ["Folder Sync Administration" on page 289](#)
- ["View Historical Mail Audit Reports" on page 296](#)

8.1. Historical Mail/Email Archive Admin Console

The administration functions described in this chapter are available by logging into the EMS Admin Console and clicking **Historical Mail**. See ["EMS Admin Console" on page 131](#) for additional information.

NOTE **Some Described Features May Not Appear**

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

TIP Support for International Date Formats

The default date format for Historical Mail/Email Archive is MM/DD/YYYY.

If your organization prefers a different date format contact Support and to have the organization's Historical Mail/Email Archive date format changed.

Currently supported date formats are:

- MM/DD/YYYY
 - MM-DD-YYYY
 - DD/MM/YYYY
 - DD-MM-YYYY
 - YYYY/MM/DD
 - YYYY-MM-DD
-

8.2. Replication Zones

Before you can start using Historical Mail/Email Archive, you must set up Replication Zones. Replication Zones allow you to associate specific mail servers with a preferred series of VaultBoxes within your environment. For smaller environments, there may only be a single Replication Zone and all mail 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 EMS. 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

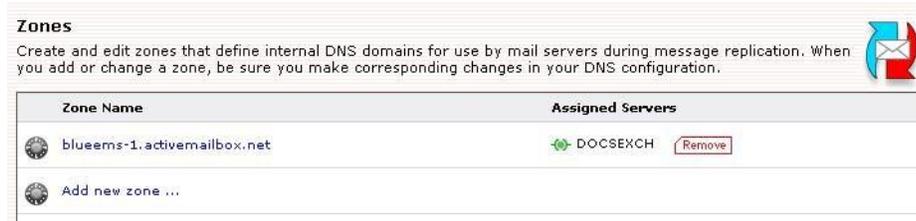
Replication Zone routing corresponds to the server that bifurcates the message (typically the first mail server to touch a message), not the server on which a particular user resides.

Task 8.1. Assign servers to replication zones:

- 1) From the EMS Admin Console, select ***Historical Mail***.

2) Click **Replication Zones**.

The **Zones** page appears, containing a list of mail servers.



3) Click **Add new zone...**

4) In the text box that appears:

- a. Enter the name of the zone you want to add.

Zones define internal DNS domains for use by mail servers during message replication. When you add or change a zone, be sure you make corresponding changes in your DNS configuration.

- b. Click **Submit**.

The newly added zone appears above the **Add new zone...** button.

5) In the **Unassigned Server Name** section of the **Zones** page, add servers to the new zone by clicking the appropriate **Add to zone (zone name)** link.

8.3. Manage Retention Policies

For information about the types of retention policies you can configure and best practices for all policies, see ["About Retention Policies" on page 30](#).

When EMS Lync Archiving is activated by Support, a Retention Policy of type `Instant Message`, with a policy name of `Global IM Capture Policy` and a default duration of 10 years is created. See ["EMS Lync Archiving Retention Policy" on page 331](#) for more information.

8.3.1. Create Retention Policies

Retention policies allow you to store email and instant messages for configurable lengths of time. To use Email Archive, at least one retention policy must be created and have users assigned to it.

To use a retention policy, you must:

- 1) **Create a retention policy**. This includes giving it a name and specifying the number of days mail retained under this policy should be kept.

2) Decide the type of retention policy:

- Membership-based
- Capture-based
- User classification

3) Decide its scope. The scope of the policy determines to which users the policy applies. The scope can be assigned based on mailing lists, servers, individual users, and user sets.

Membership within mailing lists, servers, or user sets is updated automatically when SyncManager is run, therefore the scope of the policy can be dynamic after the policy is created.

4) Decide what should happen when users are deleted from the system. With a Membership-based policy, you must decide to either keep the mail of the deleted users 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 message?

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 the message stored under a Retention Hold?

A retention hold *always takes highest priority*, preventing messages covered by a hold from being deleted, regardless of other criteria.

3) Is the message stored under a storage management policy?

See ["Storage Management" on page 261](#) for more details.

4) Of the retention policies that apply to this email, which one is highest in the priority list?**5) Based on the highest priority policy, should this message be kept or marked eligible for purging?****6) 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 the Ready state, retention policies will be applied.

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. To avoid unintentional purging of messages intended to be retained for a longer period, ensure that policies with longer durations are prioritized higher than those with shorter durations.

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.

Task 8.2. Create a retention policy

- 1) From the EMS Admin Console, click **Historical Mail**.
- 2) Click **Retention Policies**.
The **Retention Policies** page appears.
- 3) Click **Create a new retention policy**.



The **Retention Policies Details** page appears.

- 4) In the **Name** box, type a unique name for the new policy.

The screenshot shows the "Retention Policy Details" form. It includes the following fields and text:

- Retention Policy** (Section Header)
- Text: "A retention policy determines how long it keeps historical mail. The service will purge mail that has been in the system longer than the specified retention period."
 - Text: "You can assign users to this retention policy using the 'Select Users' button on the *Retention Policies* page."
- Name:**
- Retain mail for:** days

- 5) In the **Retain Mail for** box, type the number of days for the retention period.

The screenshot shows the "Retention Policy Details" form with the following elements:

- Note:** This policy does not apply to cloud users.
- Retention Type:** (dropdown menu)

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

Depending on your system's configuration, this prompt may not appear. If this is the case, a Membership-based policy is created.

Depending on your system's configuration, not all of these options may appear.

- 7) If you selected `Capture Based`, no further options are required.
- 8) If you selected `User Classification`, 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. Next, select a VaultBox for connection to the server.

The screenshot shows a configuration form for a 'User Classification' retention policy. At the top, 'Retention Type' is set to 'User Classification'. Below this, there is a section for 'Classification Folder Name' with a 'Mail Folder' text input field. A note states: 'Users will drag mail into this folder in order to classify mail under this policy.' Below the note is a checkbox labeled 'Automatically create this folder in user mailboxes.' At the bottom, there is a question: 'Which VaultBox should connect to the mail server for this policy's users to classify and archive messages?' with a dropdown menu showing 'lab105vb'.

For User Classification policy, you must also complete the steps to configure user classification retention scheduling, "[Configure Manual Retention \(User Classification\) Task schedule settings:](#)" on page 128.

- 9) If you selected Membership Based Policy, if you want to retain mail for users who have been deleted from the system, click the **Retain Deleted Users** check box.

The screenshot shows a configuration form for a 'Membership Based' retention policy. At the top, 'Retention Type' is set to 'Membership Based'. Below this, there is a section for 'Retain deleted users' with a checked checkbox labeled 'When users are deleted, keep them in the policy.' Below the checkbox is a note: 'Retaining deleted users will retain mail for the normal length of the policy, even after users are deleted.'

This option is relevant for users added to the retention policy as part of a distribution list, mail server, or user set.

Depending on your system's configuration, this prompt may not appear. If this is the case, mail is *not* retained for deleted users.

The **Retain Deleted Users** option does not apply to mail for users who are added individually to the retention policy. Mail for these *explicitly added users* is retained under the retention policy even after the users are removed from the mail system.

- With the **Retain Deleted Users** option selected, messages for users added to the retention policy as part of a distribution list, mail server, or mail store will be retained even after the users have been deleted from the mail system.

- If the **Retain Deleted Users** option is *not* selected for a membership-based retention policy, messages for users added to the policy through a distribution list, mail server, or mail store **will be purged** after those users are deleted from the mail system.

10) Click **Submit**.

11) This returns you to the retention policy page, where you must click **Select Users** to complete the creation of the Retention Policy. See [Task 8.3. "Add users to a retention policy"](#)

Task 8.3. Add users to a retention policy

1) Select a retention policy and click **Select Users**.

The **Select Users** page appears.

2) Identify the scope of the policy, which are the users to be included in 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 and System-created User Sets are Dynamically Updated

Administrators do not have to manually add or delete users to the retention policy when a list or system-created user set changes. The lists and system-created user sets are updated when SyncManager runs and the retention policy's scope is dynamically updated.

User-created user sets are NOT dynamically updated.

NOTE Deletion of Distribution Lists Used in Retention Policies

If a distribution list used by a retention policy is deleted on Exchange, the distribution list is placed on a purge list, and a fault alert notice is sent to each member of the fault alerts notifications list.

This allows a 30-day window for Administrators to recover from accidental deletion of lists, before retained data is lost.

NOTE Ensure Envelope Journaling Users Are In A Retention Policy

Envelope Journaling requires all enabled users be in a Retention Policy. However, Email Archive Retention Policy membership and Exchange Journaling membership are managed separately.

It is recommended that the same criteria (such as a distribution list) be used to identify users for a retention policy and to enable users for journaling in Exchange.

Mismatches between retention and journaling policies may result in data loss.

- c. To add all users with mailboxes on designated 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**. Deleted users display a **X** next to their names, and may be added to the policy like any other user. While no new mail will be captured for deleted users, existing retained mail for these users will be added to the retention policy.
- 3) Repeat adding users from any or all of the above categories, clicking **Add** to copy the selected users to the **Current selection** pane on the right, until the full scope of the Retention Policy is defined.

If an item listed in the right-hand pane is incorrect, check the box beside the item and click **Remove**, to remove the entry from the **Current selection** list.

- 4) When all appropriate users have been added to the retention policy, click **Next**.
The **Confirm new policy scope** page appears.
- 5) Examine the contents of the **Confirm** page, which lists all changes made to the retention policy.

To see a list of all users affected by the policy click the **Click here** link, which pops up a new window containing a user list. To export this list to a CSV file, click the **Export to file** link at the top-right of the pop-up window.

- 6) If the data is correct, click **Submit**.

Task 8.4. Prioritize retention policies

- 1) From the EMS Admin Console, click **Historical Mail**.

WARNING Retention Policy Changes Go Into Effect Immediately Upon Saving

Reprioritize policies with care. See "[Retention Policy Best Practices](#)" on [page 31](#).

- 2) Click **Retention Policies**.

- 3) Click **Reorder/Reprioritize Retention Policies** at the bottom of the page.



The user interface changes so that **DRAG** appears next to each retention policy.

| | | | | | |
|------|----------------|-----------------------|----------------------|------------|----------|
| DRAG | Retention Hold | Test Retention Hold 4 | Until hold is lifted | 01/15/2014 | Users: 0 |
| DRAG | Retention Hold | admin hold | Until hold is lifted | 01/15/2014 | Users: 0 |
| DRAG | Membership | test policy | 100days | | Users: 0 |
| DRAG | Membership | test policy2 | 30days | | Users: 0 |
| DRAG | Membership | name | 60days | | Users: 7 |
| DRAG | Capture | temp capture | 100days | | Users: 7 |

See the [Storage Report](#) section for a complete list of storage across the different policies

- 4) Click anywhere in a policy's row, and drag the policy to a new location in the list. The higher up in the list a Retention policy resides, the greater its priority.

Remember that each email's purge date is specified by the highest priority policy that includes that message. So if you move a 10-day policy above a 100-day policy, once the change is saved, all emails covered by both policies will be evaluated by the purge process and any email that is older than 10 days will be scheduled for purge.

- 5) When you're satisfied with the list, click **Save New Ordering**. Or click **Revert** to return to the previous ordering.

The screenshot shows two buttons: 'Save new ordering' and 'Revert'. Below them is a table with two rows of retention policies.

| Type | Policy Name | Retention | Last Updated | Statistics |
|------|----------------|----------------------------|----------------------|---------------------|
| DRAG | Retention Hold | Third Group Retention Hold | Until hold is lifted | 01/15/2014 Users: 0 |
| DRAG | Retention Hold | Test Retention Hold 3 | Until hold is lifted | 01/15/2014 Users: 0 |

The normal interface returns and all policies are listed in the new order, with the exception that Retention Holds always have higher priority than any other kind of retention policy, so all policies will be listed in priority order following the last of the Retention Holds.

8.3.2. Reconciling User ID Conflicts For Retention Policy Users

If a Retention Policy user's system ID (Legacy Exchange DN) changes, EMS detects a user ID conflict because more than one instance of an email address was captured in a synchronization. The conflict is reported with a fault alert notice sent to each member of the fault alerts notifications list and can be resolved by administrative action (see ["Resolve User ID Conflicts Manually" on page 162](#)). After the conflict is resolved (that is, the multiple instances of the email address are determined to be the same user), mail stored before the change becomes reassociated with the user and is correctly tagged for applicable retention policies.

8.3.3. Query-Based Retention Holds

Email Archive Reviewers, and administrators with Reviewer privileges, can create Retention Holds on collections of mail resulting from Archive Searches. These Retention Holds work similarly to retention policies, except:

- Query-Based Retention Holds are created on the **Review Company Email Archives** screen rather than the EMS Admin Console.
 - This screen can be accessed from the Admin Console using the **Historical Mail > Email Recovery > Create Search Based Recovery Archive** link.
- The Reviewer identifies and selects the messages to be archived under a Retention Hold policy.
- The messages are saved until the Retention Hold is deleted by an Administrator.
- If the Reviewer has checked the **Automatically retain new messages** checkbox when creating the Retention Hold, all new incoming messages that match the criteria for the Retention Hold will be added to the Retention Hold.

Retention holds always have the highest priority in the Retention policy list, because the messages in it are retained until an Administrator removes the hold.

NOTE Maximum Message Limits in Query-Based Retention Holds

Email Archive limits the maximum number of messages in Retention Holds to prevent improperly configured queries from monopolizing system resources. Requests to produce an over-sized query will fail, and the reason for the failure will appear in the audit log.

To create extremely large holds, create multiple holds.

NOTE Purge Delay for Query-Based Retention Holds

There is a window of time between EMS identifying a message eligible for purging and when all records of that message are actually deleted. If a Retention 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 retention hold, but will be deleted when the next purge is performed.

Task 8.5. Delete a Retention Hold

- 1) From the EMS Admin Console, click **Historical Mail**.

2) Click **Retention Policies**.

The **Retention Policies** page appears.

| Type | Policy Name | Retention | Last Updated | Statistics | Actions | |
|------|----------------|----------------|----------------------|------------|----------|---|
| 1 | Retention Hold | TestHold | Until hold is lifted | 01/15/2014 | Users: 0 | Edit Delete |
| 2 | Retention Hold | non-admin hold | Until hold is lifted | 07/12/2013 | Users: 0 | Edit Delete |

3) Identify the Retention Hold policy to be deleted, and click **Delete**. A confirmation box appears and reminds you that this action cannot be undone.

Remember that any message in this hold that is not covered by another retention policy will be purged based on the default purge criteria.

4) Click **Delete** to confirm the deletion.

Task 8.6. Edit a Retention Hold and view a hold's change history

1) From the EMS Admin Console, click **Historical Mail**.

2) Click **Retention Policies**.

The **Retention Policies** page appears.

| Type | Policy Name | Retention | Last Updated | Statistics | Actions | |
|------|----------------|----------------|----------------------|------------|----------|---|
| 1 | Retention Hold | TestHold | Until hold is lifted | 01/15/2014 | Users: 0 | Edit Delete |
| 2 | Retention Hold | non-admin hold | Until hold is lifted | 07/12/2013 | Users: 0 | Edit Delete |

3) Identify the Retention Hold policy, and click **Edit**.

Only the hold's name can be changed, along with whether or not new messages matching the query are automatically retained. The scope of the hold cannot be changed.

1 **Retention Policy**

A retention hold will retain mail until the hold is removed manually. No mail will be purged from the system until the hold has been lifted.

You may not change the scope of a retention hold. To change what is held, make a new retention hold and then remove this one.

Name:

Retain mail for: Until hold is lifted

Last Updated: 01/15/2014

Automatically retain new messages that match retention hold query

4) Edit these fields as desired.

- 5) The Change History for this hold is displayed in the third section of this page.



| Event | Actor | Date |
|---|--|--------------------------|
| TestHold's name: Changed auto update from true to false | Administrator (administrator@sample.com) | 10:39:37 AM on 1-17-2014 |
| Changed name from TestHold to TestHold's name | Administrator (administrator@sample.com) | 10:39:37 AM on 1-17-2014 |
| TestHold: held 100 messages. | Administrator (administrator@sample.com) | 4:16:38 AM on 1-15-2014 |

- 6) Click **Submit** to save the change. Or click **Cancel** to return to the **Retention Policies** page.

8.3.4. Use Retention Policies to Simulate Retention Holds

Administrators can use the Membership-based policies to simulate Retention Holds on mail for designated individuals.

For example, if your organization needs to indefinitely retain all email sent or received by two individuals in the organization, you would:

- 1) Create a Membership-based 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 Deleting Users Can Purge Mail Despite Simulated Retention Holds

If you use a Membership-based Policy to simulate a Retention Hold, care must be taken never to remove users from EMS who are covered by the policy, or their mail may be purged.

Normally, under a Membership-based Policy, mail is only retained for users included in EMS. When users are deleted from EMS, their emails are purged.

To stop this from happening, select the **When users are deleted, keep them in the policy** option when creating the Retention Policy.

8.4. Reviewer Groups

Archive users who are a member of a Reviewer Group have the ability to search and read emails or instant messages that are within the scope of that Reviewer Group, and to create Discovery or Recovery archives (see ["Search-Based Recovery Archives" on page 38](#) and ["Discovery Archives" on page 38](#)) and Retention Holds (see ["Query-Based Retention Holds" on page 37](#)).

Any EMS user can be designated as an Archive Reviewer. The individual does not have to have a personal email archive; that is, their personal user account does not need to be part of a retention policy.

Only Super Admins or root account users can create, edit or delete Reviewer Groups. Administrators can view the Reviewer Group's Mailbox Scope and list of Reviewers.

When creating Reviewer Groups, the Group's Mailbox Scope is a feature that restricts the emails each Reviewer Group is able to access. The Mailbox Scope can be defined in terms of Users, User Sets, Mailing Lists and Servers, and any combination thereof.

For example, you could specify that reviewers John Doe and Jill Smith can view all email sent and received by the Sales User Set and three additional users who used to belong to the Sales department.

Email message Reviewer Groups also have the Advanced Options feature, which allows the scope to be further narrowed by an Archive query, such as a date range. To do this, you must use the same query language that is used to perform advanced searches in the archive. For more information, see ["Reviewer Group Email Scope Advanced Options" on page 251](#).

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 access the audit report, go to **Audit Reports > Reviewer Groups**

Task 8.7. Create a Reviewer Group:

- 1) From the EMS Admin Console, using a super-admin or root account, click **Historical Mail > Reviewer Groups**.
The **Reviewer Groups** screen appears.
- 2) Click the **Create Reviewer Group** link that appears under the list of Reviewer Groups.
The **Reviewer Group Name** screen appears.
- 3) In the **Type** drop-down, select whether this Reviewer Group will have access to the **Email** archive or the **IM** (Instant Message) archive.
- 4) In the **Name** field, enter a descriptive name for the group. The name entered must be different from the names of other reviewer groups.

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.

- 5) Click the **Next** button and the **Reviewer Scope** screen appears.
- 6) The scope of the Reviewer Group identifies the sub-set of emails or instant messages the reviewer can access for their search. The scope can be defined by User Sets, Mailing Lists, Servers and individual Users, and any combination thereof.

Click the appropriate tab to include messages by **User Sets**, **Mailing Lists**, **Servers**, or individually by **Users**.

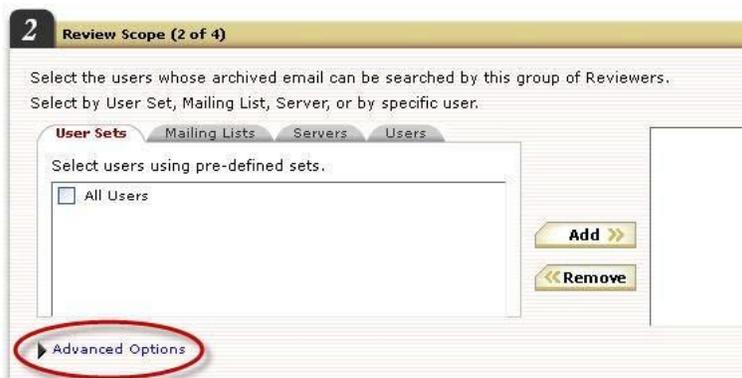
- a. If you select the **User Sets** tab, check user set(s) to select.
- b. If you select the **Mailing Lists** or **Users** tab, in the **Search** box type an email address or name and search for the results. A percent sign (%) will show all users or lists. Then check the listed mailing list(s) or user(s) to select.
- c. If you select the **Servers** tab, check server(s) to select.

Click **Add** button to copy the selected item(s) to the selection pane.

Repeat selecting tabs and items, clicking **Add** after each, until all selections are listed in the right-hand pane.

To remove items from the selection pane, check the box beside the item and click **Remove**.

- 7) If an **Email** type was selected, to further limit the messages available to the Archive Reviewer, such as email messages within a date range, or on a specific topic, click the **Advanced options** link.



In the **Query Text** box, enter a query. This query is AND'd with the results of the above User selection.

Either paste the desired query string from Email Archive's **Search Company Archives > Advanced Query Language** text field, or see ["Reviewer Group Email Scope Advanced Options" on page 251](#) for more information on building the query.

8) Click *Next*.

The **Select Reviewers** screen appears.

9) You can select reviewers either from a list of individual users or mailing lists.

- a. Select either the **Mailing Lists** or **Users** tab.
- b. In the **Search** box type an email address or name and search for the results. A percent sign (%) will show all users or lists.
- c. Check the box beside the mailing list(s) or user(s) to select.
- d. Click **Add** to copy the selection to the **Selected Reviewers** pane. Repeat until all desired users and/or mailing lists are displayed in the right-hand pane.

NOTE Mailing List Membership is Dynamic, not Static

If you select a mailing list as the Reviewer who can access the scoped messages, the distribution list membership will be re-evaluated at the time the Reviewer Search is performed and, if necessary, changed based on the latest sync from the Active Directory environment. Therefore, users able to access those scoped messages will change as the members of the mailing list changes.

10) Click *Next*.**11) The **Confirm** screen appears showing a summary of the Reviewer Group created.**
To change anything, click **Back**.

To finish creating the Reviewer Group, click **Submit**.

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.

Task 8.8. Edit a Reviewer Group:

- 1) Because editing a Reviewer Group sometimes invalidates its associated Discovery Archives, please ensure that all associated Discovery Archives have been downloaded prior to editing the Reviewer Group.
- 2) From the EMS Admin Console, using a super-admin or root account, click **Historical Mail > Reviewer Groups**.

The **Reviewer Groups** screen appears.

- 3) Locate the Reviewer Group to be deleted, and then click the **Edit** button in the row.



The edit process takes you through the same four pages as the creation process.

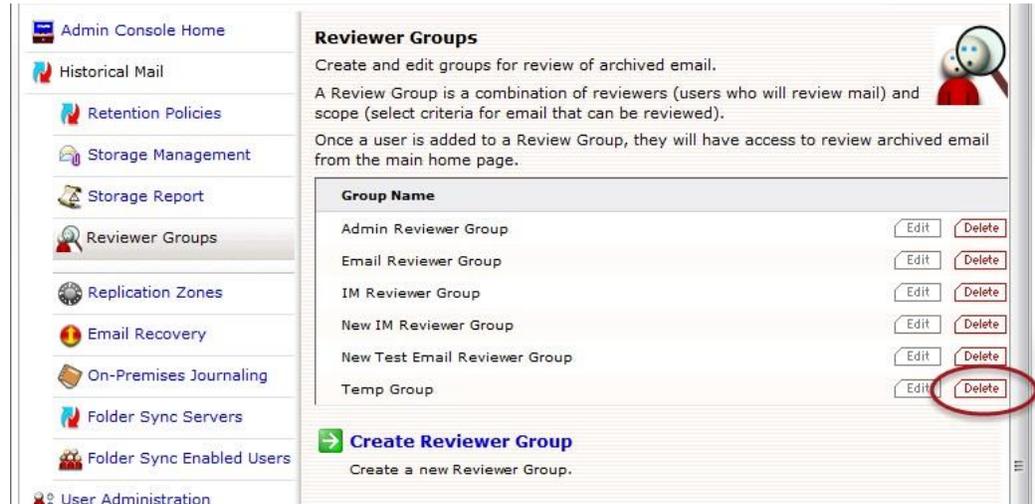
- 4) On the **Reviewer Group Name** page, only the **Name** of the group can be changed. Once a Reviewer Group is created to view emails or instant messages, this value cannot be changed. Click **Next**.
- 5) On the **Review Scope** page, add or delete users, user sets, mailing lists or servers from the scope of messages this Reviewer Group is allowed to see. Click **Next**.
- 6) On the **Select Reviewers** page, add or remove reviewers from the list. Click **Next**.
- 7) On the **Confirm** page, review the changes you have made. Click **Cancel** to erase the changes, or **Submit** to make the changes.

Task 8.9. Delete a Reviewer Group:

- 1) From the EMS Admin Console, using a super-admin or root account, click **Historical Mail > Reviewer Groups**.

The **Reviewer Groups** screen appears.

- 2) Locate the Reviewer Group to be deleted, and then click the **Delete** button in the row.



A confirmation pane appears.

- 3) If this Reviewer Group has Retention Holds still associated with it, the confirmation pane will display the number of holds and show only the **Cancel** button.

Click the **Cancel** button. Delete all the associated Retention Holds, and then return to this task. See [Task 8.5. "Delete a Retention Hold"](#).

- 4) If the Reviewer Group does not have any associated Retention Holds as **Delete** button will display on the confirmation pane. Click the **Delete** button to remove the Reviewer Group.

8.4.1. Reviewer Group Email Scope Advanced Options

TIP Refer to Email Archive Reviewer Guide

For information on creating this query string, refer to the *Email Management Services Archive Reviewer Guide* manual.

You can create complex reviewer scopes using an advanced search syntax. Use the fields described in [Table 8-1](#) to define searches that:

- Use specific terms, such as all messages that include the phrase `Quarterly Report`.
- 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.
- Use the Boolean operators `AND`, `OR`, and `NOT` to refine searches, such as messages from `bob@genericorp.com AND` that are smaller than 4 KB.

- Search for terms in proximity to other terms, such as terms that appear within four words of each other in a specified order.

8.4.1.1. Query Language Fields

Table 8-1 Query Language Fields

| Field | Description | Type | Example |
|------------------------------|---|--------|---|
| altrecipients ^{1,2} | Alternative recipients listed in the To field or Cc field of the envelope journal report. | String | altrecipients: bob_anderson@ genericcorp.com |
| attachedfiles | <ul style="list-style-type: none"> • A filename (If filename contains spaces, enclose in quotes) • Filenames joined by Boolean expressions (If filename contains spaces, enclose in quotes) • To match an ordered list of attachments use a semicolon separated list of all filenames, enclosed in quotes (No need to add extra quotes to filenames with spaces) | String | <ul style="list-style-type: none"> • attachedfiles: picture.jpg • attachedfiles: picture.jpg or "second picture.jpg" • attachedfiles: "report.xls; report.doc; Quarterly Report.ppt" |
| content | The content of the message. | String | content:"Q4 results" |
| dlists ¹ | Distribution lists listed in the To field or Cc field of the envelope journal report. | String | dlists: all_employees@ genericcorp.com |

Table 8-1 Query Language Fields

| Field | Description | Type | Example |
|----------------------------|---|--------|--|
| emaildate | <p>The date specified in the Sent Date field of the message header.</p> <p>To search by date only, use the form YYYY-MM-DD.</p> <p>To search by date and time, use the form YYYY-MM-DDThh:mm:ssZ.</p> <ul style="list-style-type: none"> T is a required constant that identifies the following characters as times. Z is an optional UTC (Coordinated Universal Time) time zone identifier. UTC is default. Use 24-hour clock when specifying time. <p>Use <code>min</code> and/or <code>max</code> to specify earliest/latest dates.</p> <p>Use <code><</code> or <code>></code> to specify dates before or after a certain date. Note: By default, <code>emaildate</code> is stored as UTC (GMT) time. To search using your local time zone value, use the <code>TIME</code> value to manually compensate for the number of hours offset from UTC. For example: <code>T05:00:00</code> is midnight in the US-Central time zone.</p> | Date | <p>To find messages sent between January 1, 2008, midnight (local) and January 3, 2009, midnight (local): <code>emaildate:range (2008-01-01T05:00:00, 2009-01-03T05:00:00)</code></p> <p>To find messages received after Aug. 21, 2012 use: <code>emaildate:>2012-08-21</code></p> <p>To find messages received before Aug. 21, 2012, use: <code>emaildate:<2012-08-21</code></p> |
| envrecipients ² | <p>The recipient information contained in the message envelope.³</p> <p><i>For non-journaled messages:</i> This field can be used to search for Bcc recipients. NOTE: Only email addresses found in retention policies can be found using this option. It will not find any email addresses that are external to your organization or not included in a retention policy.</p> <p><i>For envelope journaled messages:</i> This field contains all recipient information.</p> | String | <code>envrecipients: bob_anderson@genericcorp.com</code> |
| envsender | <p>The sender information contained in the message envelope.³</p> | String | <code>envsender:bob_anderson@genericcorp.com</code> |

Table 8-1 Query Language Fields

| Field | Description | Type | Example |
|------------------------------------|--|---------|--|
| filename | The file name of a document or message. <ul style="list-style-type: none"> When searching for an attachment, also set <code>isattachment:1</code> for the attachment file name. To search for a message, set <code>isattachment:0</code>. | String | <code>filename:report.xls</code> and <code>isattachment:1</code> |
| isattachment | An indicator of whether the document is an email attachment or a message. <ul style="list-style-type: none"> To indicate that the document is an attachment, set <code>isattachment:1</code>. To indicate that the document is not an attachment, set <code>isattachment:0</code>. | Integer | <code>filename:report.xls</code> and <code>isattachment:1</code> |
| mailbcc ^{1,2} | Recipients listed in the Bcc field of the envelope journal report. | String | <code>mailbcc:</code> <code>bob_anderson@</code> <code>genericcorp.com</code> |
| mailbccaltrecipient ^{1,2} | Alternative recipients listed in the Bcc field of the envelope journal report. | String | <code>mailbccaltrecipient</code> <code>: bob_anderson@</code> <code>genericcorp.com</code> |
| mailbccdlist ^{1,2} | Distribution lists listed in the Bcc field of the envelope journal report. | String | <code>mailbccdlist:</code> <code>all_employees@</code> <code>genericcorp.com</code> |
| mailcc | The recipients listed in the Cc field of the message header. | String | <code>mailcc:bob@</code> <code>genericcorp.com</code> |
| mailccaltrecipient ^{1,2} | Alternative recipients listed in the Cc field of the envelope journal report. | String | <code>mailccaltrecipient:</code> <code>bob_anderson@</code> <code>genericcorp.com</code> |
| mailccdlist ¹ | Distribution lists listed in the Cc field of the envelope journal report. | String | <code>mailccdlist:</code> <code>all_employees@</code> <code>genericcorp.com</code> |
| mailfrom | The sender listed in the From field of the message header. | String | <code>mailfrom:bob@</code> <code>genericcorp.com</code> |
| mailsubject | The subject of the message. <ul style="list-style-type: none"> If value contains spaces, enclose in double-quotes. | String | <code>mailsubject:</code> <code>"Quarterly Report"</code> |
| mailto | The recipients listed in the To field of the message header. | String | <code>mailto:</code> <code>bob@genericcorp.com</code> |
| mailtoaltrecipient ^{1,2} | Alternative recipients listed in the To field of the envelope journal report. | String | <code>mailtoaltrecipient:</code> <code>bob_anderson@</code> <code>genericcorp.com</code> |

Table 8-1 Query Language Fields

| Field | Description | Type | Example |
|-----------------------|---|--------|---|
| maillist ¹ | Distribution lists recipients listed in the To field of the envelope journal report. | String | maillist: all_employees@ genericorp.com |
| receiveddate | <p>The date the message was received by the email server.</p> <p>To search by date only, use the form YYYY-MM-DD.</p> <p>To search by date and time, use the form YYYY-MM-DDThh:mm:ssZ.</p> <ul style="list-style-type: none"> • T is a required constant that identifies the following characters as times. • Z is an optional UTC time zone identifier. UTC is default. • Use 24-hour clock when specifying time. <p>Use <code>min</code> and/or <code>max</code> to specify earliest/latest dates.</p> <p>Use <code><</code> or <code>></code> to specify dates before or after a certain date.</p> <p>Note: By default, <code>receiveddate</code> is stored as UTC (GMT) time. To search using your local time zone value, use the <code>TIME</code> value to manually compensate for the number of hours offset from UTC. For example: <code>T05:00:00</code> is midnight in the US-Central time zone.</p> | Date | <p>To find all messages received on or after February 3, 2008, use <code>receiveddate:range(2008-02-03, max)</code>.</p> <p>To find all messages received before February 3, 2008, use <code>receiveddate:range(min, 2008-02-03)</code></p> <p>To find messages received after Aug. 21, 2012 use: <code>receiveddate:>2012-08-21</code></p> <p>To find messages received before Aug. 21, 2012, use: <code>receiveddate:<2012-08-21</code></p> |

Table 8-1 Query Language Fields

| Field | Description | Type | Example |
|---------------------------------------|---|---------|--|
| recipients ² | <p>The recipients listed in one or more of the following:</p> <ul style="list-style-type: none"> The list of recipient information contained in the message envelope (see envrecipient field for details) The To field of the message header. The Cc field of the message header. Distribution lists listed in the To field or Cc field of envelope journal report.¹ Alternative recipients listed in the To field or Cc field of envelope journal report.¹ | String | (recipients:bob@genericcorp.com OR recipients:sue@genericcorp.com) |
| senders | The list of senders in the message envelope ³ or the From field of the message header. | String | (senders:bob@genericcorp.com OR senders:sue@genericcorp.com) |
| size | <p>The size of document (message or attachment) in bytes.</p> <p>Express sizes in bytes. For example, 4 KB as 4096.</p> <p>Use < or > to specify sizes greater or less than a certain size.</p> | Integer | To find all messages (messages only, without attachments) with a total size of at least 4KB but no greater than 8KB, use size:range (4096, 8192) |
| totalsize | <p>The size of the message, in bytes, including all attachments.</p> <p>Express sizes in bytes. For example, 4 KB as 4096.</p> <p>Or use < or > to specify sizes greater or less than a certain size.</p> | Integer | To find all messages with a total size (messages and attachments) of at least 8KB or greater, use totalsize:range (8192, max) |
| undisclosedrecipients ^{1, 2} | <p>Undisclosed recipients listed in one or more of the following:</p> <ul style="list-style-type: none"> The list of recipients in the Bcc field of the envelope journal report. The list of distribution lists in the Bcc field of the envelope journal report. The list of alternative recipients in the Bcc field of the envelope journal report. | String | undisclosedrecipients:bob_anderson@genericcorp.com |

1. This search field is only applicable to **envelope journaled messages**.
2. This search field is only applicable to **reviewer** searches.
3. The **message envelope** is the wrapper that contains the message's delivery directives.

8.4.1.2. Query Language Examples

Field Search

To search for a term in any field, type:

```
field:term
```

where

- `field` is one of the fields in Table 8-1 on page 252
- `term` is the value you want to find. To find a phrase, enclose it in double quotation marks.

For example:

To find all messages that include the phrase `Quarterly Report` in the **Subject** field

```
mailsubject:"Quarterly Report"
```

To find all messages sent from the email address `bob@genericcorp.com`

```
mailfrom:bob@genericcorp.com
```

NOTE Message Envelope Search Limitations For Non-Journaled Messages

Message envelope searches (*Recipients (Envelope)* and *All Recipients* filters, or *envrecipients* and *recipients* query language fields) can only search the envelope information that EMS is able to capture.

For undisclosed recipient information (including Bcc recipients), the only addresses that will be captured are internal addresses included in a retention policy.

When searching for undisclosed recipients, the undisclosed recipient headers will not be visible in the search results but the relevant messages will be included in the result set.

Search For Range of Dates or Sizes

To search for mail using a range of dates or a range of sizes, type

```
field:range(start, end)
```

where

- `field` is `emaildate`, `receiveddate`, `totalsize`, or `size`
- `range` defines the beginning and ending points of the search. `min` indicates the minimum size or data, and `max` indicates the maximum size or date.

For example:

To find all messages with a total size that is at least 4 KB but no greater than 8 KB

```
totalsize:range(4096, 8192)
```

To find all messages sent between December 25, 2003 and August 1, 2005 (local time)

```
emaildate:range(2003-12-25T05:00:00, 2005-08-01T05:00:00)
```

To find messages sent before December 25, 200 (local time)

```
emaildate:range(min, 2008-12-25T05:00:00)
```

To find messages received on or after August 2, 2005 (local time)

```
receiveddate:range(2005-08-02T05:00:00, max)
```

Proximity Search

NEAR

To search for words in proximity to each other, 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=numericValue` the *slop* for the search.

Slop is defined as the cumulative number of places that tokens may be moved in order to be considered a match the given phrase.

For example:

```
near(big, red, car, n=0) matches:
```

- the exact phrase "big red car"

```
near(big, red, car, n=1) matches:
```

- the phrase "big red * car" ("car" moved one token)
- and all phrases matched by `n=0`
- but does NOT match "big * red car" (both "red" and "car" moved one token, for a total slop of 2)

`near(big, red, car, n=2)` matches:

- the phrase “big red * * car” (car moved two tokens)
- the phrase “big * red car” (both “red” and “car” moved one token)
- the phrase “red big car” (both “big” and “red” moved one token)
- and all phrases matched by `n=1` and `n=0`
- but does NOT match “big * * red car” (both “red” and “car” moved two tokens, for a total slop of 4)

Boolean Operators

To combine search expressions using Boolean operators (AND, OR and NOT), use:

- AND *between* terms, to indicate *both* terms must be matched
- OR *between* terms, to indicate *either* term may be matched, but at least one *must* match
- NOT as a prefix to a term, to find terms that do *not* match the specified criteria
- Use matched parenthesis, ‘()’, to group terms

For example:

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 1, 2005, but not between those dates

```
NOT (emaildate:range (2003-12-25T05:00:00, 2005-08-01T05:00:00))
AND ("financial report" OR "balance sheet")
```

Find Partially Indexed Documents

To find only partially indexed documents, such as those that are too large or have damaged metadata, add `AND indexlevel:1` to the query.

To find documents sent before December 31, 2008 that have not been fully indexed

```
emaildate:range(min, 2008-12-31) AND indexlevel:1
```

8.4.1.3. Search Limitations

- **Use Caution When Editing Generated Queries**

The generated query may contain unfamiliar query arguments such as `linguistics` or `mode`. When editing a generated query, do not change these arguments, or the query may not return the expected search results.

- **Maximum Message Size 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.

- **Message Envelope Search Limitations**

Message envelope searches (*envrecipients* and *recipients* query language fields) can only search the envelope information that EMS is able to capture.

For undisclosed recipient information (including Bcc recipients), the only addresses that will be captured are internal addresses included in a retention policy.

When searching for undisclosed recipients, the undisclosed recipient headers will not be visible in the search results but the relevant messages will be included in the result set.

- **Limitations When Formulating Long Queries**

In Internet Explorer, the URL length limit of 2083 characters can cause errors when executing a long discovery query. If a query URL exceeds the character limit, Internet Explorer will display an error message and the query will not execute.

This scenario is most likely when using the Query Language or Query Builder options to build a complex query containing many search parameters. Simple searches are not likely to trigger this issue.

One workaround is to use a web browser with longer URL character limits, such as Mozilla Firefox. Another workaround is to narrow the search to fewer parameters.

- **Special Character Limitations**

If you submit a query containing only a single special character (such as a tilde, parenthesis, or exclamation point), the system returns all messages within your reviewer scope. The workaround for this issue is to use at least one alphanumeric character in your query in addition to the special character.

8.4.1.4. Questions and Answers

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 mail server (for example, being quarantined for spam or security reasons).
- The sender or 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.

8.5. Storage Management

Storage Management is an optional feature that must be enabled by Support.

To help reduce the size of Exchange mailboxes without using personal storage folder (PST) files, EMS provides a service called Storage Management, or *stubbing*. This service allows EMS to locate messages within end-user mailboxes that match size and age criteria defined by Administrators. When attachments are located that meet or exceed these criteria, EMS automatically removes these attachments from the messages and replaces each attachment with an HTML link (called a "stubs"), and stores the attachments within the EMS Datacenter, maintaining only one copy of an attachment that has been received by multiple recipients.

Administrators can set Storage Management policies based on the number of days the message has been in the user's mailbox, and on the size of the attachment, allowing different thresholds for standard and inline attachments.

To use any of these Storage Management features, you must first configure storage management retention scheduling as described in ["Configure Storage Management parameters" on page 125](#).

8.5.1. About Storage Management Policies

Storage Management policies differ from Retention policies in several ways:

- 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 and stubbed attachments are searchable within Email Archive.
- Storage Management policies 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.

Once a message is totally unstubbed, it reverts to the control of applicable retention policies.

Storage Management policies are set through the EMS Admin Console. Before creating Storage Management policies, consider the following:

- A minimum time period must elapse before a message can be stored. The default minimum 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 to report the effected users' messages are no longer being stubbed. The Storage Management policy is unchanged.

-
- You must have at least one VaultBox installed to implement Storage Management policies. And the VaultBox must have access to the Exchange server.
 - 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.
 - VaultBoxes used to support the Import Manager **cannot** be used in Storage Management policies.
 - If a VaultBox is to be deleted/removed, all that VaultBox's Storage Management policies must be reassigned with a new VaultBox before the old VaultBox is deleted.
 - 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. See ["Return Stubbed Files to User's Mailbox" on page 268](#)
- If multiple users' mailboxes contain the same email message, only one copy of the message will be stored by Storage Management.
- Ensure end users know to unstub messages before they use the Outlook® storage function to archive messages. If messages are not unstubbed, the messages will only retain the stubs, not the attachments themselves.

Also, if messages are archived in Outlook, Email Archive assumes the message has been deleted will not retain the attachment unless the email is subject to a retention policy.

- 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 whether email is accessed through Outlook® (users click on the stub's link to access the stored attachment) or the Outlook Extension (users' stored attachments appear the same as unstored attachments). For more information, please refer to the *Storage Management User Guide* or the online help provided with the Extension.

8.5.2. Manage Storage Management Policies

Storage Management policies can be created, edited, deleted, and reprioritized, and users can be assigned or unassigned to each policy.

Each user's messages are under the control of only *one* Storage Management policy, no matter how many policies the user is assigned to. The controlling policy is the highest priority policy that includes that user.

8.5.2.1. Create Storage Management Policies

Task 8.10. Create a Storage Management policy

- 1) From the EMS Admin Console, click the **Historical Mail** menu item and then the **Storage Management Policies** sub-menu item.

The Storage Management page is displayed.

Storage Management Policies

Storage Management Policies control the removal of attachments from messages on the primary mail server, and their storage in the Email Archive, in order to reduce the size of the primary mail store.

| Name | Criteria | Statistics | Actions |
|----------------------|---|------------|--------------------------|
| 1 Test Policy | Message older than: 90 days Attachment size larger than: 100 KB Inline content size larger than: 100 KB Vault Box: lab105vb | | Select Users Edit Delete |
| 2 Second Test Policy | Message older than: 180 days Attachment size larger than: 1000 KB Inline content size larger than: 1500 KB Vault Box: lab105vb | | Select Users Edit Delete |

[Create a new Storage Management Policy](#)
Create a new Storage Management Policy

[Reorder / Re-prioritize Policies](#)
Policies are prioritized in the order shown in the table above, with the highest priority policies at

- 2) Click the **Create a new Storage Management Policy** link.
- 3) In the **Storage Management Policy** section, **Name** field, type a name for the storage management policy.

Storage Management Policy Details

1 Storage Management Policy

Storage Management Policies control the removal of attachments from messages on the primary mail server, and their storage in the Email Archive, in order to reduce the size of the primary mail store.

To assign a user or group of users to a Storage Management Policy, use the "Select Users" button on the Storage Management Policies page.

Policy Name:

- 4) 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. (default is 90 days)

Once the above date criteria is met, then one or both of the following attachment size criteria must be met for the message's attachments to be stubbed by 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).

- 5) In the **VaultBox** section, select the appropriate VaultBox from the drop-down list.

- 6) Click **Submit** to return to the main Storage Management Policies window.
- 7) Locate the policy you just created, and click **Select Users**.

| Name | Criteria | Statistics | Actions |
|---------------|--|------------|---|
| 1 Test Policy | Message older than: 90 days Attachment size larger than: 100 KB Inline content size larger than: 100 KB Vault Box: lab105vb | | <input type="button" value="Select Users"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> |

- 8) From the user-picker, select all the users who are to become members of this Storage Management policy. Then click **Next**.
- 9) Confirm that the correct users have been selected for the policy's scope. If this is not correct, click **Back** to return to the user-picker. If correct, click **Submit** to finish creating the Storage Management policy.

8.5.2.2. Prioritize Storage Management Policies

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.

Each user's messages are under the control of only *one* Storage Management policy, no matter how many policies the user is assigned to. The controlling policy is the highest priority policy that includes that user. Before changing Storage Management policy priorities, consider the effects on the members as their controlling policy changes.

There must be two or more Storage Management policies in place for the **Reorder/Reprioritize Policies** option to appear.

Task 8.11. Prioritize Storage Management policies

- 1) From the EMS Admin 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**.

Storage Management Policies

Storage Management Policies control the removal of attachments from messages on Email Archive, in order to reduce the size of the primary mail store.

You can change the priority of storage management policies by simply dragging them

Save new ordering Revert

| Name | Criteria |
|--------------------------------|---|
| DRAG Test Policy | Message older than: 90 days Attachment size larger than: 100 KB Inline content size larger than: 100 KB Vault Box: lab105vb |
| DRAG Second Test Policy | Message older than: 180 days Attachment size larger than: 1000 KB Inline content size larger than: 1500 KB Vault Box: lab105vb |
| | Message older than: 90 days |

- 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**.

8.5.2.3. Edit Storage Management Policies

When editing Storage Management policies, you can change the name of the policy, the criteria for selecting messages to be handled by the policy, and the VaultBox that supports the policy. The editing page also shows you the **Change History** for the policy being edited.

Editing a Storage Management policy only changes the handling of future incoming messages. No messages currently stored are affected when editing a Storage Management policy.

Task 8.12. Edit Storage Management policies

- 1) From the EMS Admin Console, click **Historical Mail**.
- 2) Click **Storage Management Policies**.
- 3) Click **Edit** for the policy you want to change.

Storage Management Policies

Storage Management Policies control the removal of attachments from messages on the primary mail server, and their storage in the Email Archive, in order to reduce the size of the primary mail store.

| Name | Criteria | Statistics | Actions |
|----------------------|---|------------|--|
| 1 Test Policy 2 | Message older than: 90 days Attachment size larger than: 100 KB Inline content size larger than: 100 KB Vault Box: lab105vb | | Select Users <input type="button" value="Edit"/> <input type="button" value="Delete"/> |
| 2 Second Test Policy | Message older than: 180 days Attachment size larger than: 1000 KB Inline content size larger than: 1500 KB Vault Box: lab105vb | | Select Users <input type="button" value="Edit"/> <input type="button" value="Delete"/> |

- 4) If desired, enter a different policy name. This does not change anything in regards to the priority of the policy.
- 5) Change the Storage management criteria and/or change the VaultBox. Changing either of these two items applies only to future messages and does not change the behavior of messages already stored by the policy.
- 6) Click **Submit** to save the changes.

8.5.2.4. Delete Storage Management Policies

Deleting a Storage Management policy does two things:

- Removes the policy from the list, moving the next lower priority policy up into its place.
- Stops new messages from being stored based on the criteria of the deleted policy.

Deleting a Storage Management policy does NOT unstub its associated emails. And deleting a Storage Management policy cannot be undone.

Task 8.13. Delete Storage Management policies

- 1) From the EMS Admin Console, click **Historical Mail**.
- 2) Click **Storage Management Policies**.
- 3) Locate the policy you just created, and click **Delete**.

Storage Management Policies

Storage Management Policies control the removal of attachments from messages on the primary mail server, and their storage in the Email Archive, in order to reduce the size of the primary mail store.

| Name | Criteria | Statistics | Actions |
|----------------------|---|------------|---------------------------------|
| 1 Test Policy 2 | Message older than: 90 days Attachment size larger than: 100 KB Inline content size larger than: 100 KB Vault Box: lab105vb | | Select Users Edit Delete |
| 2 Second Test Policy | Message older than: 180 days Attachment size larger than: 1000 KB Inline content size larger than: 1500 KB Vault Box: lab105vb | | Select Users Edit Delete |

- 4) In the **Delete policy?** confirmation window, click **Delete** to delete the policy, or **Cancel** to keep the policy.

Deleting a Storage Management policy cannot be undone.

8.5.3. Return Stubbed Files to User's Mailbox

After removing a user from a Storage Management policy, email messages which had been stubbed (moved into storage and replaced with a link to the stored message) are *not* automatically unstubbed (the link removed and the attachment returned to the user's mailbox).

To unstub a message use the `unstub` command line tool, which is available on the EMS VaultBox. See "[Unstub Command Line Tool](#)" on page 269 for details.

Task 8.14. Unstub all messages for a user:

- 1) Log into the EMS Admin 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 **EMS Admin Console > Historical Mail > Storage Management.**)
- 6) Log into the VaultBox for this Storage Management Policy using the Active Directory Service Account.
- 7) Open a command prompt and navigate to the ActiveMailbox directory (usually `C:\Program Files\MessageOne\ActiveMailbox\`).
- 8) Run the following command, with 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.

8.5.4. Unstub Command Line Tool

After removing a user from a storage management policy, email messages which had previously been stubbed are *not* automatically unstubbed. To unstub a message use the `unstub` command line tool available on the EMS VaultBox.

The `unstub` command line can be found at the EMS client installation folder.

For detailed usage instructions type: `unstub -help`, you will see the following help description:

```
Usage: unstub [-verbose] and [-all], [-primarySMTPAddress
{userEmailAddress}], [-inputfile {path to the file}] or {exchange-
mailbox-id}
```

Where:

| | |
|--|--|
| <code>-all</code> | Unstub all users |
| <code>-primarySMTPAddress {the user smtp address}</code> | User's primary smtp email address to be unstubbed |
| <code>-inputfile {the path to the input file}</code> | The path to input file containing list of primary smtp email addresses to be unstubbed |
| <code>{exchange-mailbox-id}</code> | User's MailboxDN to be unstubbed |
| <code>-verbose</code> | Enable verbose output |

Example:

| | |
|---|---|
| To unstub all users | <code>unstub -all</code> |
| To unstub all users with verbose flag on | <code>unstub -verbose -all</code> |
| To unstub single user by primary smtp address | <code>unstub -primarySMTPAddress test_1@lab.com</code> |
| To unstub users based on input text file | <code>unstub -verbose -inputfile "C:\input.txt"</code> |
| To unstub single user by mailboxID | <code>unstub /o=first organization/ou=first administrative group/cn=recipients/cn=test_1</code> |

NOTE “unstub -all” Will NOT Unstub Cloud Users

If you choose the `-all` option to unstub all users, the `unstub` tool will execute for only the on-premises users who are *not* members of a storage management policy.

- Cloud users will *not* be processed.
- Users who are members of a storage management policy will also *not* be processed.

If you attempt to unstub a cloud user by specifying their primary SMTP address, you will receive an error stating the tool is unable to find the user with that SMTP email address. In verbose logging an exception is logged that the property `homeMDB` is not found. This is expected.

To unstub by primary SMTP addresses that are listed on the input file, you need to prepare the file first. The file should consist of a single primary SMTP address per line. One way to produce this file is using Exchange PowerShell (requires Exchange 2007 and above).

Example:

```
Get-MailboxDatabase -identity Exchange2007 | Get-Mailbox -
ResultSize Unlimited | Select-Object PrimarySmtpAddress >
PrimarySMTPAddressList.txt
```

The above command lists the primary SMTP address of all mailboxes on the mailbox database named "Exchange2007" store outputs that to the file `PrimarySMTPAddressList.txt`.

8.6. Storage Reports

The **Storage Reports** page provides reports for the messages stored under retention policies and for the number of messages indexed or stored per day.

If Storage Management is enabled, reports are also provided for messages stored under Storage Management policies.

All storage reports are updated daily, so statistics may not take into account changes made since the last calculations.

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 the next day.
 - 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.
-

Task 8.15. View storage reports:

- 1) From the EMS Admin Console, click **Historical Mail** menu item.
- 2) Click **Storage Report** menu item.
- 3) The **Storage Report** screen appears.

8.6.1. Retention Policy Statistics Report

The Retention Policy Statistics report lists each retention policy in priority order, along with the policy's type, name, duration, number of users and messages affected by the policy, and the total storage size of the policy.

| Retention Policy Statistics | | | | |
|-----------------------------|------------|----------------------|-----------|---|
| # | Type | Policy Name | Retention | Statistics |
| 1 | Membership | Member 60-day Policy | 60 days | Users: 1 Messages: 4 Total size: 28.1 KB |
| 2 | Membership | Member 1-year Policy | 365 days | Users: 6 Messages: 22 Total size: 115.7 KB |

Table 8-2 Retention Policy Statistics Report

| Field | | Description |
|-----------------------------|------------|--|
| # | | Priority of the retention policy. The higher priority (smaller number) policy controls the retention duration of messages included in multiple retention policies. |
| Type | | Category of retention policy. <ul style="list-style-type: none"> • Capture: Capture Based Policy: Retention rules apply to messages to or from users in the policy at the time the message was captured. • Membership: Membership Based Policy: Retention rules apply to users currently in the policy. • Retention Hold: Query-Based Retention Hold: An Email Archive Reviewer identifies specific messages (found by a query) to be retained indefinitely. • User Classification: User Classification Policy: Allows designated users to determine which messages are retained under the policy. |
| Policy Name | | The name of the retention policy |
| Retention | | The length of time (days) the messages governed by the policy are kept. |
| Statistics (Daily Snapshot) | Users | The number of users included in the scope of the policy. This count includes only current policy membership. No historical information is maintained as users are added to or removed from a policy. |
| | Messages | The number of messages included within the scope of the policy. This count includes only current policy scope. No historical information is maintained. |
| | Total size | The total storage space required for all the messages within the scope of the policy. This value includes only current storage space. No historical information is maintained. |

8.6.2. Storage Management Policy Statistics Report

This report is displayed if Storage Management is enabled.

Storage Management Policies control the removal of attachments from messages on the primary mail server, and their storage in the Email Archive, in order to reduce the size of the primary mail store.

The Storage Management Policy Statistics report displays all Storage Management policies in priority order, and ends with a summary totaling all users and messages governed by these polices and the total storage size.

| Storage Management Policy Statistics | | | |
|--------------------------------------|--|--|---|
| # | Policy Name | Criteria | Statistics |
| 1 | Automation Storage Management Policy DBCS | Minimum age: 0 days Attachment size: 70 KB Inline content size: 1 KB VaultBox: lab066vb | |
| Storage Management Totals | | | Users: 1 Messages: 11 Total size: 3.2 MB |

Table 8-3 Storage Management Policy Statistics Report

| Field | Description |
|----------------------------|---|
| # | Storage Management Policy priority. The higher priority (smaller number) policy determines which attachments are removed and stored in the archive. |
| Policy Name | The name of the Storage Management policy. |
| 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. |
| VaultBox | The VaultBox to which the policy applies. |
| Users | The total number of users governed by Storage Management policies. This count includes only current policy membership. No historical information is maintained as users are added to or removed from policies. |
| Messages | The total number of messages stored by all the Storage Management policies. |
| Total size | The total amount of storage space consumed by the messages under all the Storage Management policies. |

8.6.3. Aggregate Statistics Report

Since multiple storage or retention policies may apply to a message and/or user resulting in the message/user being included in multiple policy counts, this report totals the number of users and messages governed by all storage policies, and totals the amount of storage consumed for all policies.

| Aggregate Statistics | |
|----------------------|--------|
| Statistics | |
| Users: | 10 |
| Messages: | 50 |
| Total size: | 9.9 MB |

Table 8-4 Aggregate Statistics Report

| Field | Description |
|-------------------|--|
| Users | Total number of users affected by all policies, with each user counted only once. This count includes only current policy membership. No historical information is maintained as users are added to or removed from policies. |
| Messages | Total number of messages stored by all policies, with each message counted only once. |
| Total size | Total amount of storage space consumed by the messages stored under all policies. |

8.6.4. Daily Message Volume Report

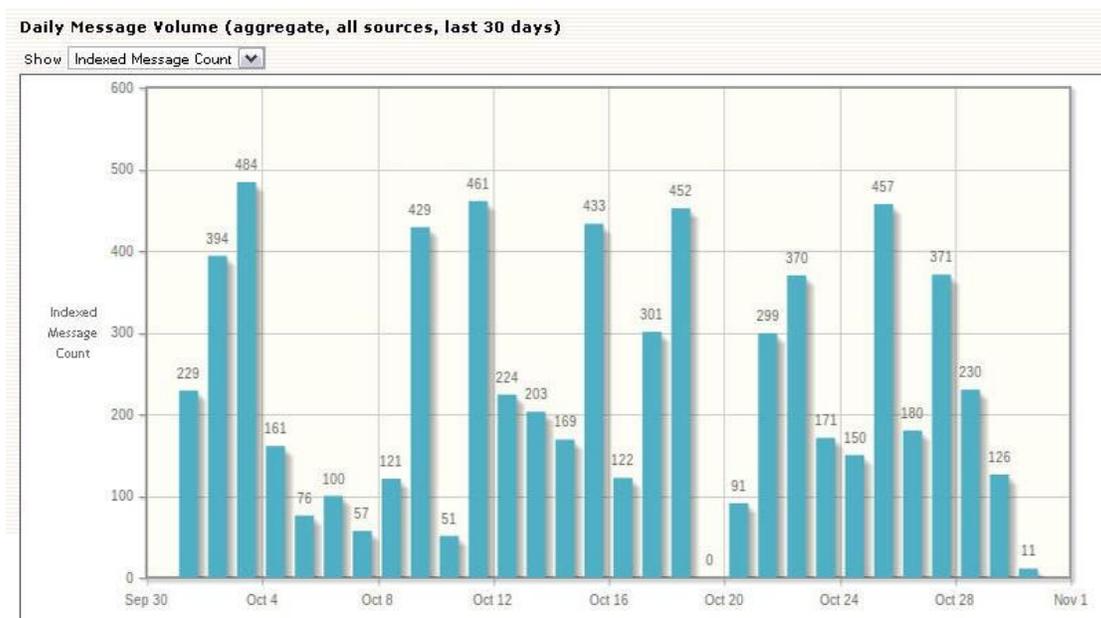
The Failed Message Tracking feature adds a new graphical Daily Message Volume report to the **Storage Report** page.

The Daily Message Volume report contains three graphs that display the aggregate number of messages processed each day, from all sources, for the last thirty days.

- **Indexed Message Count:** The number of messages that were successfully indexed.
- **Stored Message Count:** The number of messages per day that were successfully stored.
- **Failed Message Count:** The number of messages that failed to be indexed and/or stored. This count does not include messages that were able to be partially indexed.

To access this report select **Historical Mail**, then **Storage Report**, and scroll down to the bottom of the page.

The **Show** drop-down selects between the three graphs: Indexed, Stored, or Failed Message Count.



8.7. Create and Recover Archives

The sections below describe how to create Historical Mail archives. See ["Time-Based Recovery Archives" on page 275](#), ["Activation-Based Recovery Archives" on page 277](#), ["Search-Based Recovery Archives" on page 279](#) and ["Discovery Archives" on page 279](#).

After you have created an archive, you can use the RecoveryManager to restore messages to user mailboxes. See ["Use RecoveryManager to Restore Archives" on page 280](#).

Recovery Archives cannot be exported by Export Manager. If you need to use Export Manager, create a Discovery Archive.

Email messages that are contained in a Recovery or Discovery Archive are kept until the archive is deleted, regardless of any applicable retention policies. After the archive is deleted, control of each message's purge status reverts to the highest priority applicable retention policy.

8.7.1. Time-Based Recovery Archives

A Time-Based Recovery Archive allows you to create a Recovery Archive based on the following criteria:

- Start date and time

- End date and time
- Users whose emails are to be included in the archive.

Some sample definitions of Time-Based Recovery Archives might include:

- All messages for user John Jones between January 1, 2006 and September 1, 2006.
- Mail for all users on the mailing list `Sales` between July 1, 2006 and August 1, 2006.

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

Task 8.16. Create a Time-Based Recovery Archive:

- 1) From the EMS Admin 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 **Archive Name** field. All archive names must be unique.

- 5) In the **Include email from** field:
 - a. Select **click to edit** to use the calendar to define a start date and time.

- b. Select **click to edit** to use the calendar to define an end date and time.
- 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**, **User Sets**, or individually by **User**.
 - a. If you select the **Mailing Lists** or **Users** 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 **Servers** tab, click a server to select it.
 - c. If you select the **User Sets** tab, check the box by the desired user set to select it.
- 8) Click **Add**.
- 9) Repeat until all desired users are listed in the right-hand pane.
- 10) Click **Next**. A summary screen describing the Recovery Archive you've defined appears.
- 11) Click **OK** to create the archive.

You are returned to the **Email Recovery** page.

You can now use the RecoveryManager to restore these messages to end users' mailboxes, or to a designated mailbox for review.

8.7.2. Activation-Based Recovery Archives

An Activation-Based Recovery Archive allows you to create a Recovery Archive based on the following criteria:

- Start date and time
- Activation beginning date and time
- Users whose emails will be included in the archive.

Some sample definitions of Activation-Based Recovery Archives might include:

- All messages for user John Jones between January 1, 2006 2:00am and the activation that began on January 2, 2006 at 5:00am.
- Mail for all users on the mailing list `Sales` between July 1, 2006, 12:00am and the activation that began on July 3, 2006 at 3:14pm.

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

Task 8.17. Create an Activation-Based Recovery Archive:

- 1) From the EMS Admin 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 **Archive Name** field. Each archive name must be unique.

1 Select Recovery Archive Time Range (1 of 3)

Please enter a name for the Email Recovery Archive and select a time window prior to an activation to recover mail from.

Archive Name:

Include email from: [\(click to edit\)](#)

until:

Next

- 5) In the **Include email from** field, select **click to edit** to use the calendar to define a start date.

Include email from: [\(click to edit\)](#)

until:

| January, 2014 | | | | | | |
|---------------|-----|-----|-----|-----|-----|-----|
| Sun | Mon | Tue | Wed | Thu | Fri | Sat |
| | | | | 1 | 2 | 3 |
| 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 |
| 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| 25 | 26 | 27 | 28 | 29 | 30 | 31 |

Time: :

Select date

- 6) In the **until** dropdown, select the activation that will define the ending of this recovery archive.
- 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**.
- 9) Repeat until all desired users are listed in the right-hand pane.
- 10) Click **Next**. A summary screen describing the Recovery Archive you've defined appears.
- 11) Click **OK** to create the archive.

You are returned to the **Email Recovery** page.

You can now use the RecoveryManager to restore these messages to end users' mailboxes, or to a designated mailbox for review.

8.7.3. Search-Based Recovery Archives

If you are a super-admin or have Email Archive Reviewer privileges, you can create a Search-Based Recovery Archive which allows you to create a Recovery Archive based on Email Archive search criteria.

When you click the **Create Search Based Recover Archive**, you are taken to the Email Archive main search page as an Email Archive Reviewer.

Refer to the *Email Archive Reviewer Guide* for complete instructions on creating search-based recovery archives.

After the archive is created, you can use the RecoveryManager to restore the archive's messages to multiple end users' mailboxes, or to a designated mailbox for review. Recovery Archives cannot be exported by Export Manager. If you need to use Export Manager, create a Discovery Archive.

When you recover a Search-based Recovery Archive, you are not pulling up a static set of messages, but rather pulling up all the messages in the archive that currently match your stored query criteria.

NOTE Maximum Message Limits in Recovery Archives

Email Archive now limits the maximum number of messages in Recovery Archives to prevent improperly configured queries from monopolizing system resources. Requests to produce an over-sized query will fail, and the reason for the failure will appear in the audit log.

To export extremely large numbers of messages for archival, create multiple archives.

8.7.4. Discovery Archives

Discovery Archives contain email messages bundled into an archive in a way that allows it to be recovered back to the email system into a single mailbox or exported by Export Manager (see *EMS Export Manager Guide*). Discovery Archives are different than Recovery Archives because Recovery Archives can be imported into multiple mailboxes and cannot be exported by Export Manager.

Email Archive Reviewers and administrators with reviewer privileges can 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. Or the Discovery Archive can be exported to a PST or EML file using Export Manager.

For more information on creating Discovery Archives, see the *Email Archive Reviewer Guide*.

When you recover or export a Discovery Archive, you are pulling up a static set of messages that matched the query criteria at the time the Archive was created.

NOTE Maximum Message Limits in Discovery Archives

Email Archive now limits the maximum number of messages in Discovery Archives to prevent improperly configured queries from monopolizing system resources. Requests to produce an over-sized query will fail, and the reason for the failure will appear in the audit log.

To export extremely large numbers of messages for export, create multiple archives.

8.7.5. Use RecoveryManager to Restore Archives

Use RecoveryManager to recover Historical Mail archives to user mailboxes. Create the recovery archive using the instructions under ["Time-Based Recovery Archives" on page 275](#), ["Activation-Based Recovery Archives" on page 277](#), ["Search-Based Recovery Archives" on page 279](#) and ["Discovery Archives" on page 279](#) before launching the RecoveryManager.

To recover an archive that was created during an Email Continuity activation, see ["Restore Mail to Users' Mailboxes" on page 208](#)

Task 8.18. Recover a Historical Mail archive to user mailbox(es):

- 1) From the EMS server, select **Start > Programs > MessageOne > RecoveryManager**.
- 2) Log in to RecoveryManager using credentials that have sufficient permissions to access the mailboxes being imported.

Username:

Password:

Click the link below to begin the mailbox recovery process.

RecoveryManager runs under the credentials of the currently logged in user. Please make sure the account you are logged into Windows with has sufficient permissions to access the mailboxes being imported (e.g. The Service Account).

[Start Recovery](#)

- 3) Click **Start Recovery**.
- 4) Select a working directory for RecoveryManager to use as a temporary data store during the import process. You can:
 - Use the default directory.

- Click **Browse** and locate and select any directory with plenty of space.
- Type the path into the Working Directory box.

recovery process.

Working directory:

Activation Recovery Active Recovery

| Name | Mailboxes | Messages |
|--------------|-----------|----------|
| TestArchive | 1 | 169 |
| TestArchive3 | 1 | 81 |
| TestArchive4 | 1 | 11 |
| test | 1 | 11 |
| Another Test | 1 | 176 |
| temp archive | 1 | 100 |

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

- 5) Select the **Active Recovery** radio button to recover Recovery or Discovery Archives.

To recover archives generated during an Email Continuity Activation, use the **Activation Recovery** radio button. See ["Restore Mail to Users' Mailboxes" on page 208](#) for this procedure.

- 6) Click to select the appropriate archive from the list.

To refresh the list click **Refresh List**.

- 7) Click **Continue**.

If the directory chosen doesn't exist, a pop-up asks if you want to create it. Click **Yes** to continue.

Metadata about the archive is downloaded into the working directory and the Platform page is brought up.

- 8) The platform and settings information displayed as default in fields on the top part of this page reflects settings pulled from SyncManager and allows RecoveryManager to access the primary mail system. Typically, these settings are not changed as part of recovering archives.

Platform:

Directory Settings

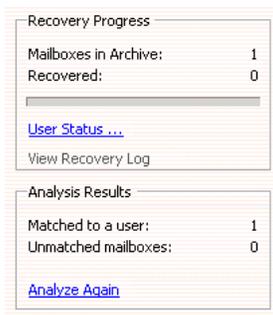
Global Catalog Server:

Mailbox Access Settings

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](#)

- 9) During an archive 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 synchronization was successful, RecoveryManager can use the cached results from the directory synchronization for the recovery process. To use this cached data, select the **Skip detailed analysis** check box.
- 10) Click **Continue** to begin the archive recovery analysis.
- 11) EMS 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**.
- 12) The next RecoveryManager page controls how the archive is recovered. Status indicators are displayed in the left column of the page.



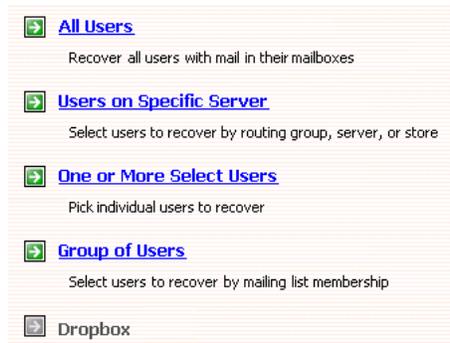
- **Mailboxes in Archive** — The total number of mailboxes in the archive.
 - **Recovered** — The number of mailboxes for which mail has been recovered.
 - Click the **User Status...** link to display the status of each individual user, including user names per server, user accounts with email data for recovery, and user accounts that cannot be matched to an account on the primary mail system.
 - **Matched to a user** — Displays the number of user accounts that 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.
 - Click the **Analyze Again** link to repeat the analysis done in [step 11](#) above.
- 13) 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, follow the directions below. Skip this step if your organization does not use a third-party journaling product. See [Task 7.3. "Recover mail from an activation:" step 13](#) on page [page 212](#) for more information.
 - 14) If you selected an archive that is a Discovery Archive, the only option on the right side of the pane is **Discovery Archive**. Otherwise, if you selected a Recovery Archive skip to [step c](#).
 - a. Click **Discovery Archive** button.

- b. From the **Server** drop-down list, select the server for the Discovery Archive.
- c. From the **Mailbox** drop-down list, select a user's mailbox for the Discovery Archive.
- d. Click **Continue**.
- e. 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 sub-folder labeled with the user name of the user who created the archive, with additional sub-folders **Inbox** and **Sent Items**.

15) Proceed with this step if you selected a Recovery Archive.

- a. From the list of options in the right column, select the set of users to recover.



- **All Users** — This option imports email data for all users who were activated during the outage, who used the webmail interface, and for whom data has not yet been recovered.
- **Users on a Specific Server** — This option recovers email data for users on a selected message store, server, or group of servers.

If you select this option, you must also:

Check any combination of individual mail stores, servers, or server groups for recovery. (Servers without users that need recovery are greyed out.)

Click **Continue**.

- **One or More Select Users** — This option recovers the mailbox of one user or the mailboxes of selected users by name.

If you select this option, you will be taken to a page that 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.

Select the users to recover, then click **Add** to copy them to the user list in the right-hand column.

When you have 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 appears 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** — This option recovers users based on distribution list membership. When selected, the display lists all distribution lists with members who have email that needs recovery.

If you select this option, you will taken to a new page to:

Select a group of users and then click **Add** which will copy the group to the right-hand column. Continue to add groups until all you desire are copied to the right.

Click **Continue**.

- **EMS Dropbox** — This 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:

Select a mailbox to which all drop box content will be imported.

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.

- b. Once you've completed the required information and clicked **Continue**, you are taken to the summary screen which lists the users identified for recovery.

c. Choose how to restore the mail.



- (1) Leave both the **Recover to alternate folder** and the **Recover all messages to single mailbox** options unchecked to import the messages into a folder labeled with the reviewer's user name with sub-folders **Inbox** and **Sent Items**.
- (2) 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 sub-folder labeled with the user name of the user who created the archive, with additional sub-folders **Inbox** and **Sent Items**.



- (3) To recover all messages 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 recovered using this option will appear in the mailbox you chose.

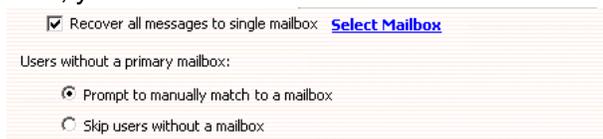


- (4) To recover all messages to a single mailbox but place them in a designated folder, complete both the **Recover to alternate folder** and **Recover all messages to single mailbox** options.

After recovery is completed, messages recovered using both options will appear in the single mailbox you designated, with the alternate folder listed, like this:



- d. During the recovery process, if RecoveryManager encounters any unmatched mailboxes, you can:

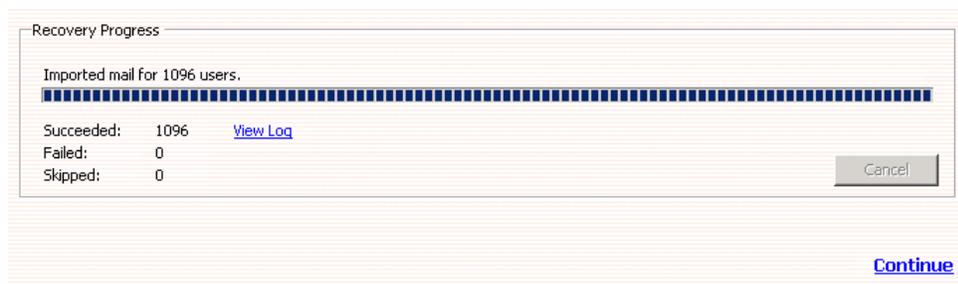


- (1) Click **Prompt to Manually Match a Mailbox** to select the correct server and mailbox for each user's account not automatically matched. If this option is chosen, whenever a mailbox cannot be matched, the following screen appears for you to select a mailbox.

- (2) Click **Skip Users** to reroute unmatched mailboxes later.

- 16) Click **Start Recovery** to begin importing data.

- 17) RecoveryManager downloads email data from the Email Management 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 Cancelling 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.

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

NOTE Email Archive 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.

- 20) Log in to the designated email account to view the contents of the Archive.

8.8. On-Premises Journaling Administration

8.8.1. Managing On-Premises Journaling Addresses

The **On-Premises Journaling** window (**Historical Mail > On-Premises Journaling**) manages the journaling addresses to which all copies of on-premises journaling mail are sent.

| Replication Zone | Journaling Address | Last Journal | Action |
|---------------------|--|----------------------------|--------|
| rustcloud.m1dev.com | 0b62c843b4e072711af58bf74056a592351a229d7db3eccc86fbb4121ed297a5@rustcloud.m1dev.com | 12-12-2012 01:10:58 AM CST | Delete |

A journaling address is a Globally Unique Identifier (GUID). On-Premises Journaling user's journaling addresses tie to an EMS Data Center.

Task 8.19. Add On-Premises Journaling Address

- 1) Click on **Historical Mail > On-Premises Journaling**
- 2) Click on **Add On-Premises Journaling Address** link.
- 3) Select the zone for which the address is to be assigned.
- 4) Click **Create**.

Task 8.20. Delete On-Premises Journaling Address

- 1) Click on ***Historical Mail > On-Premises Journaling***
- 2) To the right of the address to be deleted, click the ***Delete*** button.
- 3) In the verification pane, click ***Delete***.

NOTE Do Not Delete Journaling Address Before In-Process Tasks Complete

Before retiring an existing journaling address and beginning to use a new one, it is recommended you create and configure the new address and allow sufficient time for existing messages which may be currently in-process to be archived/imported before deleting an existing journaling address.

8.8.1.1. On-Premises Journaling Address Best Practices

For most organizations, the single On-Premises Journaling address created when the feature was enabled is sufficient.

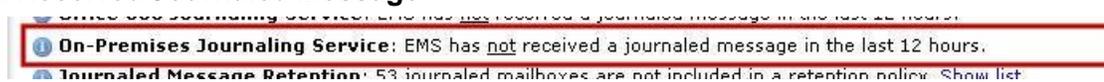
If it becomes necessary to retire a journaling address, it is recommended that all journaling rules be updated with a new journaling email address and that sufficient time (up to 48 hours) be allowed to elapse before retiring any existing journaling address.

WARNING Do Not Delete Journaling Address Until New Address Is Fully Functional

After a journaling address has been deleted from the EMS admin console, new mail received by the EMS Data Center addressed to that deleted address will be rejected, resulting in unrecoverable, lost data.

8.8.2. On-Premises Journaling Readiness Checks

Not Received Journaled Message

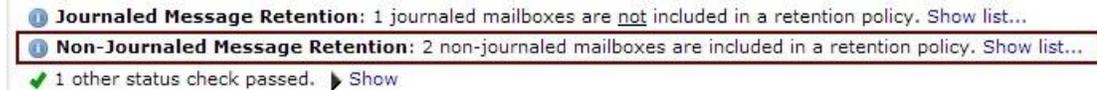


This readiness check indicates a journaled message has not been received in the last 12 hours.

If this readiness check is displayed, verify the Exchange environment is set to send journaled messages to EMS. This error message could also mean there is a misconfiguration, like an improper journaling address. Contact Support if further assistance is required.

Because Retention Policies and Exchange Journaling rules are managed separately, it is possible that there may be a mismatch between the users managed in each policy. EMS provides administration console readiness checks if one or more of the following conditions are true:

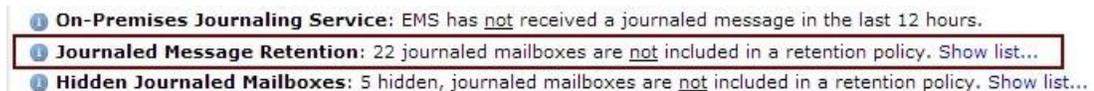
Non-journaled mailbox in retention policy



If EMS detects one or more Exchange mailboxes that are in Email Archive retention policies but not enabled for Exchange Envelope Journaling, a **Non-Journaled Message Retention** readiness check will display.

- Click on **Show List** to see the mailboxes (first 50 are shown, remainder can be downloaded into CSV file).

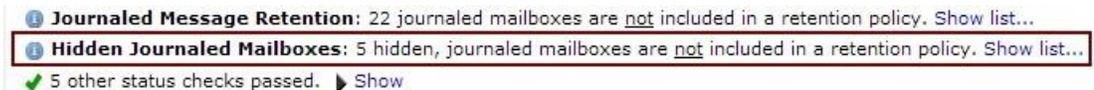
Journaled mailbox not in retention policy'



If EMS detects one or more Exchange mailboxes that is enabled for Exchange Envelope Journaling but is *not* in an Email Archive retention policy, a **Journaled Message Retention** readiness check will display

- Click on **Show List** to see the mailboxes (first 50 are shown, remainder can be downloaded into CSV file).

Hidden mailbox not in retention policy



If one or more Exchange mailboxes or distribution lists are hidden or disabled, but are enabled for Exchange Envelope Journaling, a **Hidden Journaled Mailboxes** readiness check will display.

- Click on **Show List** to see the mailboxes (first 50 are shown, remainder can be downloaded into CSV file).

8.9. Folder Sync Administration

Administration tasks for the Folder Sync feature involve maintenance of the Exchange server to Folder Sync server relationship, and enabling/disabling users whose mailbox folder structure is to be synced by the Folder Sync feature.

For additional information about the Folder Sync feature, see:

- ["About Folder Synchronization" on page 28](#)

- ["Folder Sync Prerequisites" on page 77](#)

8.9.1. Folder Sync Servers

After Folder Sync feature has been enabled by Support and VaultBoxes have been upgraded to at least the minimum Client Software version, Folder Sync Servers need to be mapped to Exchange Servers, which is done on the **Historical Mail > Folder Sync Servers** page. Exchange Servers not mapped will appear at the bottom of the page and none of the mailboxes on those Exchange Servers will be synced until they are successfully mapped to Folder Sync Servers.

- Administrators of larger environments can configure multiple Folder Sync Servers to segment sync traffic from specific Exchange servers.
- Only Exchange servers (Exchange 2007 SP1 and above) with the Mailbox Role can be mapped to a Folder Sync Server.
- When a Folder Sync Server undergoes an uninstall/unregister of its EMS client software, the Exchange Servers that were mapped to that Folder Sync Server are marked with a double asterisk. If that Folder Sync Server gets upgraded to a new client software version and uses the same key, EMS will attempt to re-map the old Exchange servers to the upgraded, if they haven't already been re-assigned.

NOTE Folder Sync Server Mapping Not Maintained In Clean Install

If the Folder Sync Server performs a clean uninstall and a clean install (NOT an upgrade), then the EMS client software will get a new registration key and the Exchange servers can not be automatically remapped to previous Folder Sync Servers.

Task 8.21. Assign Exchange Servers to Folder Sync Servers

- 1) Click the **Historical Mail > Folder Sync Servers** menu item.

The **Folder Sync Server** page appears.

Folder Sync Servers

Map Exchange servers to Folder Sync Servers. Each Exchange server may be in only one Folder Sync Server, but Folder Sync Servers may contain multiple Exchange servers.



| Folder Sync Server Name | Assigned Exchange Servers |
|---|---------------------------|
|  sample-server | |
|  sample-server-2 | |

| Unassigned Exchange Server Name | Action |
|---------------------------------|--|
| SAMPLE-EX-1 | Add to Folder Sync Server sample-server Add to Folder Sync Server sample-server-2 |
| Office365 | This server is an Exchange server that does not have the mailbox role and is not allowed to be associated with a Folder Sync Server. |

Note: Any unassigned Exchange servers marked with a ** before them indicate that they currently belong to an *inactive* Folder Sync Server. Should this Folder Sync Server come back online, these servers will automatically be re-mapped to their original Folder Sync Server. However, they may be safely remapped now, but they would *not* be re-mapped to their original Folder Sync Server after the new assignment.

- 2) The Exchange servers that are available to be assigned are listed in the bottom pane of the window. Beside each Exchange server are links that assign it to a Folder Sync server. To assign an Exchange server to a Folder Sync server, click the appropriate link.

Multiple Exchange servers can be assigned to one Folder Sync server, but each Exchange server can be assigned to only one Folder Sync server.

Unassigned Exchange servers marked with a ** before them indicate that they belonged to a currently inactive Folder Sync server. Should this Folder Sync server come back online, these Exchange servers will be automatically re-mapped to their original Folder Sync server. These Exchange servers may be safely remapped, but doing so would mean they could not be re-mapped to their original Folder Sync server should it come back online.

- 3) Once all the Exchange servers are assigned, users can be enabled for Folder Sync. See [Task 8.23. "Enable users for Folder Sync"](#)

Task 8.22. Remove Exchange Servers from Folder Sync Servers

- 1) Click the **Historical Mail > Folder Sync Servers** menu item.

The **Folder Sync Server** page appears.

- 2) In the top pane of the page, beside each Folder Sync server, the assigned Exchange servers are listed with a **Delete** button beside it.
- 3) Click the **Delete** to unassign that Exchange server.

The unassigned Exchange server will be moved to the bottom pane, ready to be reassigned.

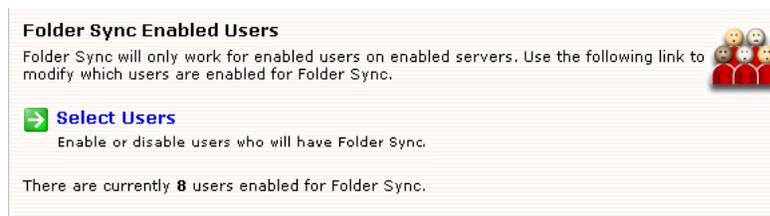
8.9.2. Folder Sync Enabled Users

By default, users are not enabled for Folder Sync, so they must be enabled before their folder data can be synchronized and made available to Email Archive.

Users *not* synced will not have their folder structure displayed in the Archive UI, but all incoming and outgoing messages will still be searchable in Email Archive.

Task 8.23. Enable users for Folder Sync

- 1) Click the **Historical Mail > Folder Sync Enabled Users** menu item.
- 2) The **Folder Sync Enabled Users** page appears.



- 3) Click the **Select Users** link.
The **Select Folder Sync Users** page appears.
- 4) Identify the users to be enabled for Folder Sync. You can locate and select users to add based on several criteria. For example:
 - a. To enable all administrators, click the **User Sets** tab, select **All Administrators**, and click **Add**.
 - b. To enable 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 and System-created User Sets are Dynamically Updated

Administrators do not have to manually add or delete users to the Folder Sync enabled user list when a distribution list or system-created user set changes. The distribution lists and system-created user sets are updated when SyncManager runs and the enabled users scope is dynamically updated. User-created user sets are NOT dynamically updated.

NOTE Deletion of Distribution Lists Used in Folder Sync Enabled Users List

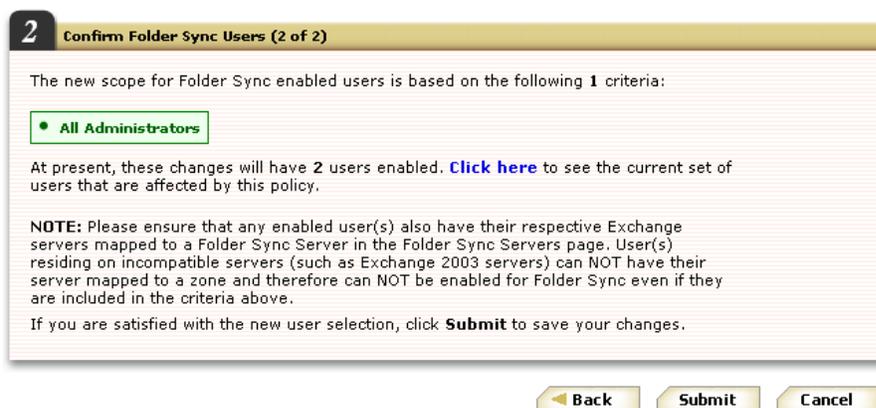
If a distribution list used as a Folder Sync enabled user is deleted on Exchange, the distribution list is placed on a purge list and a fault alert notice is sent to each member of the fault alerts notifications list. This allows a 30-day window for Administrators to recover from accidental deletion of lists, before functionality is lost.

- c. To enable all users with mailboxes on designated email servers, click the **Servers** tab. Select the appropriate server listings and click **Add**.
 - d. To enable 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**.
- 5) Repeat adding users from any or all of the above categories, clicking **Add** to copy the selected users to the **Current selection** pane on the right, until all the users to be enabled for Folder Sync have been defined.

If an item listed in the right-hand pane is incorrect, check the box beside the item and click **Remove**, to remove the entry from the **Current selection** list.

- 6) When all appropriate users have been added to the **Current selection** pane, click **Next**.

The **Confirm Folder Sync Users** page appears.



- 7) Examine the contents of this page, which lists all users now enabled.

NOTE Users must have Exchange servers mapped

Please ensure that any enabled user(s) also have their respective Exchange servers mapped to a Folder Sync Server in the Folder Sync Servers page. User(s) residing on incompatible servers (such as Exchange 2003 servers) can NOT have their server mapped to a zone and therefore can NOT be enabled for Folder Sync even if they are included in the criteria above.

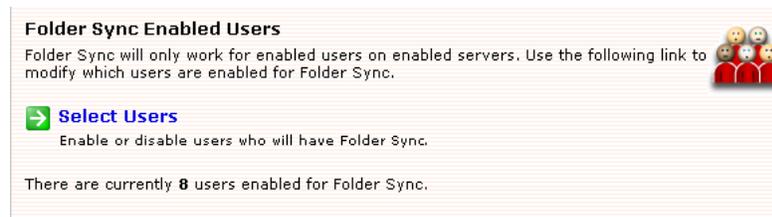
To see a list of all individual users affected by the policy click the **Click here** link, which pops up a new window containing a user list. To export this list to a CSV file, click the **Export to file** link at the top-right of the pop-up window.

- 8) If the data is correct, click **Submit**.

Task 8.24. Disable users for folder sync

- 1) Click the **Historical Mail > Folder Sync Enabled Users** menu item.

- 2) The **Folder Sync Enabled Users** page appears.



- 3) Click the **Select Users** link.

The **Select Folder Sync Users** page appears.

- 4) In the **Current selection** pane, check the box(es) beside the user, distribution list, server or users set to be disabled, and click **Remove** to remove the checked items from the **Current selection** pane.

If only groups of users (user sets, servers or distribution lists) are displayed in the **Current selection** pane and you need to disable an individual user who is a member of one or more of those groups, the individual user must be removed from the list(s) itself. An individual user cannot be disabled from Folder Sync if they are a member of a enabled group.

- 5) Click **Next**.
- 6) The **Confirm Folder Sync Users** page appears. See [step 6](#) and [step 7](#) in [Task 8.23. "Enable users for Folder Sync"](#) for more information on this step.
- 7) Verify the change, if correct click **Submit**.

8.9.3. Folder Sync Advanced Settings

The following settings are available in instances where Folder Sync operations are negatively affecting system performance.

8.9.3.1. Implement Exclusion Hours

Folder Sync configurations are stored in the registry. They can be found under `HKEY_LOCAL_MACHINE\Software\MessageOne\EMS\FolderSync`.

ExcludedStartHour: (Valid value is 0-23. Default: 0.) This is the excluded start hour in which the Folder Sync must NOT run. The sync may not stop for up to 15 minutes after the `ExcludedStartHour` because the internal timer checks the excluded hours value every 15 minutes.

ExcludedEndHour: (Valid value is 0-23. Default: 0.) This is the excluded end hour in which the Folder Sync can run after the start of this hour. The sync's start may be delayed up to 15 minutes after the `ExcludedEndHour` because the internal timer checks the excluded hours every 15 minutes.

When `ExcludedEndHour` value is equal to `ExcludedStartHour`, this means that there is no excluded hour, thus, the Folder Sync runs 24/7.

8.9.3.2. Adjust EWS Throttling Policy

Folder Sync uses Exchange Web Services and may reach the threshold defined in your EWS throttling policy, especially if other software is simultaneously using EWS. The number of items returned per EWS call can be adjusted if needed, however, it is already set to a relatively low number by default.

Call Support for more information.

8.9.4. Folder Sync Readiness Checks

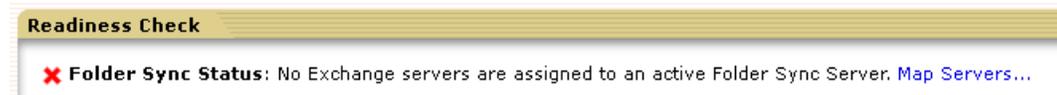
The following readiness checks have apply to the Folder Sync feature.

Folder Sync Status: No Active Folder Sync Servers Registered.



To resolve this readiness check, ensure a Folder Sync enabled client has been installed after Support has enabled the feature and all prerequisites are completed. See ["Folder Sync Prerequisites" on page 77](#).

Folder Sync Status: No Exchange servers are assigned to an active Folder Sync Server.



To resolve this readiness check, click the **Map Servers...** link and follow the procedure in [Task 8.21. "Assign Exchange Servers to Folder Sync Servers" on page 291](#)

Folder Sync Status: There are no users enabled for Folder Sync.



To resolve this readiness check, follow the procedure in [Task 8.23. "Enable users for Folder Sync" on page 292](#)

8.10. View Historical Mail Audit Reports

The service provides an audit trail of actions taken within the system. Audit reports are accessible by administrators, super administrators, and the EMS Root Account. Help desk users, reviewers, and regular system users cannot access audit reports.

Historical Mail maintains an audit trail for events that:

- Search the organization's email archive. See ["Archive Searches History Reports" on page 296](#).
- Create, delete or download archives. See ["Archive Activity History Reports" on page 298](#).
- Manually delete recovery archives. See ["Recovery Archives History Reports" on page 299](#).
- Create, delete, or change retention policies. See ["Retention Policies History Reports" on page 300](#).
- Create or update a reviewer group. See ["Reviewer Groups History Reports" on page 301](#).
- Archive messages based on User Classification policies. See ["User Classification History Reports" on page 303](#). This report is available only if your organization uses the optional User Classification feature.

8.10.1. Archive Searches History Reports

The Archive Searches History 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 8-5 Archive Searches History Report Fields

| Column | Description | Values |
|--------|--|--|
| Event | The activity involved | <ul style="list-style-type: none"> • For example, a Reviewer searches the company email archive. • A recovery archive is generated. • System users forward archived messages to themselves. |
| Actor | Name and email address of the Reviewer who initiated the event | |

Table 8-5 Archive Searches History Report Fields

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

The Archive Searches History Report shows all available historical data collected for your organization.

Task 8.25. View an Archive Searches History Report:

- 1) From the EMS Admin Console navigation menu, click **Audit Reports**.
- 2) Under the **Historical Mail** section, click **Archive Searches**. The **Archive Searches History Report** page appears.
- 3) You can narrow the report to include only events logged for specific users by entering the user name or email address in the search field and clicking **Search**. The filtered list of events appears.

You can use `%` as a wildcard for any search. To search for events logged by EMS Support users, enter `eparoot` in the search box.

- 4) To export all logged events to a CSV file, click **Export**. A **File Download** dialog box appears.

NOTE All Logged Events Are Exported

When you export an audit report to CSV, all logged events are exported. The export file does not limit events based on any filter or search you may have applied to the displayed report.

- 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. You can provide a custom name for the file, but do not change the file suffix or file type.
- d. Click **Save**.

8.10.2. Archive Activity History Reports

The Archive Activity History Report reports all archive audited events, such as creation or download of an archive. It includes the following data:

Table 8-6 Recovery Archives History Reports Fields

| Column | Description | Values |
|----------------|--|--|
| Event | Action taken | <ul style="list-style-type: none"> A recovery archive was created. A user archive was downloaded. |
| Actor | Name and email address of the person responsible for 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 | |

Task 8.26. View a Archive Activity History Report:

- 1) From the EMS Admin Console navigation menu, click **Audit Reports**.
- 2) Under the **Historical Mail** section, click **Archive Activity**. The **Archive Activity History Report** page appears.
- 3) You can narrow the report to include only events logged for specific users by entering the user name or email address in the search field and clicking **Search**. The filtered list of events appears.

You can use % as a wildcard for any search. To search for events logged by EMS Support users, enter `eparoot` in the search box.

- 4) To export all logged events to a CSV file, click **Export**. A **File Download** dialog box appears.

NOTE All Logged Events Are Exported

When you export an audit report to CSV, all logged events are exported. The export file does not limit events based on any filter or search you may have applied to the displayed report.

- 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. You can provide a custom name for the file, but do not change the file suffix or file type.
- d. Click **Save**.

8.10.3. Recovery Archives History Reports

The Recovery Archives History Report reports a recovery archive is manually deleted using the **Remove** option on the **Historical Mail > Email Recovery** page. It includes the following data:

Table 8-7 Recovery Archives History Reports Fields

| Column | Description | Values |
|----------------|--|--|
| Event | Action taken | <ul style="list-style-type: none"> A recovery archive was deleted. |
| Actor | Name and email address of the person responsible for 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 | |

The Recovery Archives History Report can only show data collected since the deployment of EMS data center version 6.6. Data from earlier EMS versions is not available.

Task 8.27. View a Recovery Archives History Report:

- 1) From the EMS Admin Console navigation menu, click **Audit Reports**.
- 2) Under the **Historical Mail** section, click **Recovery Archives**. The **Recovery Archives History Report** page appears.
- 3) You can narrow the report to include only events logged for specific users by entering the user name or email address in the search field and clicking **Search**. The filtered list of events appears.

You can use % as a wildcard for any search. To search for events logged by EMS Support users, enter `eparoot` in the search box.

- 4) To export all logged events to a CSV file, click **Export**. A **File Download** dialog box appears.

NOTE All Logged Events Are Exported

When you export an audit report to CSV, all logged events are exported. The export file does not limit events based on any filter or search you may have applied to the displayed report.

- 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. You can provide a custom name for the file, but do not change the file suffix or file type.
- d. Click **Save**.

8.10.4. Retention Policies History Reports

The Retention Policies History Report lists changes to retention policies, including the following data:

Table 8-8 Retention Policies History Reports Fields

| Column | Description | Values |
|----------------|--|---|
| Event | Action taken | <ul style="list-style-type: none"> • For example, a retention policy is created, deleted, renamed, or assigned a new priority. • Retention mode, retention period, or VaultBox settings are changed for a retention policy. • Users are added to or removed from a retention policy. |
| Actor | Name and email address of the person responsible for 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 | <ul style="list-style-type: none"> • If the audited event is initiated by a user, this field will contain the IP address of the user. • If the audited event is initiated by the EMS system itself, for situation such as Retention Holds being automatically updated, this field will contain "IP not Logged". |

Retention Policies History Reports show all available historical data collected for your organization.

Task 8.28. View a Retention Policies History Report:

- 1) From the EMS Admin Console navigation menu, click **Audit Reports**.
- 2) Under the **Historical Mail** section, click **Retention Policies**. The **Retention Policies History Report** page appears.
- 3) You can narrow the report to include only events logged for specific users by entering the user name or email address in the search field and clicking **Search**. The filtered list of events appears.

You can use % as a wildcard for any search. To search for events logged by EMS Support users, enter `eparoot` in the search box.

- 4) To export all logged events to a CSV file, click **Export**. A **File Download** dialog box appears.

NOTE All Logged Events Are Exported

When you export an audit report to CSV, all logged events are exported. The export file does not limit events based on any filter or search you may have applied to the displayed report.

- 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. You can provide a custom name for the file, but do not change the file suffix or file type.
- d. Click **Save**.

8.10.5. Reviewer Groups History Reports

The Reviewer Groups History Report lists changes to Reviewer Groups, including the following data:

Table 8-9 Reviewer Groups History Reports Fields

| Column | Description | Values |
|--------|--|---|
| Event | Action taken | <ul style="list-style-type: none"> • For example, that a reviewer group was created or deleted. • A reviewer was added to or deleted from a reviewer group. |
| Actor | Name and email address of the person responsible for the event | |

Table 8-9 Reviewer Groups History 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 | |

Reviewer Groups History Reports show all available historical data collected for your organization.

Task 8.29. View a Reviewer Groups History Report:

- 1) From the EMS Admin Console navigation menu, click **Audit Reports**.
- 2) Under the **Historical Mail** section, click **Reviewer Groups**. The **Reviewer Groups History Report** page appears.
- 3) You can narrow the report to include only events logged for specific users by entering the user name or email address in the search field and clicking **Search**. The filtered list of events appears.

You can use % as a wildcard for any search. To search for events logged by EMS Support users, enter `eparoot` in the search box.

- 4) To export all logged events to a CSV file, click **Export**. A **File Download** dialog box appears.

NOTE All Logged Events Are Exported

When you export an audit report to CSV, all logged events are exported. The export file does not limit events based on any filter or search you may have applied to the displayed report.

- 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. You can provide a custom name for the file, but do not change the file suffix or file type.
- d. Click **Save**.

8.10.6. User Classification History Reports

User Classification History Reports display lists of messages that were flagged during the processing of User Classification Retention Policies. These reports are available only for organizations using the optional User Classification feature. Columns in the report include the following:

Table 8-10 User Classification History Reports Fields

| Column | Description |
|------------|---|
| Subject | The subject of a message archived under a User Classification policy |
| SMTP ID | The SMTP ID of the message archived under a User Classification policy |
| Policy | The User Classification policy under which this message was archived |
| Actor | The user who copied the message into the designated user classification folder, thus archiving the message under the User Classification Policy |
| Audit Date | The date and time when the message was archived |

NOTE Changes to User Classification Policies Are Captured in the Retention Policies History Report

The User Classification History Report shows an audit trail of messages archived based on User Classification policies. Changes to User Classification policies themselves are reported in the Retention Policies History Report.

User Classification History Reports show all available historical data collected for your organization.

Task 8.30. View a User Classification Report:

- 1) From the EMS Admin Console navigation menu, click **Audit Reports**.
- 2) Under the **Historical Mail** section, click **User Classification**. The **User Classification History Report** page appears.
- 3) 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.
- 4) To search for classified messages by specific criteria, click a radio button to choose the type of search:
 - By Actor Email
 - By Actor Name
 - By Policy
 - By SMTP ID

- By Subject

You can narrow the report to include only events logged for specific users by entering the user name or email address in the search field. You can use % as a wildcard for any search.

- 5) Click **Search**. The report of user classification events appears.
- 6) To export all logged events to a CSV file, click **Export**. A **File Download** dialog box appears.

NOTE All Logged Events Are Exported

When you export an audit report to CSV, all logged events are exported. The export file does not limit events based on any filter or search you may have applied to the displayed report.

- 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. You can provide a custom name for the file, but do not change the file suffix or file type.
- d. Click **Save**.

9. EMS Cloud Services

This chapter covers the following topics relevant to administering EMS Cloud Services features.

- ["About EMS Cloud Services" on page 305](#)
- ["Microsoft Office 365 Prerequisites" on page 312](#)
- ["Microsoft Office 365 Installation" on page 313](#)
- ["Microsoft Office 365 Administration" on page 316](#)

9.1. About EMS Cloud Services

Cloud Services is an optional EMS Email Archive function that provides support for external "Cloud-based" email platforms. EMS Cloud Services currently supports:

- Microsoft Office 365 hybrid environments

Cloud Services is not enabled by default. To enable, please contact Support.

9.1.1. New Terms and Concepts

On-premises Users: Users whose mailboxes reside in the on-premises Exchange environment.

Cloud Users: Users whose mailboxes reside in the cloud, such as Microsoft Office 365 users.

Hybrid environment: A Microsoft-specific term defined in <http://help.outlook.com/en-us/140/ff633682.aspx>.

Exchange envelope journaling: A Microsoft-specific term defined in <http://technet.microsoft.com/en-us/library/aa998649>.

9.1.2. Special Considerations for Office 365 Hybrid Environments

Because Office 365 is a multi-tenant hosted Exchange environment, there are differences and limitations to the functionality available to EMS customers as compared to an on-premises only environment. The component differences are described below.

- ["Email Continuity" on page 306](#)
- ["SyncManager" on page 306](#)
- ["RecoveryManager" on page 307](#)
- ["Storage Management" on page 307](#)
- ["Outlook Extension" on page 307](#)
- ["Harvester" on page 308](#)
- ["Import Manager" on page 308](#)
- ["PrepareOutlookAuth" on page 308](#)

9.1.2.1. Email Continuity

Email Continuity is *not* supported for cloud mailboxes.

In the event of a partial activation, only on-premises mailboxes can be activated. In the event of a full activation cloud mailboxes are automatically excluded from the activation list.

Depending on the nature and scope of the outage as well as the mail routing configuration in use in your environment, there may be limitations to activation scenarios that are not present in a standard on-premises deployment.

For example, if the on-premises SMTP gateway and connector to Office 365 is offline as part of a partial activation, on-premises mail sent by non-active users may still be able to route to the EMS datacenter for active EMS users, but mail dependent on the inbound gateway from Office 365 cannot dynamically be routed in the Office 365 system for the active users.

In the event of a full activation, if unresolved mail is configured to be forwarded from EMS to Office 365, then Office 365 cannot also be configured to forward unresolved mail to EMS, otherwise mail for public folders and other objects without a mailbox may be looped.

It is highly recommended that, during an outage window, activation scenarios be tested to determine if the configuration of mail routing and connectors can support the intended activation scenarios. This testing may require the stopping of the hub transport server acting as the connector between the on-premises organization as well as testing MX record failover, depending on the environment.

Because Historical Mail, the thirty-day rolling email history archive, is a function of EMS Email Continuity, Historical Mail does not support Office 365 mailboxes.

9.1.2.2. SyncManager

Directory: Synchronization of Office 365 users as directory objects is not supported with SyncManager versions prior to EMS Client 6.5.

- For customers who have Office 365 users but are not enabling Office 365 users for archive within EMS, the Office 365 mailboxes are synchronized as non-mailbox objects.
- If support is enabled for archiving of Office 365 mailboxes, the users will be synchronized as cloud mailboxes.
- If support for Office 365 is enabled after SyncManager 6.5 is already installed, to take advantage of the new capabilities, stop and restart the SyncManager service, then open the SyncManager and perform a manual directory sync.

Contact & Calendar: Synchronization of Contact and Calendar items is not supported for Office 365 mailboxes. Contact & Calendar synchronization is an EMS Email Continuity feature and applies only to on-premises users.

9.1.2.3. RecoveryManager

Recovery of continuity, time-based and discovery archives using EMS RecoveryManager do not support an Office 365 mailbox as the target mailbox.

These archive types can be imported into an on-premises mailbox and subsequently exported/imported into an Office 365 mailbox using Outlook or another 3rd-party tool.

9.1.2.4. Storage Management

Storage Management is not supported for Office 365 mailboxes.

New messages will not be stubbed, existing stubbed messages which are deleted and otherwise eligible for purge will not be removed, and messages cannot be unstubbed in bulk using the `unstub` utility. For usage see ["Unstub Command Line Tool" on page 269](#)

It is strongly recommended that prior to moving a mailbox to Office 365 the mailbox first be removed from a storage management policy and the `unstub.exe` utility be used to recover existing stubbed attachments back into the user's mailbox.

Once a mailbox has been moved to the cloud, use of the `unstub` command is not supported without first moving the mailbox back on-premises.

Mailboxes must be removed from a storage management policy in order to be unstubbed. If a user is still a member of a storage management policy, the `unstub` utility will skip the user and not unstub their messages.

9.1.2.5. Outlook Extension

Outlook Extension's Storage Management operations (`Keep Attachments with Messages` and `Move Attachments to EMS Archive`) are not supported for cloud mailboxes.

Messages marked to be stubbed (`Move Attachments to EMS Archive`) will not be stubbed by the EMS Harvester Service, even if the user is a member of a storage management policy.

Messages which are already stubbed may be accessible via the Outlook Extension but access is not a supported function.

Configuration of the Outlook Extension for cloud mailboxes using `PrepareOutlookAuth` is not supported. See ["PrepareOutlookAuth" on page 308](#) for additional details.

9.1.2.6. Harvester

Bulk import of messages using the Harvester Service is not supported for Office 365 mailboxes, nor is stubbing of messages for cloud users which are members of a storage management policy.

9.1.2.7. Import Manager

Import of historical mail from cloud mailboxes or cloud Exchange archives is not currently supported. Import from PST file into the EMS Email Archive is supported for historical import with users whose mailboxes are located in Office 365.

9.1.2.8. PrepareOutlookAuth

`PrepareOutlookAuth` is only supported when run against on-premises mailboxes.

If new cloud mailboxes require an Outlook Authentication token:

- 1) Create a new on-premises mailbox.
- 2) Run `PrepareOutlookAuth` to set the Outlook Authentication token.
- 3) Move the mailbox to the cloud.

For cloud mailboxes without a token, users will need to enable the EMS Outlook Extension manually using their EMS username and password.

9.1.2.9. EMS Email Archive

User classification policies are not supported for Office 365 mailboxes.

If this Readiness check is displayed, verify your Office 365 environment is set to send secure messages. Contact Support if further assistance is required.

9.1.3.3. Cloud Services Window

The Cloud Services window manages the journaling addresses to which all copies of journaling mail are sent.



A journaling address is a Globally Unique Identifier (GUID). Cloud user's journaling addresses tie to an EMS Data Center.

New journaling addresses can be created by clicking on **Add Office 365 Journaling Address** link. Existing journaling addresses are removed by clicking on the **Delete** link to the right of the address.

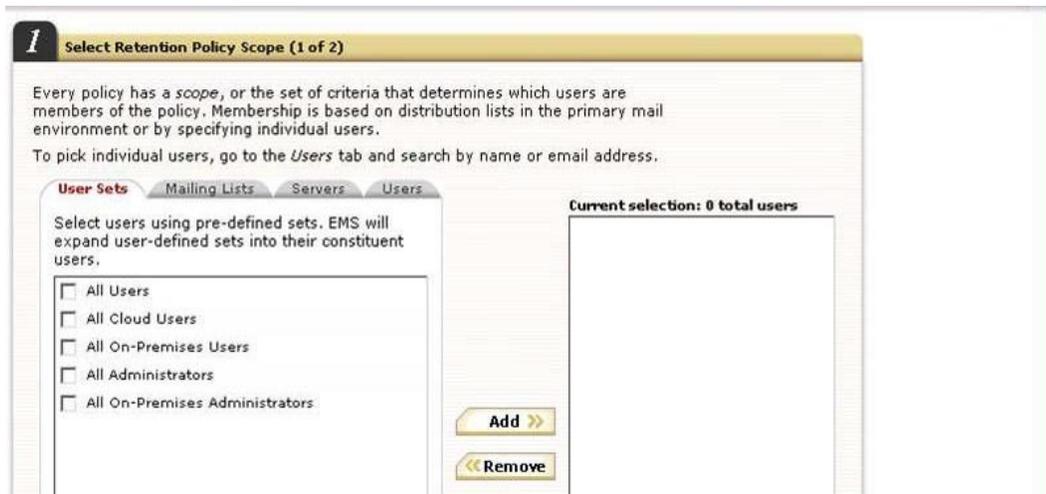
NOTE Do Not Delete Journaling Address Before In-Process Tasks Complete

If you wish to retire an existing journaling address and use a new one, it is recommended you put the new address in place and allow sufficient time for existing messages which may be currently in-process to be archived/imported before retiring an existing address in use.

9.1.3.4. Retention Policy Window

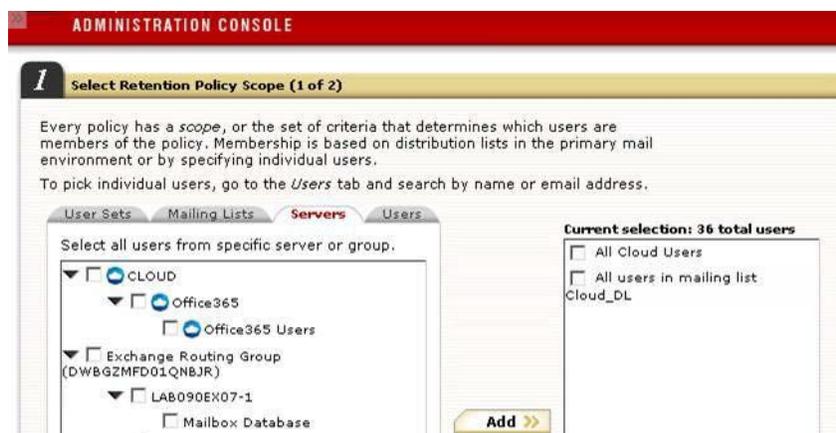
User Sets Tab

Two new groups have been created under **User Sets: All Cloud Users** and **All On-Premises Users**.



Servers Tab

We have added a new topology for Cloud users under **Servers** tab. All Cloud user checkboxes function the same, regardless of the level you choose.



Users Tab

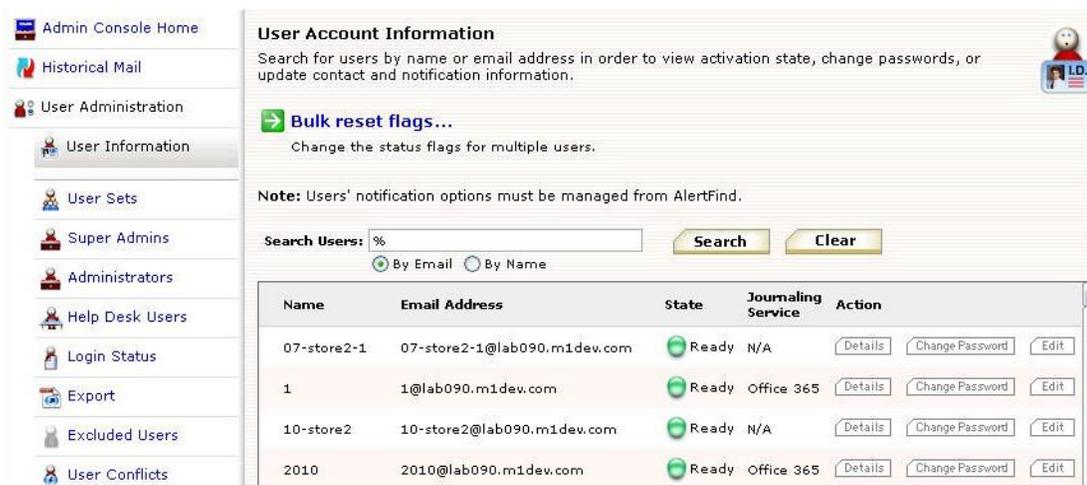
Under the Users tab, individual Office 365 users are distinguished with the cloud, ☁, icon.



9.1.3.5. User Information Window

To check the status of a user, **User Administration > User Information** contains a **Journaling Service** column which displays each users' journaling type:

- N/A: Non-journaled on-premises Exchange user
- Office 365: Office 365 journaling service user



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

Bulk reset flags...
Change the status flags for multiple users.

Note: Users' notification options must be managed from AlertFind.

Search Users: %

By Email By Name

| Name | Email Address | State | Journaling Service | Action |
|-------------|------------------------------|-------|--------------------|---|
| 07-store2-1 | 07-store2-1@lab090.m1dev.com | Ready | N/A | <input type="button" value="Details"/> <input type="button" value="Change Password"/> <input type="button" value="Edit"/> |
| 1 | 1@lab090.m1dev.com | Ready | Office 365 | <input type="button" value="Details"/> <input type="button" value="Change Password"/> <input type="button" value="Edit"/> |
| 10-store2 | 10-store2@lab090.m1dev.com | Ready | N/A | <input type="button" value="Details"/> <input type="button" value="Change Password"/> <input type="button" value="Edit"/> |
| 2010 | 2010@lab090.m1dev.com | Ready | Office 365 | <input type="button" value="Details"/> <input type="button" value="Change Password"/> <input type="button" value="Edit"/> |

9.2. Microsoft Office 365 Prerequisites

9.2.1. Requirements

9.2.1.1. Planning

As you plan your migration, we strongly recommend you contact Support so that a deployment engineer can review your migration plans and discuss best practices as it relates to your users and the EMS system.

9.2.1.2. Microsoft Office 365 Requirements

Office 365 support requires hybrid mode and the Microsoft directory synchronization tool.

Cloud managed Office 365 instances are not supported.

Exchange Journaling for Office 365: You must use an Office 365 plan which supports Exchange journaling.

9.2.1.3. EMS Client Version

Activation of Cloud Services features requires use of EMS Client 6.5 or later.

Contact Support for assistance in downloading the most current version of the EMS Client software.

9.2.1.4. EMS Data Center Configuration

Support must be contacted to activate "Cloud Support" for your environment.

9.3. Microsoft Office 365 Installation

9.3.1. Configuring Journaling for Office 365 Users

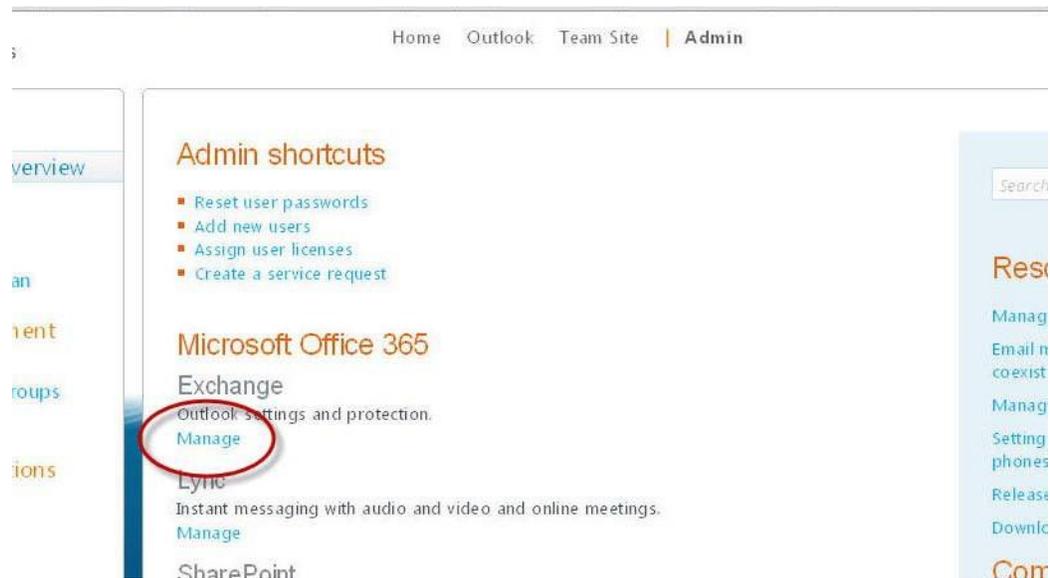
Task 9.1. Configuring Journaling for Office 365 Users

- 1) Log onto the EMS Administration Console.
- 2) In **Cloud Services**, highlight then copy the Office 365 journaling address.

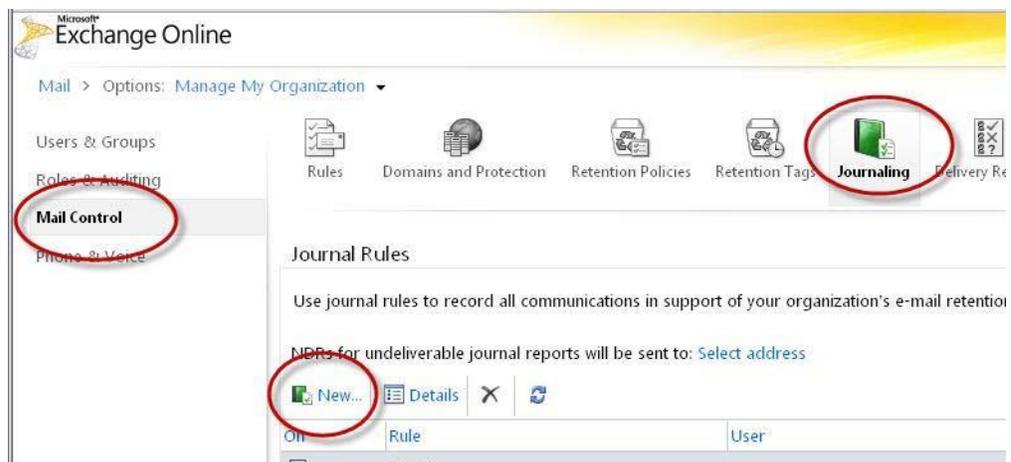


- 3) In **User Administration**, create a test user or a test distribution list.
- 4) In **Historical Mail > Retention Policies**, create a retention policy and add the test user or test distribution list to the policy.
- 5) Log into the Microsoft Office 365 Administration console.

- 6) In the Microsoft Office 365 Admin console, click **Manage**, under the Exchange heading.



- 7) In the **Manage My Organization** window, click **Mail Control** in the left menu.



- 8) Then click on the **Journaling** tab, and in the **Journal Rules** section, click on **New...** to create a new journal rule.

9) To configure the journaling rule..

- a. **If the message is sent to or from...:** This drop-down's options are: [Apply to all messages] and A specific user....

For a testing session, select `A specific user...`, which brings up a selection window. Select the test email address or the distribution list created in [step 3 on page 313](#).

After testing is completed:

- If you all your Office 365 users participate in EMS Email Archive, select [Apply to all messages], to ensure all messages sent and received are journaled.
- If you are journaling for a subset of users, select `A specific user...` and specify the distribution list which contains the users you wish to journal. This same distribution list should be used in the archive retention policy for Email Archive.

- b. **Journal the following messages...:** Select `All messages`.

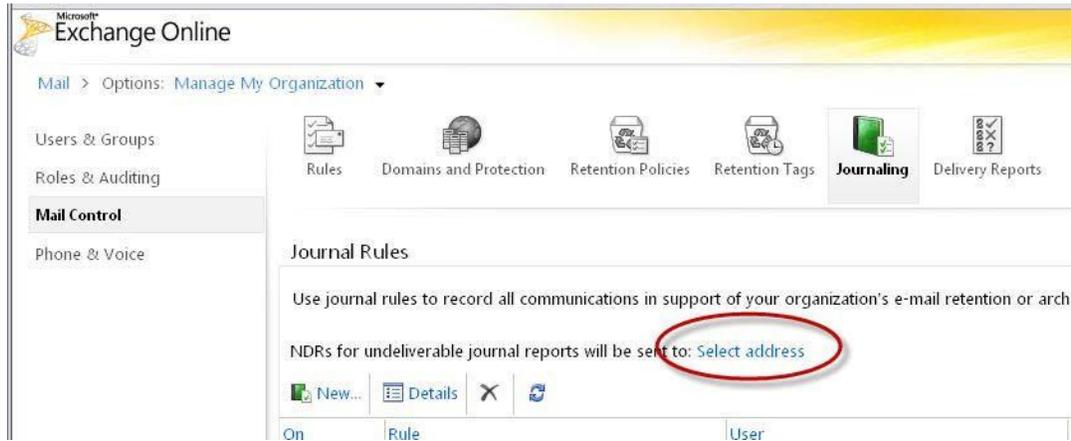
- c. **Send journal reports to::** This indicates where Office 365 is to send the messages. Paste the Office 365 Journaling Address that was copied in [step 2 on page 313](#).

Yes, the field is small, but it will hold the whole Journaling Address GUID. To verify the pasted GUID, check the beginning few characters, then hit END key, and check the ending few characters. Do not try to type the whole GUID into this field, as typing is too error-prone.

- d. **Name of rule::** Name the rule something descriptive, such as `Office 365 Test Journaling Rule`. Or if you have several rules, ensure their names clearly indicate the rule's boundaries.

10) Click **Save** to save the rule.

- 11) If you haven't already done so, specify an email address for journaling reports to be sent to.



Beside **NDRs for undeliverable journal reports will be sent to:**, Click on **Select address** and select an email address to receive the administrative reports.

All messages sent and received by the test user or members of the test distribution list will now be journal to EMS. Send test messages and verify via Exchange message tracking and/or the EMS Email Archive that messages are successfully processed.

9.4. Microsoft Office 365 Administration

9.4.1. Unstubbing Office 365 Users

For Office 365 Email Archive customers, users must be removed from a storage management policy and their mail unstubbed **prior** to moving the mailbox to Office 365.

After removing a user from a storage management policy, email messages which had previously been stubbed are *not* automatically unstubbed. To unstub a message use the `unstub` command line tool available on the EMS VaultBox. ["Unstub Command Line Tool" on page 269.](#)

NOTE “unstub -all” Will NOT Unstub Migrated Users

If you choose the `-all` option to unstub all users, the `unstub` tool will execute for only the on-premises users who are *not* members of a storage management policy.

- Cloud users will *not* be processed.
- Users who are members of a storage management policy will also *not* be processed.

If you attempt to unstub a cloud user by specifying their primary SMTP address, you will receive an error stating the tool is unable to find the user with that SMTP email address. In verbose logging an exception is logged that the property `homeMDB` is not found. This is expected.

9.4.2. EMS Email Archive and Office 365 Users

Cloud users must be added to a retention policy in order to use EMS Email Archive.

A Capture Based Policy is the preferred retention policy, but a Membership Policy can be used as well.

User Classification Policies do *not* apply to Cloud users, because EMS cannot directly access Cloud users' mailboxes.

9.4.3. Office 365 Best Practices

9.4.3.1. Before Migrating EMS Users to the Cloud

- Remove users from storage management policies.
 - Once removed, run the `unstub` command on the users to return attachments to the email messages.
 - Removing large numbers of users from Storage Management is scriptable and automatable.

9.4.3.2. Migrating Users to the Cloud

- Begin the migration process by migrating only one test mailbox.
 - Get the test mailbox working before moving on to bigger groups of users.

- Ensure EMS Email Continuity is in the *Ready* state before migrating any users. Important status information may be compromised when migrating users during a partial or full activation.

9.4.3.3. Post-migration Administration

- Exclude cloud users from Storage Management policies.
- Ensure that retention policies and Office 365 journaling policies remain in sync.

10. EMS Expanded Archive Services

This chapter covers the following topics relevant to administering EMS Expanded Archive Services features.

- ["About Expanded Archive Services" on page 319](#)
- ["About EMS Microsoft Lync Archiving" on page 319](#)
- ["EMS Lync Archive Prerequisites & Limitations" on page 320](#)
- ["EMS Lync Archiving Installation" on page 326](#)
- ["EMS Lync Archiving Administration" on page 331](#)

10.1. About Expanded Archive Services

The Enterprise Archive feature set has been expanded to include optional functionality beyond the Email Archive ability to archive and search email messages.

The first new offering is **EMS Microsoft Lync Archiving** which provides support for archiving and searching of Microsoft Lync instant message conversations.

- EMS Microsoft Lync Archiving is not enabled by default. Contact your account representative to confirm eligibility for the EMS Microsoft Lync Archiving service.

10.2. About EMS Microsoft Lync Archiving

For customers who have subscribed to this service, EMS Archive now has the ability to archive Microsoft Lync instant message conversations, and Archive Reviewers may now search and export Lync instant message conversations. All EMS Archive email message search and archive functions have been adapted to the instant message format, including support for Reviewer Group scoping, creation of Discovery Archives and Retention Holds, and export into PST and EML files using Export Manager.

EMS Lync Archiving feature supports the following:

On-Premises Lync versions:

- Lync Server 2010
- Lync Server 2013

Lync conversations that are archived to:

- Lync on-premises SQL archiving database (Lync Server 2010 & 2013)

- Exchange 2013 (Lync Server 2013 only)

Lync conversation types:

- Peer to peer (P2P) (a chat session between two users)
- Conference (a chat session between more than two users)

Lync conversation chat types:

- Regular chat
- Chat with file transfer request/response
- White boarding session
- PowerPoint sharing

Distributed client Lync archiving:

- Provides a mechanism to exclude Lync SQL archiving database(s) from being archived on a per VaultBox basis.
- Provides a mechanism to exclude Exchange server(s) from being archived on a per VaultBox basis.

10.3. EMS Lync Archive Prerequisites & Limitations

10.3.1. Planning

An individual EMS VaultBox can export Lync conversations from only one version of Lync Server (2010 or 2013), not both versions.

If you have both Lync Server 2010 and 2013 in your environment, you will need at least two VaultBoxes - one that exports from Lync Server 2010 and another that exports from Lync Server 2013. Each VaultBox must have prerequisites installed that correspond to the Lync Server version that it will be exporting from.

Users who will have their Lync conversations archived is defined on the on-premises Lync Servers. The EMS Lync Archiving feature archives all conversations that it receives from the Lync SQL archiving database(s) and/or Exchange 2013 mail server(s). There is no way to select or un-select users for archiving within the EMS Lync Archiving system.

When planning the VaultBox set-up, take the following five Lync Server environment configurations into account:

- Lync Server 2010 only.
- Lync Server 2013 only.
- Combined Lync Server 2010 and 2013 environments.
- Multi-site environments that are connected.

- Multi-site environments that are disconnected.

In single-site configurations that use only Lync Server 2010, the Lync Servers may be used individually or in pools, and they may send their Lync Archive information to a single SQL archiving database or multiple databases. The SQL archiving database(s) are then accessed by a VaultBox that has the required prerequisites for Lync Server 2010 communications.

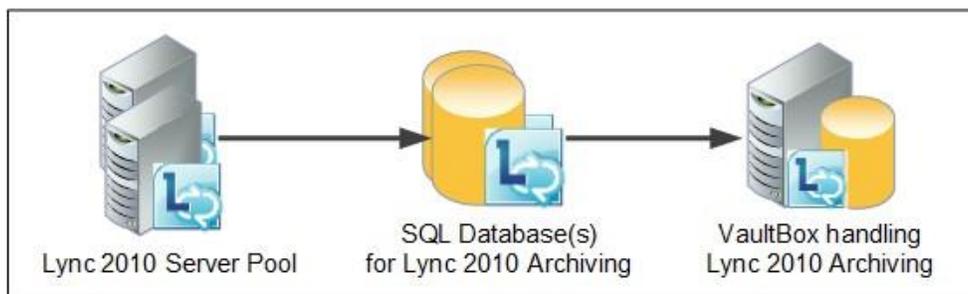


Figure 10-1 Lync Server 2010 Set-up

In single-site configurations that use only Lync Server 2013, the Lync Servers may be used individually or in pools. The Lync Servers archive Lync conversations to SQL archiving database(s) and/or Exchange 2013 mail server(s) configured for Lync Archiving. The SQL archiving database(s) and/or Exchange Server(s) are then accessed by a VaultBox that has been loaded with the prerequisites required for Lync Server 2013 communications.

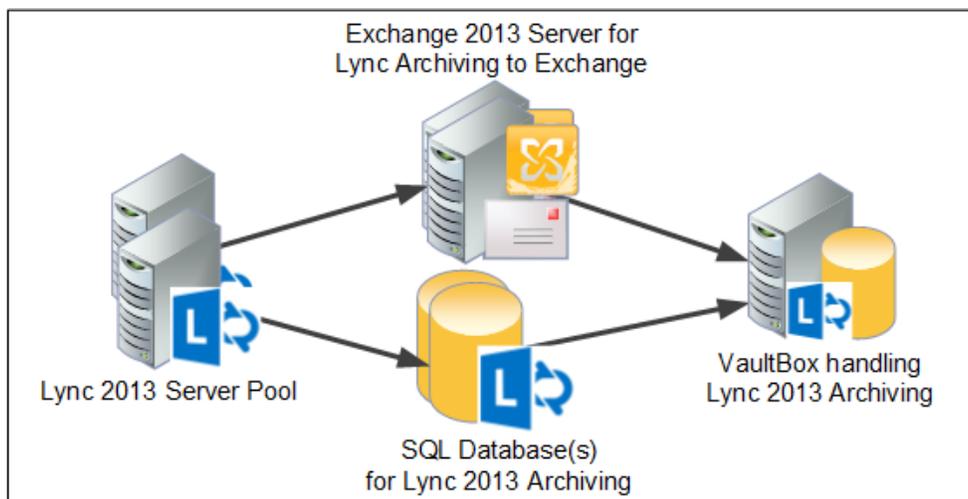


Figure 10-2 Lync Server 2013 Set-up

In combined Lync Server 2010 and 2013 configurations, the Lync Servers must access the VaultBox that has been loaded with the prerequisites required by the same Lync Server version.

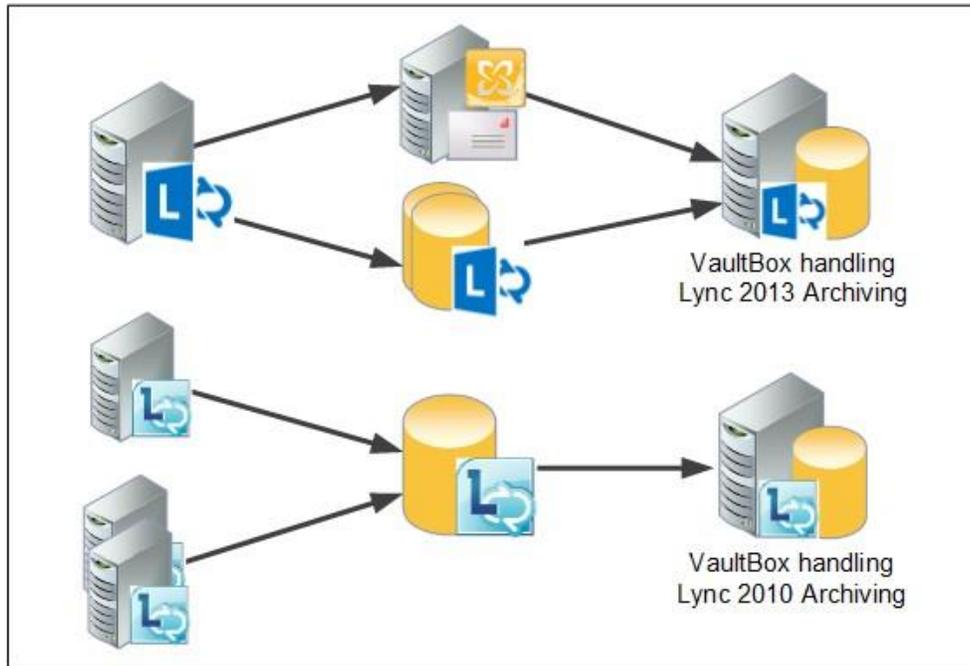


Figure 10-3 Combined Lync Server 2010 & 2013 Set-up

If your organization has different sites that share a network, there needs to be only one VaultBox per Lync Server version to handle all the Lync conversations.

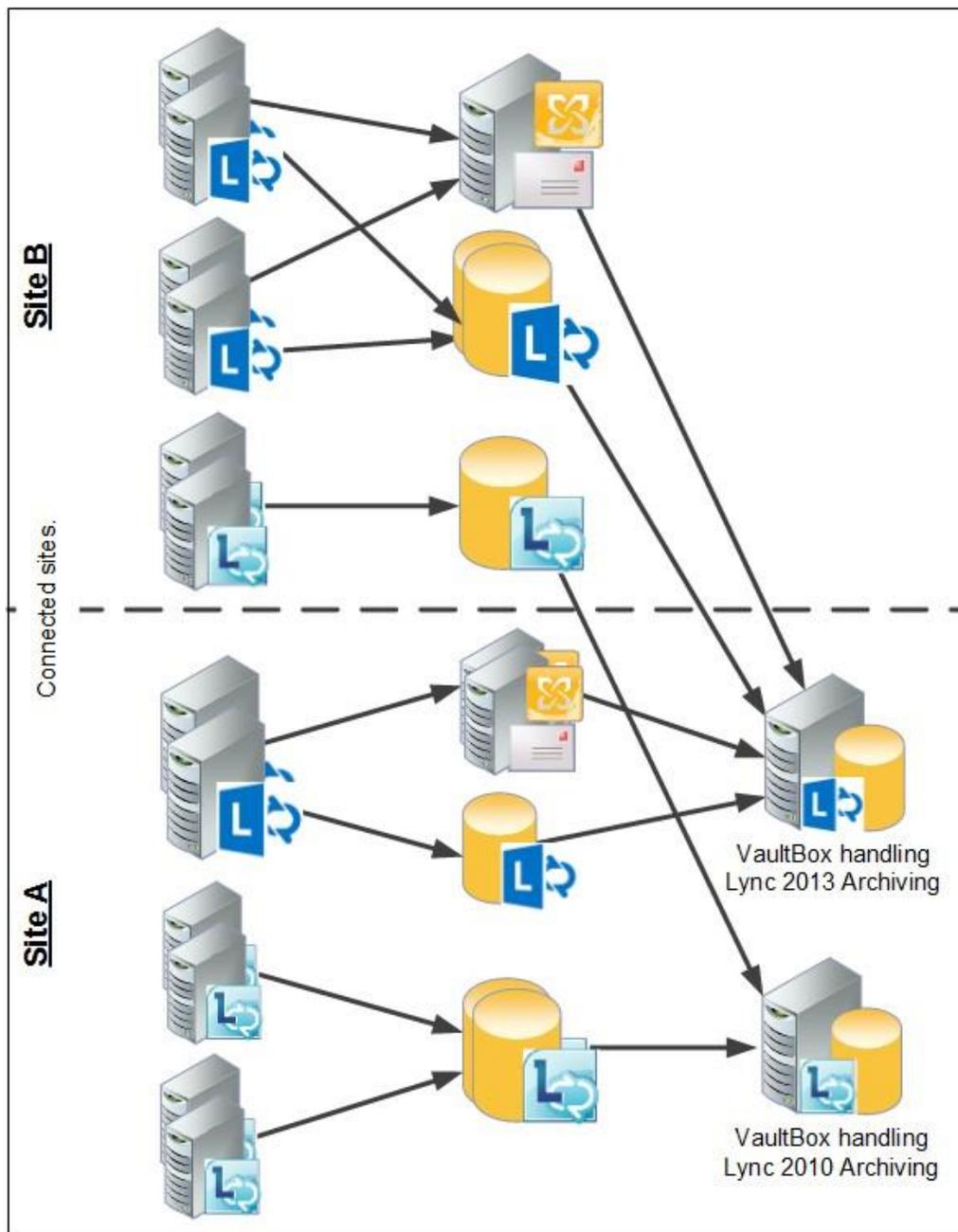


Figure 10-4 Lync 2010 & 2013 Multi-Site Connected Networks Set-up

If your organization has different sites that do not share a network or are separated by a significant distance, VaultBoxes can be installed at each site to archive each site's Lync conversations.

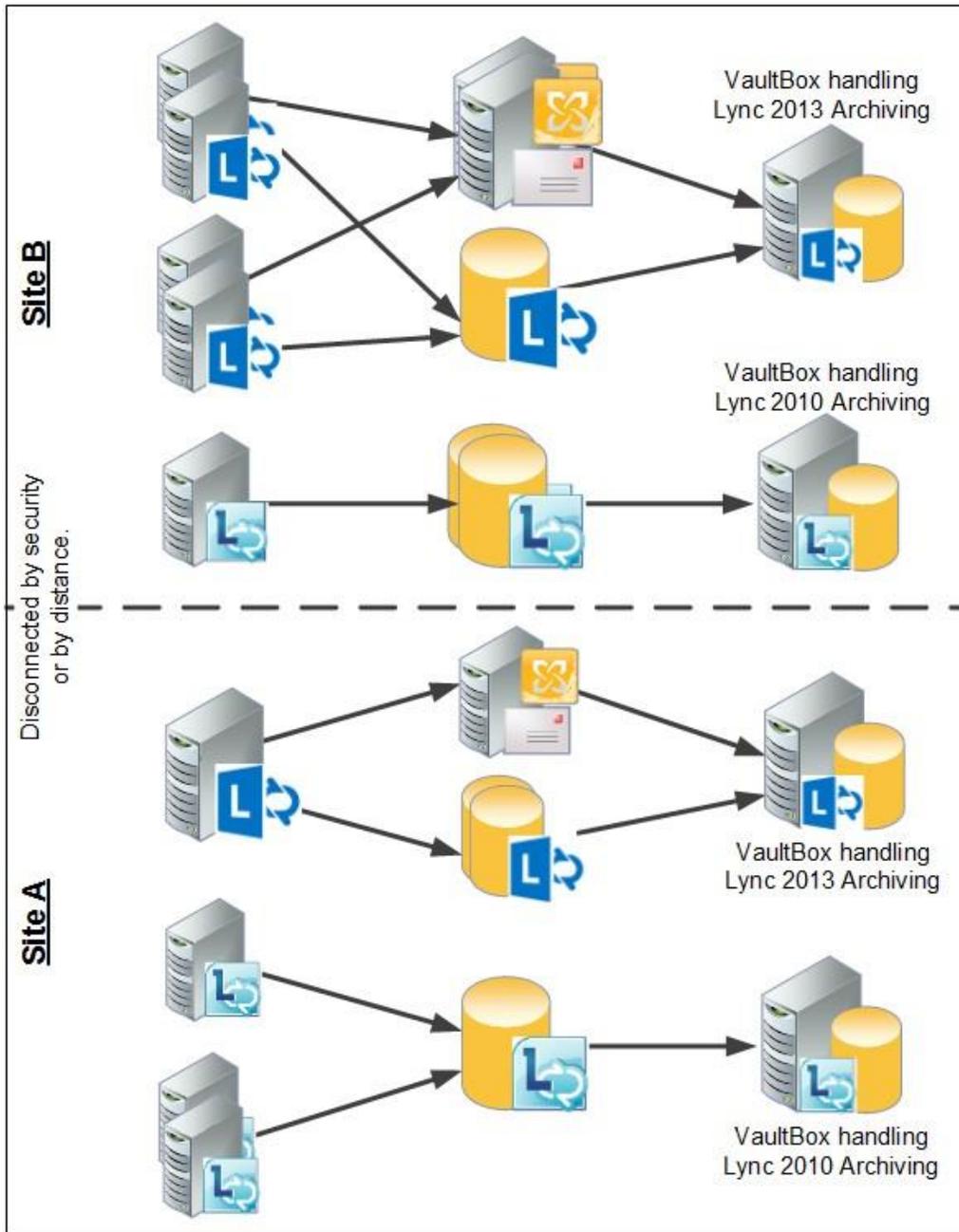


Figure 10-5 Lync 2010 & 2013 Multi-Site Disconnected Networks Set-up

10.3.2. Prerequisites

EMS Lync Archiving is not enabled by default. Contact your account representative to confirm eligibility for the EMS Lync Archiving service. Once eligibility is established, Support will activate EMS Lync Archiving for your environment.

Configuration of the EMS Lync Archiving feature requires use of EMS Client 6.12 (or later). If EMS Client 6.12 (or later) has already been installed on existing VaultBox(es) that will be synchronizing Lync conversations, the EMS Client software must be re-installed after EMS Lync Archiving is activated by Support, to ensure that the required services are installed.

10.3.2.1. VaultBox Prerequisites

If EMS Lync Archiving is being handled by a new VaultBox, make sure to install all normal VaultBox requirements before Lync-specific requirements are installed. See ["Stored/Archived Mail Prerequisites" on page 61](#)

Once the normal VaultBox prerequisites are installed, add the following required software, depending on the version of the Lync Server being served by the VaultBox.

Lync Server 2010 -- Lync Archiving Prerequisites on the VaultBox:

- PowerShell 3.0+
- Lync Server 2010 Admin Tools (primarily for Lync 2010 PowerShell module)

Lync Server 2013 -- Lync Archiving Prerequisites on the VaultBox:

- PowerShell 3.0+
- Lync Server 2013 Admin Tools (primarily for Lync 2013 PowerShell module)

10.3.2.2. Active Directory Service Account Prerequisites

In addition to the normal Active Directory Service Account settings (["Active Directory Service Account Requirements" on page 50](#)), the following are required to ensure that Lync conversations are archived correctly.

Lync Server 2010 and 2013: Required additional Active Directory memberships:

- A member of the Active Directory `RTCUniversalServerAdmins` security group
- A member of the Active Directory `RTCComponentUniversalServices` security group

NOTE: When making changes to Active Directory, the changes may not be immediately propagated.

Lync Server 2013 (Exchange 2013 only): In addition to the above permissions, if using Lync Server 2013 and archiving through Exchange 2013 mail servers:

- The EMS Active Directory Service Account must be configured for Exchange impersonation: [http://msdn.microsoft.com/en-us/library/bb204095\(v=EXCHG.140\).aspx](http://msdn.microsoft.com/en-us/library/bb204095(v=EXCHG.140).aspx)

10.3.3. Limitations

Following are the EMS Lync Archiving feature limitations:

- For EMS Lync Archiving, the SIP domain must match the email domain.

The following Lync features are not supported:

- Lync Online archiving.
- Persistent Chat for Lync 2013.
- Group Chat for Lync 2010.

The following Lync content types are not archived:

- Peer-to-peer file transfers
- Audio/video for peer-to-peer instant messages and conferences
- Desktop and application sharing for peer-to-peer instant messages and conferences

10.4. EMS Lync Archiving Installation

After the prerequisites have been met, the following steps are required to install EMS Lync Archiving:

- 1) Configure Microsoft Lync Server(s).
- 2) Install Client 6.12+ software on VaultBoxes.
- 3) Run Directory Sync between VaultBoxes and Exchange Server(s).
- 4) Enable and configure EMS Lync Archiving on VaultBox console(s).

10.4.1. Configure Lync Server Archiving

The EMS Client software uses Lync Server Archiving to export Lync conversations to the Data Center, therefore Lync Server Archiving must be configured in your environment per Microsoft's documentation.

For Lync Server 2010 Archiving configuration, refer to: <http://www.microsoft.com/en-us/download/details.aspx?id=4711>

For Lync Server 2013 Archiving configuration, refer to: <http://www.microsoft.com/en-us/download/details.aspx?id=36823>

When configuring your Lync Servers, take the following into account:

- EMS Client and Data Centers support different source formats depending on the Lync Server version:
 - **Lync Server 2010:** EMS supports only SQL archiving databases as the source.
 - **Lync Server 2013:** EMS supports both SQL archiving databases *and* Exchange 2013 as sources.
- Lync users who are enabled for archiving on the Lync Servers will be automatically detected by the EMS Client and the users' Lync conversations will be imported into the EMS Archive.

NOTE: Lync Servers can be configured after installing EMS Client software, but must be configured before enabling EMS Lync Archiving on the VaultBoxes.

10.4.2. Install Client Software

As a result of the differing requirements of Lync Server 2010 and 2013, if your organization has both versions of Lync Servers there will need to be at least one VaultBox for each version of Lync Server software.

Task 10.1. Install and configure EMS Client Software

- 1) Install EMS Client Software, version 6.12 or greater, on the computer that will become the VaultBox following the normal procedure: "[Task 5.1. Install service software:](#)" on page 80.
- 2) Configure the SyncManager following the normal procedure: "[Task 5.3. Configure the SyncManager:](#)" on page 83. Once the SyncManager is configured, an initial Directory Sync is automatically run. Ensure the Directory Sync completes successfully.
- 3) Configure the VaultBox that will be connecting to the Lync Server(s) following the normal procedure: "[Configure VaultBoxes](#)" on page 92.

10.4.3. Configure EMS Client for EMS Lync Archiving

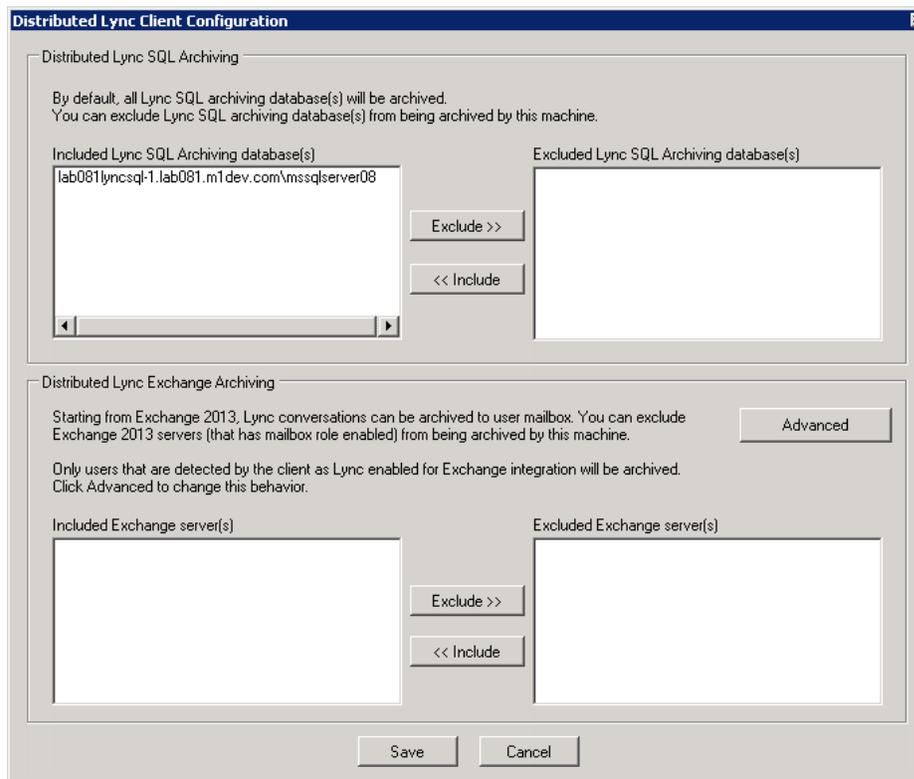
After the EMS Client software has been installed on the VaultBox machine, a Directory Sync successfully run, and the VaultBox is fully configured, it is time to configure the VaultBox for EMS Lync Archiving based on the plan established in "[Planning](#)" on [page 320](#).

Task 10.2. Configure EMS Client for EMS Lync Archiving

- 1) Once the VaultBox is configured (if necessary re-launch the VaultBox Console: **Start > Programs > MessageOne > VaultBox Console**), in the **Lync Archive** section of the **VaultBox Console** click the **Edit Settings** button.

The screenshot displays the VaultBox Console interface. At the top, the title bar reads "VaultBox Console". Below this, the "VaultBox Components" section explains that the VaultBox handles receiving, gathering, compressing, encrypting, and transferring mail data. Three task sections are visible: "Storage Management Task", "User Classification Retention Task", and "Lync Archive". Each task section includes a "Not yet started" status, a brief description, and "Start" and "Edit Settings ..." buttons. The "Lync Archive" section is highlighted with a red rounded rectangle and shows the status "Lync archive is currently disabled." with "Enable", "Edit Settings ...", and "Statistics" buttons. At the bottom, the "Transfer Service Status" section shows "No messages since 11/24/2014 2:56:08 PM" and displays metrics for Queue (0 msgs), Rate (0 msgs/sec, 0 KB/sec), and Free space (22,633.4 MB).

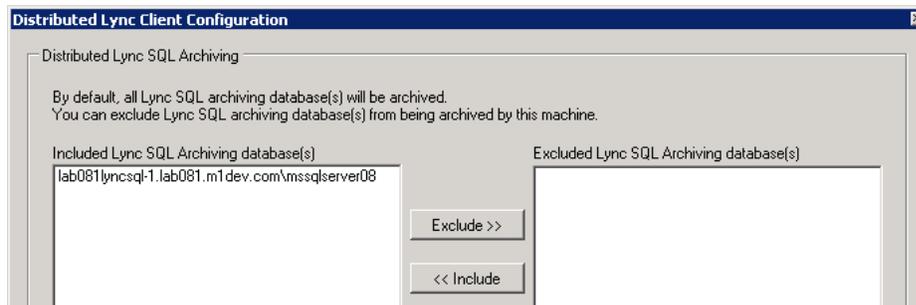
- 2) The **Distributed Lync Client Configuration** window, displays all the Lync SQL Archiving databases and/or Lync Archiving Exchange Servers that have been identified by the EMS system.



By default, for both Lync Server 2010 and 2013, the EMS Lync Archiving software on a VaultBox will archive conversations from *all* Lync SQL archiving databases. For Lync Server 2013, if archiving is being done through Exchange Servers, conversations from *all* Exchange Servers will be archived by the VaultBox.

There are times when certain Lync SQL archiving databases and/or Exchange servers need to be excluded from being archived by a certain VaultBox. For example, in [Figure 10-5 on page 324](#) when sites are disconnected or separated by distance, one VaultBox would be set to *Include* SQL archiving databases and/or Exchange servers that are close to that VaultBox's network or location, and all other SQL databases and/or Exchange servers would be *Excluded* from that VaultBox and *Included* on another VaultBox enabled for EMS Lync Archiving.

- 3) If applicable for your system configuration and plan, click the name of the Lync Server SQL archiving database in the left-hand column that needs to be *Excluded* from being archived using this VaultBox. Click the **Exclude** button, which moves the name of that Lync Server SQL archiving database to the Excluded column.



Repeat this until all SQL archiving databases that are to be excluded have been moved to the right-hand column.

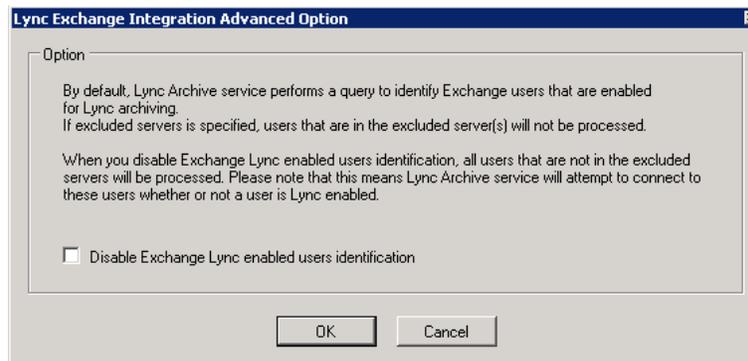
- 4) If applicable for your system configuration and plan, click the name of the Lync Archiving Exchange Server in the left-hand column that needs to be *Excluded* from being archived using this VaultBox. Click the **Exclude** button, which moves the name of that Exchange Server to the Excluded column.



Repeat this until all Exchange Servers that are to be excluded have been moved to the right-hand column.

The EMS system tries to detect which Exchange mailboxes have Lync Archiving enabled through the Exchange Server and archives Lync conversations only for those identified mailboxes. In some situations, this does not work as expected, so this setting can be over-riden and all Exchange 2013 mailboxes will have their Lync conversations archived.

To archive Lync conversations for all Exchange mailboxes, click the **Advanced** button in the **Distributed Lync Exchange Archiving** pane.



Check the box beside **Disable Exchange Lync enabled users identification** and click **OK**.

- 5) When all Lync SQL archiving databases and/or Exchange servers have been excluded according to the plan made in ["Planning" on page 320](#), click **Save**.

In the confirmation box, click **OK** to return to the **VaultBox Console**.

- 6) Enable EMS Lync Archiving by clicking the **Enable** button in the Lync Archive section.
- 7) A pop-up window appears for you to verify that a directory sync has been successfully completed and that any planned distributed Lync servers have been excluded from being synced with this VaultBox. Click **Yes**.

Lync conversations will begin to be transferred to the Data Center after the archive interval timer has expired. The default archive interval value is 5 hours.

10.5. EMS Lync Archiving Administration

10.5.1. EMS Lync Archiving Retention Policy

When EMS Lync Archiving is activated by Support, a Retention Policy of type `Instant Message`, with a policy name of `Global IM Capture Policy` and a default duration of `10 years` is created.

This Instant Message Retention Policy can be edited to change its name or the retention duration. But the policy cannot be deleted, nor can another Instant Message Retention Policy be added.

The Retention Policy's duration determines how far back into the Lync Server's archives the EMS system goes when Lync data is exported from the Lync Server to the Data Center.

If the duration is changed to a longer period, EMS Lync Archiving goes to the Lync Servers and gets the older conversations that were not archived in the shorter archive duration period. Lync conversations may be re-archived during this process, but the EMS system's message matching function should prevent duplicates from appearing in the archive.

If a shorter retention period is entered, the next time the EMS system's purge processes are run, the conversations older than the new retention period will be deleted from the Data Center. This purge process does not affect the Lync conversations stored on the Lync Servers.

Task 10.3. Edit EMS Lync Archiving Retention Policy

- 1) On the EMS administration console, click the **Historical Mail** button in the left-hand menu.

The **Retention Policies** page is brought up.

- 2) If necessary, scroll down the list of Retention Policies to locate the one policy with the **Type** of Instant Message.



| ID | NAME | TYPE | GLOBAL IM CAPTURE POLICY | RETENTION PERIOD (DAYS) | USERS |
|----|-----------------|--------------------------|--------------------------|-------------------------|----------|
| 35 | Instant Message | Global IM Capture Policy | | 3650days | Users: 0 |

- 3) Click the **Edit** button in the row of the Retention Policy's name.
- 4) If desired, enter a new name for the Instant Message Retention Policy into the **Name** field.
- 5) If desired, enter a new retention duration value into the **Retain mail for** field. This value is the number of days the EMS Lync Archiving conversations are to be retained on the EMS system before the conversations are purged.
- 6) Click **Submit** to save your changes.

10.5.2. Create EMS Lync Archiving Reviewer Groups

Lync conversations require their own type of Reviewer Group to limit the scope of the search. Email Reviewer Groups will not have access to instant message conversations, nor will Instant Message Reviewer Groups have access to email messages. Archive Reviewers can be assigned to both types of Reviewer Groups.

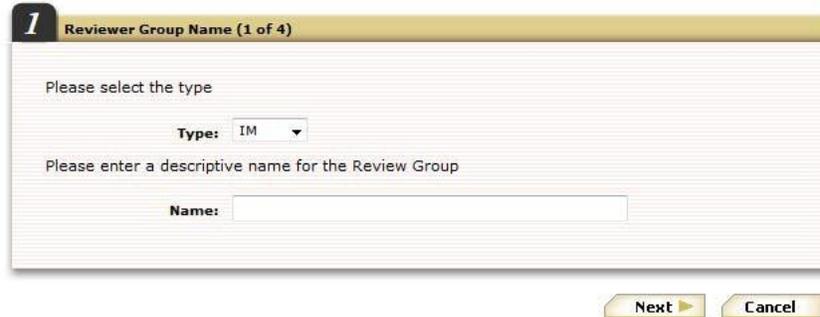
At least one Instant Message Reviewer Group must be created before Archive Reviewers can search Lync conversations. Administrators can create as many Reviewer Groups as needed for each organization's unique needs.

Task 10.4. Create EMS Lync Archiving Reviewer Group

- 1) On the EMS administration console, click the **Historical Mail** button in the left-hand menu, then click the **Reviewer Groups** button.

The **Reviewer Groups** page is brought up.

- 2) Click the **Create Reviewer Group** button at the bottom of the page.
- 3) In the **Type** drop-down, select **IM** to create an Instant Message Reviewer Group.



- 4) Enter a name for this new Reviewer Group.
Make this name descriptive so it is easy to determine exactly which subset of conversations and users are included in this Reviewer Group when it is viewed on Archive Reviewer pages.
- 5) Click the **Next** button.
- 6) In the same manner as used when creating Email Reviewer Groups, select the scope of this Reviewer Group. The scope of the Reviewer Group identifies the sub-set of instant message conversations the Archive Reviewer can access for their searches. You can define the scope by User Sets, Mailing Lists, Servers or individual Users. See. "[Task 8.7. Create a Reviewer Group:](#)" on page 247 for more information. When all are selected, click **Next**.
- 7) In the same manner as used when creating Email Reviewer Groups, select the Archive Reviewers who will have access to this Reviewer Group. You can define these users by Mailing Lists or individual Users. When all are selected, click **Next**.
- 8) The **Confirmation** page is shown. Ensure that all is correct. Click **Back** to correct any errors.
- 9) When completed, click **Submit** to save the new Reviewer Group.

Other EMS Lync Archiving Reviewer Group administration tasks are the same as email Reviewer Groups. See "[Reviewer Groups](#)" on page 247

10.5.3. Reviewer Created Lync Instant Message Retention Holds

Archive Reviewers can create Lync Instant Message Retention Holds that override the default Instant Message Retention Policy for the conversations contained in the Retention Hold. Conversations contained in the Hold will not be purged while the Hold is still in effect. Once the Retention Hold is deleted, all the conversations in the Hold return to the control of the Instant Message Retention Policy, and will be purged based on the duration of that policy.

Only users with Administrator, or greater, privileges can delete Retention Holds.

See ["Task 8.5. Delete a Retention Hold" on page 244](#) for the procedure to delete a Retention Hold.

10.5.4. Reviewer Created Lync Instant Message Discovery Archives

Archive Reviewers can create Lync Instant Message Discovery Archives that can be exported using Export Manager. Export Manager can export Instant Message Discovery Archives as PST or EML files.

Conversations contained in the Instant Message Discovery Archive are also exempt from the Instant Message Retention Policy and will not be purged while the Archive exists. Once the Instant Message Discovery Archive is deleted, all the conversations in the Archive return to the control of the Instant Message Retention Policy, and will be purged based on the duration of that policy.

Only users with Administrator, or greater, privileges can delete Instant Message Discovery Archives.

See ["Create and Recover Archives" on page 275](#) for the procedure to delete Discovery Archives.

10.5.5. EMS Lync Archiving Statistics

The EMS Client system provides Lync conversation processing statistics, available on the VaultBox Console. The statistics available are:

- **Total messages exported from Lync SQL:** Number of Lync conversations exported from the Lync Server SQL archiving database(s) since the time the `MessageOne Lync Archive Service` was started or restarted.

- **Total messages exported from Exchange user(s):** Number of Lync conversations exported from the Exchange user(s) since the time the MessageOne Lync Archive Service was started or restarted.
- **Transform rate for messages from Lync SQL:** Number of Lync conversations from the Lync Server SQL archiving database(s) transformed per second. This statistic is only calculated during active transforms, and is zero during times transforms are not being performed.
- **Transform rate for messages from Exchange users:** Number of Lync conversations from Exchange users transformed per second. This statistic is only calculated during active transforms, and is zero during times transforms are not being performed.

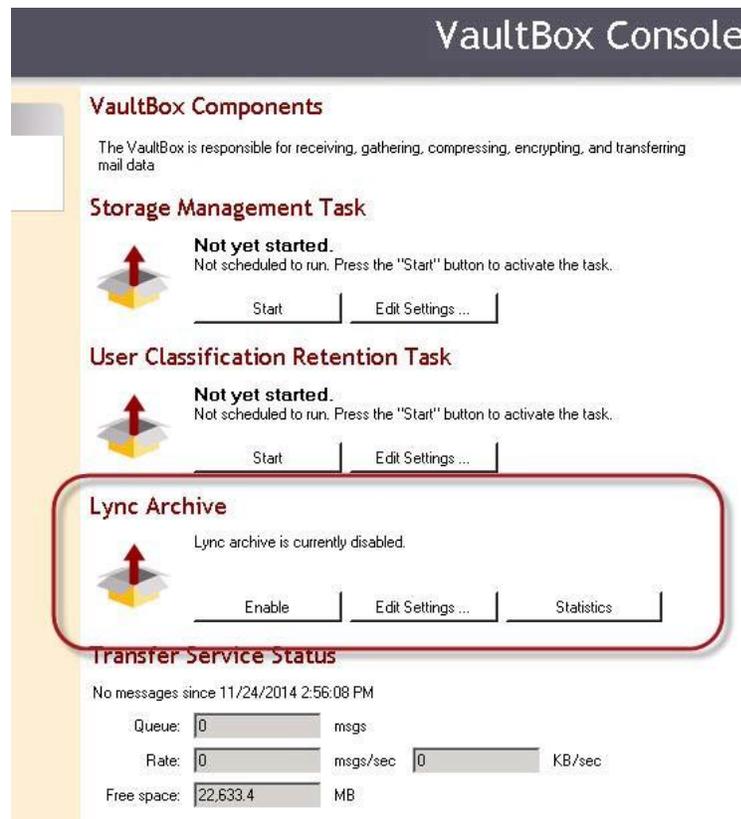
Restarting the services will reset the counters to zero.

NOTE: If you do not see any export activity-- for instance, there are no Lync conversations being exported for a period of time-- it could be due to the Lync `cmdlet` processing conference conversations. When an export begins, the Lync `cmdlet` exports peer-to-peer conversations first, then Lync conference conversations are exported. Sometimes there may appear to be some delay due to `cmdlet` processing before the Lync conference conversations begin being exported.

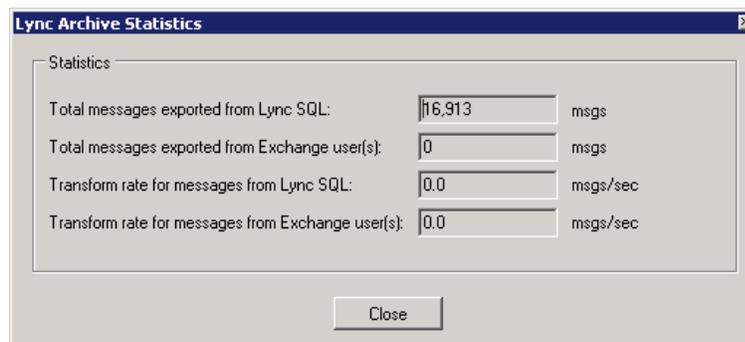
Task 10.5. View EMS Lync Archiving statistics

- 1) On the EMS Client VaultBox machine, open the VaultBox Console, **Start > Programs > MessageOne > VaultBox Console.**

- 2) In the **Lync Archive** section of the **VaultBox Console** click the **Statistics** button.



- 3) The **Lync Archive Statistics** window appears.



- 4) When done viewing the statistics, click the **Close** button.

10.5.6. EMS Lync Archiving Administration Advanced Topics

10.5.6.1. EMS Lync Archiving Log File

The MessageOne Transform windows service produces one log file:
TransformService.log.

MessageOne Lync Archive windows service produces three log files:

- `LyncArchiveService.log`: the main Lync archive windows service's log file
- `LyncArchiveServiceError.log`: this log file contains only the errors
- `LyncArchiveServiceSummary.log`: this log file contains the Lync archiving summary

10.5.6.2. EMS Lync Archiving Registry Values

When EMS Lync Archiving is first installed and activated, the EMS system will start exporting Lync conversations to the Data Center from oldest conversation to newest conversation. The parameters controlling this export are set to values estimated to be suitable for most organizations. However, there may be situations where the export variables need to be adjusted for optimum performance in a specific environment. Below are the values that can be adjusted. Call Support for more information.

Archive Range In Days: Lync conversations are, by default, exported in 5 day time slices. The next time slice will be processed during the next scheduled archiving run.

Archive Interval In Hours: Once the EMS system has completed the initial download of all Lync conversations archived on the Lync Servers, the default update interval for new incoming conversations is every 5 hours.

Trailing Export In Hours: Because Lync conversations may last for several hours, by default there is at least a 12 hour delay before new conversations are exported to the Data Center, to ensure that all conversations have completed and are archived in their entirety.

10.5.6.3. Disabling EMS Lync Archiving

To disable EMS Lync Archiving on the EMS System, contact Support to have the feature disabled. After that is completed, the EMS Client software must be re-installed on all the VaultBoxes that were handling EMS Lync Archiving conversations, to ensure the all settings are correctly set to disable the Lync archiving functionality.

10.5.6.4. Select New EMS Lync Archiving Working Directory

On the VaultBoxes that handle EMS Lync Archiving, the default working directory for the EMS Lync Archiving exporting functions is: `<CommonAppData folder>\MessageOne\LyncArchive`

If it is necessary to change this working directory, it can be done during the process of installing the Client software on the VaultBoxes by selecting a **Custom** install rather than the normal *Complete* install.

When the **Custom Setup** window appears, click the **Lync Archiving** subsystem under the **VaultBox** system. A **Browse...** button is displayed under the list of systems. Click **Browse** and in the **Change destination folder** window select a new working directory folder, then click **OK**. Click **Next** to continue with the install.

The working directory's path can also be changed using the registry key:
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\MessageOne\EMS\Lync\ArchiveService. If this registry key is changed after the EMS Lync Archiving services have begun archiving conversations to the Data Center, the `Metadata` subfolder from the old working directory path should be copied to the new path. If this step is missed, then it could result in exporting Lync conversations that have already been exported.

10.5.6.5. Stop EMS Lync Archiving Service

If you attempt to stop the `MessageOne Lync Archive` service while it is in the middle of exporting a large number of Lync conversations from Lync SQL archiving database(s), the service may not stop immediately.

By design, the `MessageOne Lync Archive Service` will wait for the export to complete before it stops, because the service cannot cancel the export for a given timeslice once the export has begun.

When stopping a long export, `MessageOne Lync Archive Service` will log a warning to the log file every 10 seconds until the export is fully completed.

10.5.6.6. EMS Lync Archiving Conversation Transformation Failures

Lync conversations that fail to transform will be placed into a `TransformFailed` subfolder under the EMS Lync Archiving Working Directory (For example: `C:\ProgramData\MessageOne\LyncArchive\TransformFailed`). Additional information about the failure can be found in the corresponding `TransformService.log` file.

11. Getting Support

This chapter provides information on getting support for your EMS products, including the following sections:

- ["Support Overview" on page 339](#)
- ["Contact Customer Support" on page 339](#)
- ["Service Availability" on page 340](#)
- ["Improve Customer Support" on page 341](#)

11.1. Support Overview

For any system problem or question the first point of contact should be our Customer Support Center.

The Customer Support Center is staffed 24 hours a day, 365 days a year to assist you with product activations/recoveries, upgrades, questions, documentation requests, product updates, training, or any issue that impacts your mail flow or other key business process.

11.2. Contact Customer Support

To contact Support for either service requests or incident management, refer to the *Customer Support Guide* for the appropriate phone number to call from your area. The guide can be accessed from the **Help and Downloads** menu item on the EMS Administration Console.

11.2.1. Prior to Contacting Support

Before you contact the Customer Support Center, please consider the following questions and have appropriate information available to speed the solution of your issue:

- What were you trying to do when the problem occurred?
- Which user/users are affected by this issue?
- What were your expected results versus the results you received?
- Have you tested this process successfully before? Has this problem happened before?
- Did you receive any error messages?

- Can this problem be duplicated? Is it consistent?
- What operating system and environment are you using?

[Table 11-1](#) is used to classify both Incidents and Service Requests.

Table 11-1 Incident Classification

| Severity | Criteria |
|--------------|--|
| 1 (Critical) | The Services are non-operative or significantly impaired. Access of Services cannot be conducted without significant delay, if at all. No known workaround is currently available. |
| 2 (High) | The Services are non-operative or significantly impaired. Access of Services cannot be conducted without significant delay, if at all. A known workaround is currently available. |
| 3 (Medium) | Services are operative with minor impairment. Issue has little or no impact on daily business process. |
| 4 (Low) | Services are operative. This category includes administrative requests and general questions about product functionality. |

11.2.2. Service Requests and Telephone Authorization Form

The Telephone Authorization form is very important, as it documents the specific individuals within your organization who are authorized to contact our Customer Support Center.

Persons named within this list have the ability to contact support and request the activation or deactivation of services on your organizations behalf. Designated individuals must be able to verify identity and service entitlement by answering the challenge question submitted by the authorizing administrator via the Telephone Authorization form.

This allows your organization to use MessageOne services even in the event you are unable to login to the product directly.

To obtain a telephone authorization form, please contact Support and request a new template.

11.3. Service Availability

MessageOne maintains service availability goals for EMS. Certain events are exceptions to this availability goal, including:

- Failure of access through the circuits to the MessageOne network
- Networking and configuration issues outside the direct control of MessageOne
- Scheduled maintenance
- Emergency maintenance and upgrades
- Circumstances beyond the reasonable control of MessageOne
- Customer acts or omissions

11.4. Improve Customer Support

Your feedback matters to us. Please contact our Customer Support Center and let us know how we can help you and how we can improve our service.

Index

Symbols

.NET Framework 49

Numerics

3rd-party archive support (enabling) 191

A

account requirements

 See Active Directory Service account

 See also permissions

Activation (Email Continuity)

 customizing message on log in screen 200

 overview 204

 partial 3

 reports 229

 start 205

 starting recovery from 207

Active Directory Service account

 Exchange permissions 325

 Lync Archiving membership 325

 membership 50

 requirements 50

Admin Console 132, 309

administrator account

 assign privileges 155

 intro 131

 permissions 152

 remove privileges 155

AlertFind integration

 about 1

 administration 195

 importing data to 195

 limitations 78

 mapping 195

 requirements 78

AlertFindintegration

 users' contact information and 150

aliases, creating 166

antivirus 82

Archive Searches History Report 296

archives

 discovery 38, 279, 334

 max size 280

 Lync Archiving

 See Lync Archiving 319

 search-based 279

 max size 279

archiving

 Lync Archiving

 See Lync Archiving 319

attachments

 storage management 261

audit 296

audit logs

 Email Archive 296

 Email Continuity 229

 EMS 179

audit reports 179

audit trail

 for email routing configuration 186

Authentication Manager, See Windows Authentication Manager

B

BCC Journaling 212

BlackBerry

 See Wireless Continuity for BlackBerry 71

browser 42

browsers

 supported 48

Bulk Flag Resets History Report 180

Bulk Password Updates History Report 180

C

cached mode 68

Cloud Services

 about 2, 305

 admin console updates 309

 envelope journaling 305

 hybrid environment 305

 journaling address 310

 Office 365

 administration 316

 best practices 317

 installation 313

 prerequisites 312

 readiness checks 138, 309

 retention policies 61

 unstub users 316

 on-premises users 305

 readiness checks 138, 309

 special considerations 305

customer support

 contact 339

 overview 339

 service request 340

 telephone authorization form 340

D

date

 international 236

Discovery Archives

- defined 38, 279
 - Lync Discovery Archive 334
 - max size 280
 - recovering mail from 38, 279
 - reviewer groups 247
 - dropbox 232
- E**
- Email Archive
 - audit logs 296
 - current membership retention policies 32
 - defined 235
 - discovery archives 38, 279
 - enable classic interface 202
 - international dates 236
 - retention holds 37, 244
 - reviewer groups 247
 - See also Historical Mail
 - simulate retention holds 246
 - storage management 261
 - time-of-capture retention policies 33
 - user classification retention policies 34, 128
 - Email Continuity
 - activate 205
 - audit logs 229
 - changing message to users during each state 200
 - completing recovery 217
 - defined 10
 - Office 365 306
 - partial activation 3, 205
 - restoring mail to user mailboxes 208
 - starting recovery 207
 - states of 19
 - testing 232
 - welcoming users
 - See welcome process
 - Email Disclaimer History Report 183
 - EMS root account
 - access audit reports 179
 - assign admin privileges 155
 - assign help desk privileges 156
 - BlackBerry 71, 73
 - can create Super Admin 131
 - change Active Directory import 184
 - change email disclaimer 194
 - change password 203
 - configure SyncManager 83
 - features limited to 153
 - install RedirectorManager 90
 - install service software 81
 - intro 131
 - logging in using 132
 - modify system settings 184
 - needed to install service software 80
 - permitted actions 152
 - protect 132
 - remove super admin privileges 154
 - Exchange 2000/2003
 - interaction with service components 8
 - Exchange 2003
 - server software requirements 58
 - Exchange 2007
 - interaction with service components 8
 - server software requirements 49
 - transport agent 88
 - Exchange 2013
 - note regarding CU 1 & 2 88
 - note regarding transport agent priority 88
 - Exchange Resource Forest 66
 - excluded users
 - change status for multiple users 148
 - creating 160
 - Excluded Users History Report 180
 - expanded archive services
 - about 319
 - export
 - users contact info 158
 - Export Manager
 - current version 9
- F**
- Failed Message Tracking
 - about 27
 - additional information 27
 - failed message archive 39
 - failed message count 274
 - indexed message count 274
 - limitations 27
 - message volume report 274
 - storage report page 274
 - stored message count 274
 - why messages fail 27
 - fault alerts
 - adding users to notification list 176
 - for user deletion during sync 197
 - for user ID conflicts 161
 - readiness checks that trigger 135
 - Fault and Transition Alerts History Report 182
 - firewall
 - port 43
 - requirements 43
 - Folder Sync
 - about 28
 - about servers 290
 - additional information 28
 - adjust EWS throttling 295
 - administration 289

- advanced settings 294
- assign Exchange servers 291
- disable users 293
- enable users 292
- Exchange Autodiscover 77
- Exchange Impersonation 77
- excluded folders 28
- exclusion hours 294
- limitations 28
- minimum client version 77
- prerequisites 77
- readiness checks 295
- remove Exchange servers 291

G

- Global Address List 185

H

- hardware
 - requirements 46
 - requirements for Historical Mail 61
- Harvester
 - defined 6
 - data collected and logged by 126
 - how it works 126
 - Office 365 308
 - scheduling 125
- help desk account
 - assign privileges 156
- help desk user account
 - permissions 152
 - remove privileges 156
- Historical Mail
 - defined
 - configure 49
 - configuring VaultBoxes for 92
 - hardware requirements 61
 - replication zones 236
 - retention holds 246
 - reviewer groups 247
 - routing requirements 65
 - storage management 261
 - storage reports
 - aggregate 274
 - retention policy 271
- holds
 - See retention holds 334
- home page 198
- Home Page History Report 183
- HTTPS 42

I

- Import Manager

- current version 9
- Office 365 308
- Instant Message Archiving
 - See Lync Archiving 319
- iOS app
 - administration 164
 - Continuity Archive access 22
 - current version 9
 - download app 164
 - enable 122
 - enable users 122, 164
 - Enterprise Archive access 24
 - minimum iOS version 121

J

- Journaling services
 - manage
 - permissions 152

K

- known issues
 - Wireless Continuity for BlackBerry 72

L

- limitations
 - AlertFind integration 78
 - Email Archive
 - search 259
 - generated queries 259
 - long query 260
 - message envelope 260
 - message size 260
 - special character 260
 - On-Premises Journaling 61
 - Outlook Extension 69
 - Webmail 206
 - Windows Authentication 67
 - Wireless Continuity for BlackBerry 72
- Location-specific Settings 42
- logging in
 - to Email Continuity via a welcome message 167
 - to the administration console 131
 - using Windows Authentication 12
- login status of users 157
- Lync Archiving
 - about 319
 - administration 331
 - advanced topics 336
 - archiving log file 336
 - archiving statistics 334
 - change working directory 337
 - disabling Lync Archiving 337

- discovery archives 334
 - registry values 337
 - retention holds 334
 - retention policy 331
 - reviewer groups 332
 - stop archiving service 338
 - transformation failures 338
 - installation 326
 - client software 327
 - configure client software 327
 - configure Lync server 326
 - limitations 326
 - planning 320
 - prerequisites 325
 - Active Directory Service account 325
 - vaultbox 325
 - supported
 - chat types 320
 - conversation types 320
 - distributed archiving 320
 - Lync Server archive sources 319
 - Lync Server versions 319
 - Lync Server
 - configure Lync Archiving 326
- M**
- mail routing requirements 43
 - See also next hop routing
 - MAPI
 - note regarding Exchange 2013 80
 - MAPI/CDO 49
 - messages
 - adding disclaimer to 194
 - maximum size imported to archive 6
 - undeliverable placed in dropbox 232
 - Messaging and Collaboration client 49
 - messaging software
 - supported 47, 48
 - Microsoft Data Access Components 49
 - Microsoft Exchange Server 48
 - Microsoft Internet Connectivity Wizard 42
 - Microsoft Internet Information Server 49
 - Microsoft Office 365
 - See Cloud Services
 - mobile app
 - about 2
 - administration 164
 - Continuity Archive access 22
 - current version 9
 - download app 164
 - enable 122
 - enable users 122, 164
 - Enterprise Archive access 24
 - minimum software version 121
- MTA 205
- MX Record
 - adding for routing mail to the service 43
 - Configuration 42
 - during activation 205
 - for replication zones 236
 - syntax 44
 - used for forwarding mail 187
 - used for sending outbound mail during activation 189
- N**
- network requirements 42
 - Network Restrictions History Report 183
 - networking requirements 42
 - next hop routing
 - inbound, configuring 186, 187
 - inbound, described 45
 - outbound during activation, configuring 189
 - outbound during activation, described 45
 - next hop status 139, 188
- O**
- Office 365
 - see Cloud Services 305
- On-Premises Journaling
 - about 26
 - best practices 92
 - Capture Policy Service 26
 - Cloud Journaling differences 26
 - configure 92
 - hybrid mode 26
 - limitations 61
 - prerequisites 61
 - readiness check
 - hidden journaled mailboxes 139, 289
 - journaled message retention 139, 289
 - non-journaled message retention 139, 289
 - not received message 139, 288
 - Redirector 57
 - supported environments 60
- operating systems
 - supported 47
- Outlook Extension
 - defined 13
 - authentication of users for 97
 - current version 9
 - customizing Outlook 2010 ribbon 104
 - defined 4
 - enabling and disabling 227
 - exporting list of users 228
 - feature comparison with webmail 14
 - installing 96

- limitations 69
- Office 365 307
- prerequisites 68
- registry keys updated for 105, 107
- remove manually 104
- requirements 67, 68
- supported environments 67
- users active with 227
- using during activation 204

P

Partial Activation

- defined 3

passwords

- changing administrator 203
- Email Continuity 143
- resetting multiple users' 144
- root account 80
- temporary welcome 168
- Windows Authentication of 12

permissions

- grant Exchange admin 53
- grant send as/receive as 53
- help desk user 156
- user levels 151

policies

retention

- add users 241
- create 239
- current membership 32
- delete hold 244
- edit hold 245
- history report 300
- Lync Archiving 331
- manage 237
- prioritize 242
- retention holds (query-based) 37, 244
- statistics 271
- time-of-capture 33
- user classification 34, 128
- using to simulate retention holds 246
- warning 239, 242

storage management

- create 264
- prioritize 266, 267, 268
- statistics 272

preferences, editing home page 198

PrepareOutlookAuth 97

- command line arguments 97
- install 97
- Office 365 308
- Outlook Extension 97

prerequisites

- Outlook Extension 68

Wireless Continuity for BlackBerry 73

proxy requirements 43

proxy servers 14

- note regarding Exchange 2013 80

Q

query language

- examples 257

- boolean 259

- date range 257

- field search 257

- partially indexed 259

- proximity 258

- size range 257

fields 252

- altrecipients 252

- attachedfiles 252

- content 252

- dlists 252

- emaildate 253

- envrecipients 253

- envsender 253

- filename 254

- isattachment 254

- mailbcc 254

- mailbccaltrecipient 254

- mailbccdlist 254

- mailcc 254

- mailccaltrecipient 254

- mailccdlist 254

- mailfrom 254

- mailsubject 254

- mailto 254

- mailtoaltrecipient 254

- mailtodlist 255

- receiveddate 255

- recipients 256

- senders 256

- size 256

- totalsize 256

- undisclosedrecipients 256 query-

based retention holds

See retention holds

R

readiness checks

- blackberry continuity agent 137

- cloud services 138, 309

- Folder Sync 295

- next hop status 139, 188

- on-premises journaling 139, 288

- overview 135

- received journaled message 138, 309

- sending fault alerts when failed 176
- TLS warning 138, 309
- Recovery
 - defined 4
 - completing 217
 - of discovery archives 279
 - restoring mail to user mailboxes 208
 - starting (from an activation) 207
- Recovery Archives
 - creating 276, 277
 - restoring mail from 208
 - search-based recovery archives 279
 - max size 279
- Recovery Archives History Report 299
- RecoveryManager
 - defined 4
 - antivirus 82
 - installation 80
 - Office 365 307
 - Outlook Extension 70
 - restore archives 280
 - See also Recovery
- Redirector component
 - Exchange requirements 58
 - geographic diversity 58
 - note regarding upgrade failure 87
 - prerequisites 57
 - supported platforms 57
- RedirectorAgent
 - defined 3
 - installing 88
- RedirectorController
 - defined 3
 - installation 80
 - status screen 140
- RedirectorManager
 - defined 3
 - configuring 90
 - installation 80
 - upgrading 91
- RedirectorSink
 - defined 3
 - installing
 - on clustered Exchange servers 87
 - standalone 90
 - planning 59
 - planning placement 59
 - status screen 140
 - upgrading RedirectorManager 91
- reminders
 - sending 175
- replication zones 236
 - assign servers 236
- reports
 - activation 229
 - audit 179, 229, 296
 - Outlook Extension 227
 - reviewer group 301
 - storage
 - aggregate 274
 - retention policy 271
 - storage management policy 272
 - test 230
- requirements
 - Active Directory Service account 50
 - communications 42
 - firewall 43
 - hardware 46
 - hardware for Historical Mail 61
 - mail routing 43
 - messaging software 47, 48
 - networking 42
 - operating systems 47
 - proxy 43
 - routing for historical mail 65
 - server software 49
 - SMTP connector for Historical Mail 65
 - third-party gateway 44
- retention holds
 - delete 244
 - edit 245
 - Lync Archiving retention hold 334 query-based 37, 244
 - max message limit 244
 - retention policy to simulate 246
- retention policy
 - add users 241
 - create 239
 - date 30
 - history report 300
 - Lync Archiving 331
 - manage 237
 - prioritize 242
 - statistics report 271
 - warning 239, 242
- reviewer groups
 - defined 247
 - advanced search options 251
 - create 247
 - delete 250
 - edit 249
 - Lync Archiving 332
 - permission to create 152
 - reports 301
 - restoring mail from discovery archives 38, 279
- Reviewer Groups History Report 301
- RFC-822 70
- RIM Agent 4

- root account
 - See EMS root account
- RPC
 - note regarding RPC over HTTP 80
- S**
- search-based recovery archives 279
 - max size 279
- service account
 - See Active Directory Service account
 - See EMS root account
- service availability 340
- SMTP
 - connector for Historical Mail 65
 - gateway servers 60
 - message gateway 43
 - used in Windows Authentication 67
- statistics
 - Lync Archiving 334
- Storage Management
 - defined 261
 - configuring VaultBoxes for 123
 - harvester 6
 - Office 365 307
 - policies
 - create 264
 - plan 261
 - prioritize 266, 267, 268
 - reports
 - aggregate 274
 - policy statistics 272
 - scheduling 125
 - stubbing
 - defined 261
 - unstub 268, 269
- storage reports 270
 - aggregate 274
 - retention policy 271
 - storage management policy 272
 - view 271
- store and forward mail routing 45, 190
- superadmin account
 - assign admin privileges 155
 - assign help desk privileges 156
 - assign privileges 153
 - create 154
 - features limited to 153
 - intro 131
 - modify system settings 184
 - permissions 152
 - remove privileges 154
- support
 - contact 339
 - overview 339
- service request 340
- telephone authorization form 340
- SyncManager
 - defined 3
 - configuring 82
 - configuring user deletion to trigger alert 197
 - installation 80
 - Office 365 306
 - port used 42
 - setting schedules for 82
 - synchronizing RIM data 111
- system settings
 - enable classic archive interface 202
- T**
- test
 - Email Continuity 232
 - reports 230
- Test History Report 230
- third-party gateway requirements 44
- TLS Security readiness check 309
- transition alerts 177
- transition reports 229
- transport agent 88
 - note regarding Exchange 2013 88
 - note regarding Redirector upgrade failure 87
- U**
- undeliverable mail 232
- unstub 268
 - all users 269
 - command-line tool 269
 - Office 365 users 316
 - PowerShell 270
 - primary SMTP address 270
 - single user 268
- user
 - permissions 152
- User Classification History Report 303
- User Conflicts History Report 180
- user flags
 - set/clear
 - flags
 - user set/clear 148
- user ID conflict
 - global settings for resolving 162, 196
 - history report 180
 - identified by SyncManager 83
 - resolve automatically 162
 - resolve CSV upload 162
 - resolve individually 163
 - resolve manually 161, 162
- User Information Exports History Report 180

User Permissions History Report 180
User Sets History Report 180
users
 activate Email Continuity for 205
 add manually to Email Continuity 165
 administrator 155
 attributes
 displayed in Global Address List 185
 imported from Active Directory 184
 change opt-out status 148
 change status in the system 148
 create aliases 166
 deletion during sync, configuring warnings 197
 exclude from the service 148, 160
 export contact info 158
 grant administrative privileges 155
 help desk 156
 keep stored mail for when new mailbox is created 83, 161, 162
 login status of 157
 passwords for 143
 permission levels 151
 permission requirements 47
 restore mail after an activation 208
 search information 141
 send reminders 175
 set/clear flags 148
 superadmin 153
 update contact information 150
 user set (define) 150
 user set (upload) 150
 welcoming to the service
 See welcome process
Users Welcomed History Report 182

V

VaultBox
 defined 3
 capacity sizing 64
 communications with data center 8
 components
 for ActiveMailbox 6
 configuring
 for Historical Mail 92
 for storage management 123
 console 92
 hardware requirements 61
 Lync Archiving
 prerequisites 325
 mail routing requirements 65
 planning 62
 preinstallation requirements 62
 replication zones for 236
virtualization 56

W

Warnings, See Fault Alerts
Webmail
 limitations 206
welcome process
 about 167
 automatic welcome message process 174
 best practices 169
 change status for multiple users 148
 message to new users 170
 message variables 169
 resent to any user 171
 resent to no permanent password 173
 resent to non-responders 172
 send reminder 175
 send reminder to keep info current 175
 send reminder to non-responders 175
Windows Authentication
 defined 12
 change users' passwords 143
 limitations 67
 requirements 66
Windows Authentication Manager
 defined 4
 status screen 140
Windows Installer 47
Wireless Continuity for BlackBerry
 administration 221
 defined 15, 71
 known issues 72
 limitations 72
 manage users and devices 222
 prerequisites 73
 provision 221
 requirements 71
 supported configurations 71
 synchronize RIM data 111