## Preface
- Audience ................................................................. xxii
- Documentation Accessibility .................................... xxii
- Related Documents .................................................. xxii
- Conventions ............................................................... xxii

## What’s New in Oracle Mail ........................................... xxiii

## 1 Introduction to Oracle Mail Administration

### Overview of Oracle Mail ........................................... 1-1

### Overview of Oracle Mail Administration .................. 1-1
- Oracle Collaboration Suite 10g WebMail Client .... 1-2
- Oracle Enterprise Manager 10g Application Server Control Console for Collaboration Suite 1-3
- Oracle Enterprise Manager 10g Grid Control Console 1-4
- Oracle Mail Command-Line Utilities ...................... 1-4

## 2 Managing Oracle Mail Objects

### Managing Oracle Mail Users ................................. 2-1
- Adding E-mail Users ............................................. 2-2
- Modifying E-mail User Attributes ......................... 2-4
- Setting Default New User Attributes ...................... 2-6
- Removing E-mail Users ......................................... 2-8
- Recovering Deleted Messages ............................... 2-8

### Managing Oracle Mail Domains .......................... 2-10
- Creating Domains .................................................. 2-11
- Modifying Domain Settings .................................... 2-11

### Managing Distribution Lists .............................. 2-12
- Setting Default Distribution List Attributes .......... 2-13
- Distribution List Parameters ................................. 2-16
- Creating a Distribution List ................................... 2-19
- Modifying Distribution List Properties ................. 2-20
- Modifying Default Distribution List Parameter Values 2-20
- Deleting a Distribution List ................................... 2-21
- Managing Distribution List Members .................... 2-21
Rule Execution Guidelines ........................................................................................................ 3-19
Oracle Mail Rewriting Rules ................................................................................................. 3-19
Creating an Oracle Mail Address Rewriting Rule .............................................................. 3-21
SMTP Server Parameters .................................................................................................... 3-22
Managing SMTP Servers ...................................................................................................... 3-22
SMTP Routing Control ........................................................................................................ 3-23
Housekeeper Server ........................................................................................................... 3-23
Configuring Housekeeper Tasks ........................................................................................ 3-24
Process Control Message Cleanup ...................................................................................... 3-25
Setting Up LogMiner to Recover Mail ................................................................................ 3-26
Oracle Text .......................................................................................................................... 3-27
Enabling E-mail Body Searching for Various Languages ...................................................... 3-28
Verifying Oracle Text Installation ....................................................................................... 3-29
Creating a Housekeeper Server Instance to Index Text .................................................... 3-29
Enabling Text Indexing for a User ...................................................................................... 3-30
Tertiary Storage ................................................................................................................... 3-31
Moving the ESTERSTORE Tablespace ................................................................................ 3-31
Enabling Tertiary Storage .................................................................................................. 3-32
Housekeeper Server Parameters ....................................................................................... 3-33
Managing Housekeeper ..................................................................................................... 3-33
List Server .......................................................................................................................... 3-33
List Server Mail Interface .................................................................................................... 3-34
Archiving Distribution List Posts ......................................................................................... 3-34
External Distribution Lists .................................................................................................. 3-35
Distribution List Digests ....................................................................................................... 3-37
Distribution List Bounce Processing ..................................................................................... 3-38
Multiple Language Responses .......................................................................................... 3-38
Mail Merge .......................................................................................................................... 3-38
List Server Parameters ....................................................................................................... 3-41
Managing List Servers ........................................................................................................ 3-41
NNTP Server ....................................................................................................................... 3-41
About News Servers ............................................................................................................ 3-42
Controlling News Storage ................................................................................................. 3-42
Article Caching for Performance ......................................................................................... 3-43
NNTP Processes .................................................................................................................. 3-43
NNTP Inbound Server .......................................................................................................... 3-43
NNTP Outbound Server ...................................................................................................... 3-43
NNTP Server Parameters ................................................................................................. 3-44
Managing NNTP Servers ................................................................................................. 3-44

4 Oracle Collaboration Suite 10g WebMail Client

Oracle WebMail Client Overview ....................................................................................... 4-1
Oracle WebMail Tool Kit Default Settings ......................................................................... 4-2
Oracle WebMail Client Properties ..................................................................................... 4-2
Oracle WebMail oc4j.properties File Properties ............................................................... 4-3
Service Registry Dependency ............................................................................................ 4-8
Configuring SSL Between Oracle WebMail and Oracle Internet Directory ....................... 4-9
5 Directory Cache

About Directory Cache ........................................................................................................... 5-1
Directory Cache Search Behavior ......................................................................................... 5-1
Directory Cache Default Behavior ......................................................................................... 5-2
Location of Directory Cache Logs ......................................................................................... 5-2
Enabling Directory Cache ...................................................................................................... 5-2

6 Oracle Mail Security

Oracle Mail Security Overview ............................................................................................... 6-1
E-mail System Component Security ....................................................................................... 6-1
Information Storage Database ............................................................................................... 6-2
Oracle Collaboration Suite Applications Tier .......................................................................... 6-2
Identity Management Infrastructure ....................................................................................... 6-3
Mail Clients ............................................................................................................................ 6-3
Network Security .................................................................................................................... 6-3
Firewalls ................................................................................................................................. 6-4
Non-technical Considerations ............................................................................................... 6-4
SSL and TLS .......................................................................................................................... 6-5
Antispam Methods ................................................................................................................ 6-5
Third-Party Antispam Filters ............................................................................................... 6-5
Routing Control for SMTP ................................................................................................. 6-6
Routing Control for NNTP ................................................................................................... 6-9
Wildcards ............................................................................................................................... 6-9
Routing Control Parameters for NNTP and SMTP .............................................................. 6-9
Symantec AntiVirus Scan Engine ......................................................................................... 6-10
Editing SAVSE Filters ....................................................................................................... 6-10
Applying SAVSE Filters ..................................................................................................... 6-13
Virus Scrubber ...................................................................................................................... 6-14
  Configuring the Virus Scrubber with the Oracle Enterprise Manager 10g Application Server Control Console for Collaboration Suite ........................................................... 6-15
Virus Scanning and Removal Using PL/SQL Scripts .......................................................... 6-18
Usage Examples ................................................................................................................... 6-19

7 Monitoring Oracle Mail

Monitoring Oracle Mail Using Oracle Enterprise Manager 10g Grid Control Console ......... 7-1
Overview of Oracle Mail Target Types ................................................................................. 7-1
Identifying Oracle Mail Hosts and Databases ..................................................................... 7-2
  Identifying the Oracle Mail Component Hosts .................................................................. 7-2
  Identifying Locations of Oracle Collaboration Suite Databases ...................................... 7-2
  Identifying the Connection String for an Oracle Collaboration Suite Database ................ 7-3
About Oracle Mail Service Targets ....................................................................................... 7-3
Creating Oracle Mail Service Targets .................................................................................. 7-4
Creating an Oracle WebMail Web Application Target ....................................................... 7-5
8 Oracle Mail Policies

Overview of Oracle Mail Policies ................................................................. 8-1
Managing Oracle Mail Filters .................................................................... 8-2
Creating a Filter ......................................................................................... 8-2
Editing Filters ......................................................................................... 8-3
Reordering Filters .................................................................................. 8-3
Applying Filters ..................................................................................... 8-4
Editing Applied Filters ......................................................................... 8-7
Oracle Mail Routing Control .................................................................... 8-8
Configuring Routing Control for Incoming Mail ...................................... 8-8
Configuring General Routing Control Settings for Incoming Mail .......... 8-9
Configuring Reject Routing Control Settings for Incoming Mail .......... 8-10
Configuring Trust Routing Control Settings for Incoming Mail ............ 8-13
Configuring Advanced Routing Control Settings for Incoming Mail ...... 8-16
Saving and Copying Routing Control Settings for Incoming Mail ........ 8-18
Configuring Routing Control for Outgoing Mail ..................................... 8-19
Configuring Routing Control for Incoming News ................................... 8-21
Configuring General Routing Control Settings for Incoming News ...... 8-21
Configuring Reject Routing Control Settings for Incoming News ........ 8-22
Configuring Trust Routing Control Settings for Incoming News .......... 8-24
Oracle Mail Archive Policies ................................................................. 8-26
Creating an Archive Policy ...................................................................... 8-27
Editing an Archive Policy ....................................................................... 8-28
Associating Users with an Archive Policy .............................................. 8-28
Enabling Message Archiving ................................................................. 8-29
Message Recall ....................................................................................... 8-30
# Oracle Mail Server-Side Rules

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>What Is a Server-Side Rule?</td>
<td>9-1</td>
</tr>
<tr>
<td>Managing Server-Side Rules</td>
<td>9-8</td>
</tr>
<tr>
<td>Creating Server-Side Rules</td>
<td>9-8</td>
</tr>
<tr>
<td>Displaying Existing Server-Side Rules with oesrl</td>
<td>9-8</td>
</tr>
<tr>
<td>Creating Server-Side Rules with oesrl</td>
<td>9-8</td>
</tr>
<tr>
<td>Editing Server-Side Rules</td>
<td>9-9</td>
</tr>
<tr>
<td>Deleting Server-Side Rules</td>
<td>9-9</td>
</tr>
<tr>
<td>Creating Server-Side Rules Using an E-mail Client</td>
<td>9-10</td>
</tr>
<tr>
<td>How Server-Side Rules Are Stored</td>
<td>9-10</td>
</tr>
<tr>
<td>Order in Which Server-Side Rules Are Executed</td>
<td>9-10</td>
</tr>
</tbody>
</table>

## Server-Side Rule Examples

# Backing Up and Recovering Oracle Mail

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview of Oracle Mail Backup and Recovery</td>
<td>10-1</td>
</tr>
<tr>
<td>Backing Up and Recovering the Oracle Collaboration Suite Database</td>
<td>10-1</td>
</tr>
<tr>
<td>Backing Up and Restoring User Data with oesbkp</td>
<td>10-2</td>
</tr>
<tr>
<td>Recovering Messages with LogMiner</td>
<td>10-4</td>
</tr>
<tr>
<td>Recovering Messages with Oracle Flashback Query</td>
<td>10-5</td>
</tr>
<tr>
<td>Using Oracle Flashback Query to Recover Messages</td>
<td>10-5</td>
</tr>
<tr>
<td>MAIL_RECOVERY_FQ Package</td>
<td>10-7</td>
</tr>
</tbody>
</table>

# Troubleshooting Oracle Mail

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Becoming Aware of a Problem</td>
<td>A-1</td>
</tr>
<tr>
<td>End-User Issues</td>
<td>A-3</td>
</tr>
<tr>
<td>Problems with Mail Clients</td>
<td>A-3</td>
</tr>
<tr>
<td>User Unable to Log In to Account</td>
<td>A-3</td>
</tr>
<tr>
<td>High Login Time Experienced</td>
<td>A-4</td>
</tr>
<tr>
<td>It Takes a Long Time to Download a Mail Message</td>
<td>A-6</td>
</tr>
<tr>
<td>Unable to Read a Particular Message</td>
<td>A-6</td>
</tr>
<tr>
<td>During Peak Periods, Valid Users Receive Invalid Username and Password Error</td>
<td>A-6</td>
</tr>
<tr>
<td>Cannot Send Mail</td>
<td>A-6</td>
</tr>
<tr>
<td>Server Says Password is Incorrect but Password Has Not Changed</td>
<td>A-7</td>
</tr>
<tr>
<td>It Takes a Long Time to Open the Inbox</td>
<td>A-7</td>
</tr>
<tr>
<td>Oracle WebMail Client Issues</td>
<td>A-7</td>
</tr>
<tr>
<td>Problems with Mail Delivery</td>
<td>A-7</td>
</tr>
<tr>
<td>User Says Mail Delivery to Internet Addresses Does Not Occur</td>
<td>A-8</td>
</tr>
<tr>
<td>User Did Not Receive a Mail Message That Was Certainly Sent</td>
<td>A-8</td>
</tr>
<tr>
<td>User Does Not Receive Mail for 4 to 5 Minutes, but There Is Little Database Load</td>
<td>A-10</td>
</tr>
<tr>
<td>User Receives Most Messages Quickly, but Some Are Delayed for Hours or Days</td>
<td>A-10</td>
</tr>
<tr>
<td>Users say They Received Mail from a Distribution List, While Others Say They Have Not</td>
<td>A-10</td>
</tr>
<tr>
<td>Message Is Caught in a Mail Loop</td>
<td>A-11</td>
</tr>
<tr>
<td>Messages Are Being Rejected</td>
<td>A-11</td>
</tr>
<tr>
<td>Message delivery is slow</td>
<td>A-12</td>
</tr>
<tr>
<td>Problems with a Single Message</td>
<td>A-12</td>
</tr>
</tbody>
</table>
B Oracle Mail Error Messages
Overview of Oracle Mail Error Messages .......................................................... B-1
IMAP and POP Error Messages ........................................................................... B-1
SMTP Error Messages ...................................................................................... B-4
Housekeeper Error Messages ........................................................................... B-6
List Server Error Messages .............................................................................. B-7
NNTP Error Messages ....................................................................................... B-8
Virus Scrubber Error Messages ..................................................................... B-11
Oracle WebMail Error Messages ................................................................ B-11

C Shared Folders
Overview of Shared Folders ........................................................................... C-1
Understanding Access Control Lists for Shared Folders ................................ C-1
Managing Public Folders ................................................................................. C-3
Creating Public Folders .................................................................................. C-3
## D Oracle Mail Command-Line Reference

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>oesdl</td>
<td>D-2</td>
</tr>
<tr>
<td>oesmon</td>
<td>D-6</td>
</tr>
<tr>
<td>oesrl</td>
<td>D-8</td>
</tr>
<tr>
<td>oesctl</td>
<td>D-9</td>
</tr>
<tr>
<td>opmnctl</td>
<td>D-10</td>
</tr>
<tr>
<td>oesng</td>
<td>D-10</td>
</tr>
<tr>
<td>oespr</td>
<td>D-10</td>
</tr>
<tr>
<td>oesusr</td>
<td>D-11</td>
</tr>
<tr>
<td>oesctl</td>
<td>D-12</td>
</tr>
<tr>
<td>opmnctl</td>
<td>D-14</td>
</tr>
<tr>
<td>oesusr</td>
<td>D-15</td>
</tr>
<tr>
<td>oesctl</td>
<td>D-17</td>
</tr>
<tr>
<td>opmnctl</td>
<td>D-15</td>
</tr>
<tr>
<td>oesusr</td>
<td>D-18</td>
</tr>
<tr>
<td>oesctl</td>
<td>D-20</td>
</tr>
<tr>
<td>opmnctl</td>
<td>D-20</td>
</tr>
<tr>
<td>oesusr</td>
<td>D-20</td>
</tr>
<tr>
<td>oesctl</td>
<td>D-20</td>
</tr>
<tr>
<td>opmnctl</td>
<td>D-20</td>
</tr>
<tr>
<td>oesusr</td>
<td>D-20</td>
</tr>
<tr>
<td>oesctl</td>
<td>D-21</td>
</tr>
<tr>
<td>opmnctl</td>
<td>D-21</td>
</tr>
<tr>
<td>oesusr</td>
<td>D-21</td>
</tr>
<tr>
<td>oesctl</td>
<td>D-22</td>
</tr>
<tr>
<td>opmnctl</td>
<td>D-22</td>
</tr>
<tr>
<td>oesusr</td>
<td>D-22</td>
</tr>
<tr>
<td>oesctl</td>
<td>D-22</td>
</tr>
<tr>
<td>opmnctl</td>
<td>D-22</td>
</tr>
<tr>
<td>oesusr</td>
<td>D-22</td>
</tr>
<tr>
<td>oesctl</td>
<td>D-24</td>
</tr>
<tr>
<td>opmnctl</td>
<td>D-24</td>
</tr>
<tr>
<td>oesusr</td>
<td>D-24</td>
</tr>
<tr>
<td>oesctl</td>
<td>D-26</td>
</tr>
<tr>
<td>opmnctl</td>
<td>D-26</td>
</tr>
<tr>
<td>oesusr</td>
<td>D-26</td>
</tr>
<tr>
<td>oesctl</td>
<td>D-26</td>
</tr>
<tr>
<td>opmnctl</td>
<td>D-26</td>
</tr>
<tr>
<td>oesusr</td>
<td>D-26</td>
</tr>
<tr>
<td>oesctl</td>
<td>D-27</td>
</tr>
<tr>
<td>opmnctl</td>
<td>D-27</td>
</tr>
<tr>
<td>oesusr</td>
<td>D-27</td>
</tr>
<tr>
<td>oesctl</td>
<td>D-27</td>
</tr>
<tr>
<td>opmnctl</td>
<td>D-27</td>
</tr>
<tr>
<td>oesusr</td>
<td>D-27</td>
</tr>
<tr>
<td>oesctl</td>
<td>D-29</td>
</tr>
<tr>
<td>opmnctl</td>
<td>D-29</td>
</tr>
<tr>
<td>oesusr</td>
<td>D-29</td>
</tr>
<tr>
<td>oesctl</td>
<td>D-30</td>
</tr>
<tr>
<td>opmnctl</td>
<td>D-30</td>
</tr>
<tr>
<td>oesusr</td>
<td>D-30</td>
</tr>
</tbody>
</table>
E  Oracle Mail Supported RFCs

F  Oracle Mail Server Parameters and Log Files

Oracle Mail Server Parameter Definitions ...........................................................................  F-1
  Oracle Mail Housekeeper ...............................................................................................  F-2
    Oracle Mail Housekeeper Instance Setting Parameters .............................................  F-3
    Oracle Mail Housekeeper Debug Parameters ............................................................  F-5
  Oracle Mail IMAP Server ..............................................................................................  F-6
    Oracle Mail IMAP Server Instance Setting Parameters .............................................  F-6
    Oracle Mail IMAP Server Debug Parameters ............................................................  F-11
  Oracle Mail IMAP Oracle Collaboration Suite Database Connection Parameters ......  F-12
Oracle Mail NNTP Inbound Server ..................................................................................  F-12
  Oracle Mail NNTP Inbound Server Instance Setting Parameters ...............................  F-12
  Oracle Mail NNTP Inbound Server Debug Parameters ................................................  F-12
  Oracle Mail NNTP Inbound Oracle Collaboration Suite Database Connection Parameters  F-15
Oracle Mail NNTP Outbound Server ..............................................................................  F-15
  Oracle Mail NNTP Outbound Server Instance Setting Parameters .............................  F-16
  Oracle Mail NNTP Outbound Server Debug Parameters .............................................  F-17
Oracle Mail NNTP Outbound Oracle Collaboration Suite Database Connection Parameters ................................................. F-17
Oracle Mail POP Server ......................................................................................................................................................... F-18
Oracle Mail POP Server Instance Setting Parameters ........................................................................................................ F-18
Oracle Mail POP Server Debug Parameters .......................................................................................................................... F-20
Oracle Mail POP Server Oracle Collaboration Suite Database Connection Parameters ....................................................... F-21
Oracle Mail Virus Scrubber ...................................................................................................................................................... F-21
Oracle Mail Virus Scrubber Instance Settings ............................................................................................................................ F-21
Oracle Mail Virus Scrubber Debug Parameters .......................................................................................................................... F-24
Oracle Mail Virus Scrubber Oracle Collaboration Suite Database Connection Parameters .......................................................... F-24
Oracle Mail List Server .............................................................................................................................................................. F-25
Oracle Mail List Server Target-Level Settings ............................................................................................................................ F-25
Oracle Mail List Server Instance Debug Parameters .................................................................................................................. F-33
Oracle Mail List Server Oracle Collaboration Suite Database Connection Parameters .............................................................. F-34
Oracle Mail SMTP Inbound Server .............................................................................................................................................. F-34
Oracle Mail SMTP-Inbound Instance Settings ............................................................................................................................... F-34
Oracle Mail SMTP-Inbound Instance Debug Parameters ......................................................................................................... F-43
Oracle Mail SMTP-Inbound Oracle Collaboration Suite Database Connection Parameters .......................................................... F-44
Oracle Mail SMTP Outbound Server .......................................................................................................................................... F-44
Oracle Mail SMTP Outbound Instance Settings ............................................................................................................................ F-44
Oracle Mail SMTP Outbound Instance Debug Parameters ........................................................................................................ F-47
Oracle Mail SMTP Outbound Oracle Collaboration Suite Database Connection Parameters .......................................................... F-48

G  Alias and Distribution List Lookup

   Enabling Alias Lookup from Standard Clients .................................................................................................................. G-1
   Enabling Distribution List Lookup from Standard Clients ..................................................................................................... G-2
   Distribution List Synchronization Utility ................................................................................................................................. G-4
   Synchronizing One or Multiple Distribution Lists .................................................................................................................. G-4
   Synchronizing All Distribution Lists from a Private E-mail Namespace .................................................................................. G-4

H  Oracle Mail Server Metrics

   Metrics Common to All Oracle Mail Servers .......................................................................................................................... H-1
   POP Server Metrics ................................................................................................................................................................. H-2
   IMAP Server Metrics ............................................................................................................................................................... H-3
   SMTP Inbound Server Metrics ................................................................................................................................................ H-3
   SMTP Outbound Server Metrics .............................................................................................................................................. H-4
   Housekeeper Server Metrics .................................................................................................................................................. H-5
   List Server Metrics ................................................................................................................................................................. H-6
   NNTP Inbound Server Metrics ................................................................................................................................................ H-6
   NNTP Outbound Server Metrics .............................................................................................................................................. H-7
   Virus Scrubber Server Metrics .............................................................................................................................................. H-7

I  Plug-in for Oracle Mail User Provisioning Customizations

   Generating a User ID Based on User's First and Last Names .................................................................................................. I-3
List of Figures

3–1 IMAP and POP Data Flow ........................................................................................................ 3-11
3–2 Oracle WebMail Client Data Flow ........................................................................................ 3-12
3–3 SMTP Message Flow ............................................................................................................ 3-15
3–4 Message Header .................................................................................................................. 3-18
3–5 Rewriting Rule Example ..................................................................................................... 3-20
3–6 Changing Uppercase to Lowercase ................................................................................ 3-20
3–7 Message Flow through Rewriting Rules .......................................................................... 3-22
9–1 Life Cycle of an E-mail Message ...................................................................................... 9-2
D–1 User Entry Checks ............................................................................................................ D-33
D–2 Distribution List Entry Checks ........................................................................................ D-35
D–3 Alias Entry Checks ........................................................................................................... D-37
D–4 Foreign User Entry Checks ............................................................................................. D-38
D–5 Process Entry Checks ........................................................................................................ D-39
D–6 Newsgroup Entry Checks ................................................................................................ D-40
D–7 News Peer Entry Checks .................................................................................................. D-41
D–8 Shared Folder Entry Checks ............................................................................................ D-42
D–9 Private Address Book Entry Checks .............................................................................. D-44
**List of Examples**

<table>
<thead>
<tr>
<th>Example</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3–1</td>
<td>List of SMTP Outbound Server Log Files</td>
<td>3-4</td>
</tr>
<tr>
<td>3–2</td>
<td>Oracle Mail Server Log Files Listed in the opmn Log Directory</td>
<td>3-4</td>
</tr>
<tr>
<td>3–3</td>
<td>Debug Output</td>
<td>3-4</td>
</tr>
<tr>
<td>3–4</td>
<td>Example of Original Header</td>
<td>3-18</td>
</tr>
<tr>
<td>3–5</td>
<td>Resulting Header as Seen by the Recipient</td>
<td>3-19</td>
</tr>
<tr>
<td>A–1</td>
<td>Structure of a Rule</td>
<td>A-13</td>
</tr>
<tr>
<td>A–2</td>
<td>Structure of a Rule in user_source View</td>
<td>A-13</td>
</tr>
<tr>
<td>A–3</td>
<td>Status of Listener</td>
<td>A-23</td>
</tr>
<tr>
<td>D–1</td>
<td>File Containing Multiple Users</td>
<td>D-13</td>
</tr>
<tr>
<td>D–2</td>
<td>esd_logscan.pl Example</td>
<td>D-47</td>
</tr>
<tr>
<td>D–3</td>
<td>esd_find_message.sql Output Example</td>
<td>D-50</td>
</tr>
<tr>
<td>D–4</td>
<td>esd_show_message.sql Output Example</td>
<td>D-51</td>
</tr>
<tr>
<td>D–5</td>
<td>Sample esd_show_sessions.sql Output</td>
<td>D-55</td>
</tr>
<tr>
<td>D–6</td>
<td>Sample esd_show_session_usage.sql Output</td>
<td>D-57</td>
</tr>
</tbody>
</table>
List of Tables

<table>
<thead>
<tr>
<th>Page</th>
<th>Table Title</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-1</td>
<td>Distribution List Group Types</td>
<td>2-15</td>
</tr>
<tr>
<td>2-2</td>
<td>Distribution List Subscription Types</td>
<td>2-15</td>
</tr>
<tr>
<td>2-3</td>
<td>Distribution List Posting Types</td>
<td>2-16</td>
</tr>
<tr>
<td>2-4</td>
<td>Distribution List Parameters</td>
<td>2-16</td>
</tr>
<tr>
<td>3-1</td>
<td>Oracle Collaboration Suite Database Connection Parameters</td>
<td>3-2</td>
</tr>
<tr>
<td>3-2</td>
<td>Mailer, Host, and User Parameters</td>
<td>3-17</td>
</tr>
<tr>
<td>3-3</td>
<td>Rewriting Rule Components</td>
<td>3-19</td>
</tr>
<tr>
<td>3-4</td>
<td>Tertiary Storage Usage and the ESTERSTORE Tablespace</td>
<td>3-31</td>
</tr>
<tr>
<td>3-5</td>
<td>customer_list Table</td>
<td>3-37</td>
</tr>
<tr>
<td>3-6</td>
<td>Types of Mail Merge and Customizable Features</td>
<td>3-39</td>
</tr>
<tr>
<td>3-7</td>
<td>Example emp_payroll Table</td>
<td>3-40</td>
</tr>
<tr>
<td>3-8</td>
<td>send_schedule Parameter Descriptions</td>
<td>3-41</td>
</tr>
<tr>
<td>4-1</td>
<td>Oracle WebMail Client Properties</td>
<td>4-3</td>
</tr>
<tr>
<td>4-2</td>
<td>Overwriting SMTP Host and Port Properties</td>
<td>4-8</td>
</tr>
<tr>
<td>4-3</td>
<td>Oracle Mail Portlet API Properties</td>
<td>4-10</td>
</tr>
<tr>
<td>6-1</td>
<td>Security Components of the Information Storage Database</td>
<td>6-2</td>
</tr>
<tr>
<td>6-2</td>
<td>Symantec Filter String Parameters</td>
<td>6-12</td>
</tr>
<tr>
<td>6-3</td>
<td>Virus Scrubber General Parameters</td>
<td>6-15</td>
</tr>
<tr>
<td>7-1</td>
<td>E-Mail IMAP Service Target Properties</td>
<td>7-4</td>
</tr>
<tr>
<td>7-2</td>
<td>E-Mail SMTP Inbound Service Target Properties</td>
<td>7-5</td>
</tr>
<tr>
<td>7-3</td>
<td>E-Mail Collaboration Suite Database Target Properties</td>
<td>7-6</td>
</tr>
<tr>
<td>7-4</td>
<td>Oracle Internet Directory Client Target Properties</td>
<td>7-7</td>
</tr>
<tr>
<td>7-5</td>
<td>oesmon Syntax Options</td>
<td>7-9</td>
</tr>
<tr>
<td>7-6</td>
<td>Different Service Types Used in Target Names</td>
<td>7-10</td>
</tr>
<tr>
<td>7-7</td>
<td>es_perf_process Table</td>
<td>7-13</td>
</tr>
<tr>
<td>7-8</td>
<td>es_perf_metric Table</td>
<td>7-13</td>
</tr>
<tr>
<td>7-9</td>
<td>es_perf_timestamp Table</td>
<td>7-13</td>
</tr>
<tr>
<td>7-10</td>
<td>es_perf_sample Table</td>
<td>7-13</td>
</tr>
<tr>
<td>7-11</td>
<td>es_perf_data View</td>
<td>7-14</td>
</tr>
<tr>
<td>7-12</td>
<td>oeschart Mandatory Properties</td>
<td>7-14</td>
</tr>
<tr>
<td>7-13</td>
<td>oeschart Optional Properties</td>
<td>7-15</td>
</tr>
<tr>
<td>8-1</td>
<td>System Flags</td>
<td>8-3</td>
</tr>
<tr>
<td>9-1</td>
<td>Server-Side Rule Expressions</td>
<td>9-4</td>
</tr>
<tr>
<td>9-2</td>
<td>Message Header Attributes</td>
<td>9-5</td>
</tr>
<tr>
<td>9-3</td>
<td>Message Status Attributes</td>
<td>9-5</td>
</tr>
<tr>
<td>9-4</td>
<td>Server-Side Rule Actions</td>
<td>9-6</td>
</tr>
<tr>
<td>10-1</td>
<td>oesbkp Parameters</td>
<td>10-3</td>
</tr>
<tr>
<td>10-2</td>
<td>get_recover_messages Parameters</td>
<td>10-7</td>
</tr>
<tr>
<td>A-1</td>
<td>Options Used to Authenticate a Client to an Oracle Internet Directory Server</td>
<td>A-5</td>
</tr>
<tr>
<td>A-2</td>
<td>Oracle Mail Storage Tablespaces</td>
<td>A-22</td>
</tr>
<tr>
<td>B-1</td>
<td>IMAP and POP Error Messages</td>
<td>B-2</td>
</tr>
<tr>
<td>B-2</td>
<td>SMTP Error Messages</td>
<td>B-4</td>
</tr>
<tr>
<td>B-3</td>
<td>Housekeeper Error Messages</td>
<td>B-7</td>
</tr>
<tr>
<td>B-4</td>
<td>List Server Error Messages</td>
<td>B-7</td>
</tr>
<tr>
<td>B-5</td>
<td>NNTP Error Messages</td>
<td>B-8</td>
</tr>
<tr>
<td>B-6</td>
<td>Virus Scrubber Error Messages</td>
<td>B-11</td>
</tr>
<tr>
<td>B-7</td>
<td>Oracle WebMail Error Messages</td>
<td>B-11</td>
</tr>
<tr>
<td>C-1</td>
<td>Oracle Mail Identifiers</td>
<td>C-1</td>
</tr>
<tr>
<td>C-2</td>
<td>Domain Rights</td>
<td>C-2</td>
</tr>
<tr>
<td>D-1</td>
<td>oesdl File Attributes</td>
<td>D-2</td>
</tr>
<tr>
<td>D-2</td>
<td>oesng Parameters</td>
<td>D-7</td>
</tr>
<tr>
<td>D-3</td>
<td>oespr Parameters</td>
<td>D-9</td>
</tr>
<tr>
<td>D-4</td>
<td>Options Used with the oesuclr Command-Line Utility</td>
<td>D-11</td>
</tr>
<tr>
<td>Section</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D-5</td>
<td>oesuerc Attributes</td>
<td></td>
</tr>
<tr>
<td>D-6</td>
<td>oesctl Commands</td>
<td></td>
</tr>
<tr>
<td>D-7</td>
<td>oeschk Attributes</td>
<td></td>
</tr>
<tr>
<td>E-1</td>
<td>Supported RFCs</td>
<td></td>
</tr>
<tr>
<td>F-1</td>
<td>LDAP Connection Pool Parameters</td>
<td></td>
</tr>
<tr>
<td>F-2</td>
<td>LDAP Connection Retry Parameters</td>
<td></td>
</tr>
<tr>
<td>F-3</td>
<td>Housekeeping Operations</td>
<td></td>
</tr>
<tr>
<td>F-4</td>
<td>Housekeeper General Parameters</td>
<td></td>
</tr>
<tr>
<td>F-5</td>
<td>Housekeeper Debug Parameters</td>
<td></td>
</tr>
<tr>
<td>F-6</td>
<td>IMAP Thread Parameters</td>
<td></td>
</tr>
<tr>
<td>F-7</td>
<td>IMAP Shared Message Flags</td>
<td></td>
</tr>
<tr>
<td>F-8</td>
<td>IMAP Rules and Routing Control Parameters</td>
<td></td>
</tr>
<tr>
<td>F-9</td>
<td>IMAP General Parameters</td>
<td></td>
</tr>
<tr>
<td>F-10</td>
<td>IMAP Debug Parameters</td>
<td></td>
</tr>
<tr>
<td>F-11</td>
<td>NNTP Inbound Thread Parameters</td>
<td></td>
</tr>
<tr>
<td>F-12</td>
<td>NNTP Inbound Access and Routing Control Management Parameters</td>
<td></td>
</tr>
<tr>
<td>F-13</td>
<td>NNTP Inbound General Parameters</td>
<td></td>
</tr>
<tr>
<td>F-14</td>
<td>NNTP Inbound Debug Parameters</td>
<td></td>
</tr>
<tr>
<td>F-15</td>
<td>NNTP Outbound Thread Parameters</td>
<td></td>
</tr>
<tr>
<td>F-16</td>
<td>NNTP Outbound General Parameters</td>
<td></td>
</tr>
<tr>
<td>F-17</td>
<td>NNTP Outbound Debug Parameters</td>
<td></td>
</tr>
<tr>
<td>F-18</td>
<td>POP General Parameters</td>
<td></td>
</tr>
<tr>
<td>F-19</td>
<td>POP Debug Parameters</td>
<td></td>
</tr>
<tr>
<td>F-20</td>
<td>Virus Scrubber General Parameters</td>
<td></td>
</tr>
<tr>
<td>F-21</td>
<td>Virus Scrubber Debug Parameters</td>
<td></td>
</tr>
<tr>
<td>F-22</td>
<td>List Server SMTP Protocol Timeouts</td>
<td></td>
</tr>
<tr>
<td>F-23</td>
<td>List Server DSN Parameters</td>
<td></td>
</tr>
<tr>
<td>F-24</td>
<td>List Server Rules and Routing Control Parameters</td>
<td></td>
</tr>
<tr>
<td>F-25</td>
<td>List Server General Parameters</td>
<td></td>
</tr>
<tr>
<td>F-26</td>
<td>List Server Debug Parameters</td>
<td></td>
</tr>
<tr>
<td>F-27</td>
<td>SMTP Inbound Thread Parameters</td>
<td></td>
</tr>
<tr>
<td>F-28</td>
<td>SMTP Inbound DSN Parameters</td>
<td></td>
</tr>
<tr>
<td>F-29</td>
<td>SMTP Inbound Rules and Routing Control Parameters</td>
<td></td>
</tr>
<tr>
<td>F-30</td>
<td>SMTP Inbound General Parameters</td>
<td></td>
</tr>
<tr>
<td>F-31</td>
<td>SMTP Inbound Debug Parameters</td>
<td></td>
</tr>
<tr>
<td>F-32</td>
<td>SMTP Outbound Thread Parameters</td>
<td></td>
</tr>
<tr>
<td>F-33</td>
<td>SMTP Outbound General Parameters</td>
<td></td>
</tr>
<tr>
<td>F-34</td>
<td>SMTP Outbound Debug Parameters</td>
<td></td>
</tr>
<tr>
<td>F-35</td>
<td>SMTP Inbound DSN Parameters</td>
<td></td>
</tr>
<tr>
<td>F-36</td>
<td>SMTP Inbound Rules and Routing Control Parameters</td>
<td></td>
</tr>
<tr>
<td>F-37</td>
<td>SMTP Inbound General Parameters</td>
<td></td>
</tr>
<tr>
<td>F-38</td>
<td>SMTP Inbound Debug Parameters</td>
<td></td>
</tr>
<tr>
<td>F-39</td>
<td>SMTP Outbound Thread Parameters</td>
<td></td>
</tr>
<tr>
<td>F-40</td>
<td>SMTP Outbound General Parameters</td>
<td></td>
</tr>
<tr>
<td>F-41</td>
<td>SMTP Outbound Debug Parameters</td>
<td></td>
</tr>
<tr>
<td>H-1</td>
<td>Metrics Common to All Oracle Mail Servers</td>
<td></td>
</tr>
<tr>
<td>H-2</td>
<td>POP Server Metrics</td>
<td></td>
</tr>
<tr>
<td>H-3</td>
<td>IMAP Server Metrics</td>
<td></td>
</tr>
<tr>
<td>H-4</td>
<td>SMTP Inbound Server Metrics</td>
<td></td>
</tr>
<tr>
<td>H-5</td>
<td>SMTP Outbound Server Metrics</td>
<td></td>
</tr>
<tr>
<td>H-6</td>
<td>Housekeeper Server Metrics</td>
<td></td>
</tr>
<tr>
<td>H-7</td>
<td>List Server Metrics</td>
<td></td>
</tr>
<tr>
<td>H-8</td>
<td>NNTP Inbound Server Metrics</td>
<td></td>
</tr>
<tr>
<td>H-9</td>
<td>NNTP Outbound Server Metrics</td>
<td></td>
</tr>
<tr>
<td>H-10</td>
<td>Virus Scrubber Server Metrics</td>
<td></td>
</tr>
</tbody>
</table>

xix
Preface

This document contains information necessary for managing and administering Oracle Mail.

This Preface contains these topics:

- Audience
- Documentation Accessibility
- Related Documents
- Conventions

Audience

This manual is intended for system and domain administrators of Oracle Mail.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at

http://www.oracle.com/accessibility/

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.
TTY Access to Oracle Support Services
Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, seven days a week. For TTY support, call 800.446.2398.

Related Documents

For more information, see the following Oracle resources:

**Oracle Collaboration Suite 10g Mail**
- Oracle Mail Application Developer’s Guide
- Oracle Mail Java API Reference

**Oracle Collaboration Suite 10g**
- Oracle Collaboration Suite Administrator’s Guide
- Oracle Collaboration Suite Deployment Guide
- Oracle Collaboration Suite Installation Guide for Solaris Operating System
- Oracle Collaboration Suite Licensing Information
- Oracle Collaboration Suite Security Guide

**Oracle Database**
- Oracle Database Administrator’s Guide
- Oracle Database Backup and Recovery Advanced User’s Guide
- Oracle Database Backup and Recovery Basics

**Oracle Enterprise Manager**
- Oracle Enterprise Manager Advanced Configuration
- Oracle Enterprise Manager Concepts
- Oracle Enterprise Manager Grid Control Installation and Basic Configuration
- Oracle Enterprise Manager Configuration for Oracle Collaboration Suite
- Oracle Enterprise Manager Metric Reference Manual

Conventions

The following text conventions are used in this document:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong></td>
<td>Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.</td>
</tr>
<tr>
<td><em>italic</em></td>
<td>Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.</td>
</tr>
<tr>
<td>monospace</td>
<td>Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.</td>
</tr>
</tbody>
</table>
What’s New in Oracle Mail

This preface describes changes in the administration of Oracle Collaboration Suite 10g Mail (Oracle Mail). In addition to changes in administration, there are also new features for this release of Oracle Mail, and associated administration tasks.

New Oracle Mail administration features include:

- New Features with the Oracle Collaboration Suite 10g Cumulative Patch (10.1.2.2.0)
- Strong Authentication Support
- Oracle Collaboration Suite 10g Web Access Client
- Directory Cache
- Global Address Book
- Message Recovery
- Archiving
- Message Recall
- Routing Control
- End-User Documentation Portal
- Troubleshooting

New Features with the Oracle Collaboration Suite 10g Cumulative Patch (10.1.2.2.0)

The following new features are available after installation of the Oracle Collaboration Suite 10g Cumulative Patch (10.1.2.2.0):

- Display optional name or contact name in system generated messages
  
  Oracle Mail now supports modification of the From: header in generated automatic reply or Notification messages to optionally allow the use of the friendly Displayname field instead of a simple e-mail address.

- Oracle Database 10g JDBC connection pooling has been implemented

- Shared folders listing performance has been improved

- Quota management enhancements
  
  - IMAP support for RFC 2087
  
  - SMTP inbound server rejects messages and connections from users who are over quota (use the oidadmin tool to configure the orclMailQmNoSend parameter)
– New PL/SQL package generates warning messages for users over multiple soft warning limits (use the oidadmin tool to configure the orclMailQmNotifications parameter)

**Strong Authentication Support**
Oracle Mail now supports strong authentication for SMTP, IMAP, and POP.

**Oracle Collaboration Suite 10g Web Access Client**
Oracle Collaboration Suite 10g Web Access Client (Oracle Web Access Client) is a browser-based application that looks, feels, and performs like a desktop application. It provides access to various features of Oracle Collaboration Suite, including:

- E-mail with support for HTML editing
- Personal and shared address books with corporate directory (Global Address Book) integration and support for shared contacts
- TimeBar view of calendar appointments and reminders, with direct access to the Oracle Calendar Web Client for creating and editing meetings

Oracle Web Access Client supports standard Web browsers, including Internet Explorer, Mozilla, and Mozilla Firefox. Your personal preferences are stored on the server so you can access your mail wherever and whenever you want, through a familiar interface on the supported browser of your choice. Work with and manage your information using drag-and-drop functionality, cascading menus, context menus, and resizable panes.

**See Also:** "Managing Oracle Web Access" in Chapter 5 of *Oracle Collaboration Suite Administrator’s Guide* for more information about administering Oracle Web Access Client

**Directory Cache**
The Directory Cache enables faster lookup of directory information when using the Oracle Collaboration Suite 10g WebMail client.

**See Also:** Chapter 5, "Directory Cache" for more information

**Global Address Book**
This new feature for Oracle Collaboration Suite 10g enables Oracle Mail users to use a Suite-wide address book.

**See Also:** "Managing the Address Book" in Chapter 5 of *Oracle Collaboration Suite Administrator’s Guide* for more information

**Message Recovery**
This feature enables recovery of deleted e-mails.

**See Also:** "Recovering Deleted Messages" on page 2-8 for more information

**Archiving**
New archiving policies enable archiving of users’ messages in a third-party storage facility.

**See Also:** "Oracle Mail Archive Policies" on page 8-26 for more information
Message Recall
Message recall enables administrators to locate messages in an Oracle Collaboration Suite 10g Database and to move those messages to a specified folder for further analysis.

See Also: "Message Recall" on page 8-30 for more information

Routing Control
New routing control features reject messages based on e-mail attachments.

See Also: "Oracle Mail Routing Control" on page 8-8 for more information

End-User Documentation Portal
End-user information about the Oracle WebMail client can be found in the End-User Documentation Portal. The End-User Documentation Portal is a set of customizable HTML pages that provide an overview of Oracle Collaboration Suite clients, including Oracle WebMail, as well as information about how to use the client. The End-User Documentation Portal also includes links to the Troubleshooting and FAQ site on the Oracle Technology Network, as well as Oracle Collaboration Suite end-user tutorials.

Administrators can easily host the End-User Documentation Portal. They can customize the default content, add additional content, and administrators can choose which content to show or hide.

The End-User Documentation Portal is included with the installation CD as a ZIP file located in the DVD/Doc/EUDP/eudp.zip directory. For End-User Documentation Portal installation instructions, see Oracle Collaboration Suite Installation Guide for Solaris Operating System.

For information about deploying the End-User Documentation Portal, see "Managing the End-User Documentation Portal" in Chapter 5 of Oracle Collaboration Suite Administrator’s Guide.

Troubleshooting
This guide contains expanded troubleshooting information for a variety of potential Oracle Mail issues.

See Also: Appendix A, "Troubleshooting Oracle Mail"
Introduction to Oracle Mail Administration

Oracle Collaboration Suite 10g Mail (Oracle Mail) is a reliable, scalable, and secure messaging system that uses Oracle Database 10g to store and manage e-mail, voice-mail, and fax messages for your company. Oracle Mail provides message delivery, browser-based clients, and administration utilities by taking advantage of the Oracle core competencies in providing access to, storing, and managing all types of information.

This chapter contains an overview of Oracle Mail flow and of the various tools used to administer Oracle Mail.

This chapter includes the following topics:

- Overview of Oracle Mail
- Overview of Oracle Mail Administration

Overview of Oracle Mail

See Also: "Understanding the Oracle Mail Architecture and Functionality" in Chapter 8 of Oracle Collaboration Suite Deployment Guide for an overview of Oracle Mail

Troubleshooting and diagnostic information can be found in Appendix A, "Troubleshooting Oracle Mail".

Overview of Oracle Mail Administration

There are three levels of administration in Oracle Mail, each with a different set of privileges:

- **System Administrator**: Has privileges to administer and configure the entire Oracle Mail system. System administrators have control over the entire system, including the computer upon which Oracle Collaboration Suite is installed. In addition to being able to shut down the application, system administrators can shut down the computer.

- **Domain Administrator**: Has privileges to administer and configure Oracle Mail within a particular domain. Domain administrators can manage only domain-specific issues. For example, a domain administrator can create and manage users only in whatever domain they control.

- **User**: Has privileges to access, read, and send e-mail and voice-mail messages, and to administer an individual mail account through client-side rules, automated replies, and message management.
This document is intended for system and domain administrators only.

Several tools are available to administrators for Oracle Mail administration. Each tool is used to accomplish different administration tasks, such as user creation, routing control, and system monitoring.

This section includes the following topics:

- Oracle Collaboration Suite 10g WebMail Client
- Oracle Enterprise Manager 10g Application Server Control Console for Collaboration Suite
- Oracle Enterprise Manager 10g Grid Control Console
- Oracle Mail Command-Line Utilities

**Oracle Collaboration Suite 10g WebMail Client**

Use the Oracle Collaboration Suite 10g WebMail (Oracle WebMail) client to manage Oracle Mail objects, including domains, users, distribution lists, aliases, newsgroups and peer servers, filters and routing of mail, and archiving policies.

Access the Oracle WebMail client at either of the following URLs:

http://host_name:port/pls/portal
http://host_name:port/um

Enter the host name of the system upon which Oracle Mail is installed and enter the Oracle Application Server Web Cache port number.

Click the appropriate subtab in the **Administration** tab of the Oracle WebMail client to perform domain, user, list, alias, news, and policy management tasks.

While the **Administration** tab is part of the Oracle WebMail client, it is only available to those users who have been granted privileges of system or domain administrator.

**See Also:**

- Chapter 2, "Managing Oracle Mail Objects" for information about administering Oracle Mail using the Oracle WebMail client
- Chapter 4, "Oracle Collaboration Suite 10g WebMail Client" for information about the Oracle WebMail client
Oracle Enterprise Manager 10g Application Server Control Console for Collaboration Suite

The Oracle Enterprise Manager 10g Application Server Control Console for Collaboration Suite is an administration tool used to configure the various components of Oracle Collaboration Suite. Concerning Oracle Mail, the Application Server Control Console for Collaboration Suite is used to administer the various Oracle Mail servers, such as Housekeeper, POP, and SMTP.

The Application Server Control Console for Collaboration Suite is part of Oracle Enterprise Manager 10g and comes packaged with Oracle Collaboration Suite 10g.

To log in to the Application Server Control Console for Collaboration Suite:

1. Open a Web browser and enter the following URL:
   
   http://host_name:port_number/emd/console

2. Enter a user name and password.

3. Click the name of the Oracle Collaboration Suite Applications tier in the Name column.

4. Click Mail Application in the System Components section to display the Mail Application page.

Listed In the Service Targets section are all of the Oracle Mail servers. Click any one to display the server home page and to manage the chosen server.

See Also:  Chapter 3, "Oracle Mail Servers" for information about administering Oracle Mail servers using Application Server Control Console for Collaboration Suite
Oracle Enterprise Manager 10g Grid Control Console

With Oracle Enterprise Manager 10g Grid Control Console, you can monitor the performance of Oracle Mail and drill down to analyze specific performance metrics. The Grid Control Console provides a convenient grouping and dashboard summarization of Oracle Mail status and performance.

See Also: Chapter 7, "Monitoring Oracle Mail" for information about administering Oracle Mail using Oracle Enterprise Manager 10g Grid Control Console

Oracle Mail Command-Line Utilities

An administrator can employ various utilities from the command line to perform administrative tasks.

See Also: Appendix D, "Oracle Mail Command-Line Reference" for a list of Oracle Mail command-line utilities
Managing Oracle Mail Objects

This chapter contains information necessary for managing Oracle Mail objects, including domains, users, distribution lists, newsgroups, and aliases. Additionally, it discusses the delegation of certain administration tasks.

Both system and domain administrators have the necessary privileges to manage Oracle Mail objects, although domain administrators are limited to specific domains.

This chapter includes the following topics:

- Managing Oracle Mail Users
- Managing Oracle Mail Domains
- Managing Distribution Lists
- Managing Aliases
- Managing News Objects

Managing Oracle Mail Users

Using the Oracle WebMail client, you can perform user management tasks, such as adding, removing, and modifying e-mail users.

---

Notes:

- After a successful installation of Oracle Mail, a user with full administrative privileges (a system administrator) must be created using Oracle Delegated Administration Services prior to any user being provisioned or deprovisioned using Oracle WebMail, and also prior to creating any domains.

- Base users having multiple mail IDs cannot be managed from the centralized provisioning framework in Oracle Collaboration Suite 10g. Users that have multiple mail IDs cannot be managed from Oracle Delegated Administration Services; Oracle WebMail must be used to manage such users.

---

See Also:  "oesucr" on page D-11 for information about managing users from the command line

This section includes the following topics:

- Adding E-mail Users
Adding E-mail Users

Notes:

- A base user must exist in Oracle Internet Directory before an e-mail account can be created. If the intended e-mail user has no entry in the directory, a message displays with a link directing you to the directory’s Oracle Delegated Administration Services page. You can create and provision the user there.

- Once users are created using Oracle Delegated Administration Services, it is not necessary to re-create them using the Oracle WebMail client.

- If the Oracle Collaboration Suite Database was down when user provisioning occurred (whether from Oracle Delegated Administration Services or Oracle WebMail), the Oracle Mail servers and Oracle WebMail will create the folders in the Oracle Collaboration Suite Database for the user when they receive a message or when the user logs in.

To add e-mail users:

1. Open the Oracle WebMail client.

   **See Also:** "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client

2. Click the Administration tab.

3. Click the User subtab. The Add E-mail Service to User page displays by default.

4. Select a domain from the E-mail Domain list.

5. Click Select to display the following list of user attributes for an e-mail account:

   - **E-mail User Account Name**: Enter an account name for the user, such as `firstname.lastname`.
Managing Oracle Mail Users

Managing Oracle Mail Users

Managed by Oracle Mail Users

1. Base Subscriber: Select a domain from the list.
   This is the Oracle Internet Directory realm under which the base users are provisioned. The Oracle Internet Directory realm can be different than the domain of the e-mail address. For example, base users can be provisioned under the realm `dc=foo,dc=com`; however, the domain of the e-mail address could be `us.foo.com` or `sales.foo.com`. Use this field to select the Oracle Internet Directory realm under which the base user is provisioned to enable Oracle WebMail to ascertain with which base user to associate this user ID.

2. Collaboration Suite Database: Select an information store from the list.

3. E-mail Quota (MB): Enter a number to represent the number of megabytes (MB) of e-mail storage assigned to this user.
   1048576 MB is the maximum quota that can be specified in this field.
   Enter 0 to give a user unlimited quota.

4. Role: Specifies the permissions of a particular user.

5. Archive Policy: Select an archive policy to assign to the user.
   Archive policies can be applied to any e-mail user so that all of the user's incoming and outgoing e-mail messages are stored in a third-party storage facility. If you do not want to associate the user with an archive policy, leave this option blank. If archive policies are created later, you can modify archive policy application for a user.
   If no archive policies exist, this field will not be displayed.

6. Click Add to add the user to the domain or Cancel to return to the previous page.

A Word About Quota

Two quota values can be set for users: user-quota and voice-quota. When usage reaches user-quota, it means that the sum of e-mails and voice mails is equal to the user-quota value. The voice-quota is an additional buffer provided to users so that voice-mail delivery is not affected when users reach their quota.

Note: Only US-ASCII characters are accepted in this field. Spaces in account names are converted to periods (.).

Account names containing the following non-US-ASCII characters are not supported:

ä  Ä  ö  Ö  ü  Ü  ß

See Also: "Overview of Oracle Mail Administration" on page 1-1 for information about the various administrator roles

See Also: "Oracle Mail Archive Policies" on page 8-26 for more information about archive policies
All e-mails and voice mails are delivered to users as long as they are under user-quota. Once users reach their user-quota, e-mails are held in the system and not delivered. In addition, users cannot save new messages in the server folders when they reach user-quota. For example, saving a copy of outgoing messages to the Sent folder is not allowed. The IMAP server informs the client that the user is over quota when the user tries to save new outgoing mail.

However, voice-mail delivery continues as long as total usage is under the user-quota plus voice-quota value. For example, if user-quota is 50 MB and voice-quota is 20 MB, e-mail delivery stops after the usage is 50 MB, but voice-mail delivery continues until user-quota and voice-quota reach 70 MB.

E-mail messages are received as usual when a user is over quota. They are stored in exactly the same tables but there is a flag that sets the status of the message so that it cannot be viewed by the user. The system will continue to receive messages until the disk space fills to capacity.

The message ID of any message received while a user is over quota is set to a negative number to indicate that it was received while the user was over quota. Once the user is back under quota, the message ID is set to a positive number and the messages can then be retrieved.

When users clean up their accounts and are under the user-quota and user-quota plus voice-quota values, e-mail and voice-mail delivery resume.

**Modifying E-mail User Attributes**

To modify the attributes of an existing user:

1. Open the Oracle WebMail client.

   See Also: "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client

2. Click the Administration tab.

3. Click the User subtab.

4. Click Modify User.

5. Enter the user ID in the Search Criteria field. Enter an asterisk ( *) to perform a wildcard search.

6. Select the user’s domain from the Domain list.

7. Click Go.

8. Click Go.

9. Click the name of the user in the E-mail User Account Name column to modify attributes for that user.

9. Modify the following attributes, as necessary:

   - **E-mail User Account Name**: The e-mail user account address. This information cannot be modified.

   - **Collaboration Suite Database**: Global database name of the information storage database containing this user’s folders and messages. This information cannot be modified.

   - **E-mail Quota (MB)**: This is the maximum amount of e-mail messages, measured in megabytes, that an individual can store on the mail store. If you enter 0, a user has unlimited quota.
• **Additional Voice Mail Quota (MB):** This is the maximum amount of voice mail messages, measured in megabytes, that an individual can store on the mail store. If you enter 0, a user has unlimited quota.

  This quota is in addition to the e-mail quota. For example, if a user has 40 MB of e-mail quota and 10 MB of voice mail quota, the user has a total of 50 MB of message storage. While e-mail quota cannot exceed the amount given, voice-mail quota can exceed its given amount up to the total amount of message storage.

  If either of these quotas is set to 0, a user has unlimited overall storage. However, if the voice-mail quota is set to 0, and e-mail quota is set to a finite value, such as 40 MB, when the voice-mail quota reaches 40 MB, the user will no longer be able to receive e-mail.

• **User State:** Choose either **Active** or **Inactive** from the **User State** list.

---

**Notes:**

An inactive user cannot access the mail system at all. However, messages sent to an inactive account are stored in the Oracle Collaboration Suite Database and can be accessed if the account is reactivated.

If the user state is changed to inactive and if the user owns mailing lists or newsgroups, Oracle WebMail displays a warning message listing the names of distribution lists or newsgroups owned by the user. This warning message informs the administrator that because the owner of these lists or newsgroups is inactive, some administrative activities handled by the owner will not be possible for these distribution lists or newsgroups.

---

• **Auto Reply Mode:** Select from the list one of the following automatic reply choices:

  - Reply with original message, along with "Auto Reply Message" below
  - Reject sender's e-mail
  - Vacation, reply only one e-mail with each sender
  - Reply each incoming e-mail with "Auto Reply Message" below

• **Auto Reply Text:** Enter any text to be included in automatic replies.

• **Auto Reply Expiration:** Enter a date at which automatic reply will cease.

• **Forward E-mail Address:** Specify an address to which messages will be forwarded.

  If an e-mail address is entered here, an `orclforwardaddress` entry is created in Oracle Internet Directory, and all messages are forwarded to the specified address. No messages are delivered to the original recipient's Inbox.

  In order for messages to continue being delivered to the user’s Inbox, a filter must be created to accomplish this task.

• **Text Indexing:** When enabled, Oracle Mail servers index messages as soon as possible after the messages enter the system so that the user can search the Oracle Collaboration Suite Database and return results in seconds. This task is performed by the Housekeeper server.
Managing Oracle Mail Users

**Role**: Specifies the permissions that a particular user has:

- **System Administrator**: A system administrator will have permissions to administer and configure the entire Oracle Mail system.
- **Domain Administrator**: A domain administrator will have permissions to administer and configure Oracle Mail within a particular domain.
- **User**: A user will have permissions only to access, read, and send e-mail, fax, and voice-mail messages.

**Archive Policy**: Select an archive policy to assign to the user.

Archive policies can be applied to any e-mail user so that all of the user’s incoming and outgoing e-mail messages are stored in a third-party storage facility. If you do not want to associate the user with an archive policy, leave this option blank. If archive policies are created later, you can modify archive policy application for a user.

If no archive policies exist, this field will not be displayed.

**See Also**: "Configuring Housekeeper Tasks" on page 3-24 for more information about index synchronization

**Setting Default New User Attributes**

All new e-mail users created in a particular domain are given default attributes that can later be changed.

To set the default attributes of new users in a particular domain:

1. Open the Oracle WebMail client.

   **See Also**: "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client

2. Click the **Administration** tab. The Default New User page in the **Domain** subtab displays by default.

3. Select an installation from the **Installation** list.

4. Select a domain from the **Domain** list.

5. Click **Submit**.
6. Modify the following attributes:

- **Collaboration Suite Database**: Select an information store from the list where each user's mail is to be stored.

- **E-mail Quota (MB)**: Enter a number to represent the number of megabytes of e-mail storage assigned to each user.
  
  Enter 0 to give a user unlimited quota.

- **Additional Voice Mail Quota (M)**: Enter a number to represent the number of megabytes of voice-mail storage assigned to each user.

- **User State**: Defines the user as active or inactive. If **User State** is set to **Active**, the user has full use of the mail protocols that are exposed by the implementation.
  
  A message sent to an inactive user will result in a **delivery status notification (DSN)** being sent to the sender of the message.

- **Text Indexing**: When text indexing is enabled, e-mail messages are indexed for searching.

- **Role**: Defines the user as either a regular user, a system administrator, or a domain administrator.

  **See Also**: "Overview of Oracle Mail Administration" on page 1-1 for more information about system and domain administrators

- **Number of Messages Displayed in Oracle WebMail**: Specifies the number of message headers displayed at one time on the Oracle WebMail client. For example, you can specify to display 20 messages at a time.

- **Display Headers (Oracle WebMail)**: Select **Full** from the list to display Oracle WebMail headers in detail.

- **Archive Policy**: Select an archiving policy to assign to new users.
  
  Archive policies can be applied to any e-mail user so that all of the user's outgoing and incoming e-mail messages are kept in an archive. If no archive policies exist or you do not want to associate the user with an archive policy, leave this option blank. If archive policies are created later, you can modify archive policy application for a user.

  **See Also**: "Oracle Mail Archive Policies" on page 8-26 for more information about archive policies

7. Click **Submit** to apply the changes.
Removing E-mail Users

Notes:

- When an e-mail user is removed, any shared folders and public shared folders owned by that user are also deleted; however, user data stored in the Oracle Collaboration Suite Database is not removed.

- If the user being deleted owns a distribution list or newsgroup, the user deletion will not proceed. An error message displays that will contain the names of the distribution lists or newsgroups owned by this user. The administrator must change the ownership of these lists and newsgroups for deletion of the user to succeed.

See Also: "oesucr" on page D-11 for information about removing a user’s data from the Oracle Collaboration Suite Database

To remove individual e-mail users:

1. Open the Oracle WebMail client.

   See Also: "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client

2. Click the Administration tab.

3. Click the User subtab.

4. Click Remove User.

5. Enter the user ID in the Search Criteria field. Enter an asterisk (*) to perform a wildcard search.

6. Select the user's domain from the Domain list.

7. Click Go.

8. Select the user you want to remove.

9. Click Remove to display a confirmation page.

10. Click Return to User Management.

Recovering Deleted Messages

Using this feature, you can recover deleted messages for users using the LogMiner feature of the Oracle Collaboration Suite 10g Database.
To recover deleted messages:

1. Set up LogMiner to recover deleted messages as described in "Setting Up LogMiner to Recover Mail" on page 3-26.
2. Open the Oracle WebMail client.

   See Also: "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client.
3. Click the Administration tab.
4. Click the User subtab.
5. Click Recover E-mail to display the Recover E-mail page.
6. Enter information in the following fields:
   - **E-mail Account Name**: Enter the fully qualified e-mail address of the user for whom you are recovering messages.
   - **Sender**: Enter the fully qualified e-mail address of the sender if the user is searching for deleted messages by sender.
   - **Subject**: Enter a string of text to search the Subject field of deleted messages.
   - **Date Range From**: Enter a date from which to begin searching messages.
   - **Date Range To**: Enter a date at which to end searching messages.

   If more than one field is given for a search, the search is performed on all the criteria. For example, if the **Date Range From**, **Date Range To**, and **Sender** fields contain values, the search returns deleted messages where the **Date Range From** is \texttt{mm/dd/yyyy} (or \texttt{dd/mm/yyyy}, depending upon your locale), the **Date Range To** is \texttt{mm/dd/yyyy} (or \texttt{dd/mm/yyyy}, depending upon your locale), and the **Sender** is \texttt{sender}.

   The **Subject** and the **Sender** fields are used to perform regular POSIX and Unicode expression matching.
7. Click **Search** to display a list of recoverable messages.

**Note**: Recovering deleted messages from the redo log is an expensive operation because it involves searching the redo log file with the LogMiner utility.

The time it takes to recover deleted messages is a function of:

- The size and number of the redo logs being searched
- The number of messages to be recovered
- The size of the MIME message

The greater the number of messages to be recovered, the longer the operation takes. The operation can take from several minutes to several hours, depending upon the preceding factors. If a large number of messages must be recovered, Oracle recommends running LogMiner during off-peak hours.

You must run Housekeeper server before you can recover deleted messages.
8. The list of recoverable messages includes the following information:

- **Sender**: Fully qualified e-mail address of the sender of the message
- **Date**: Date that the message was sent
- **Subject**: Contents of the Subject field of the message
- **Database Instance ID**: The system identifier (SID) of the Oracle instance (especially applicable in an Oracle Real Application Clusters environment) on which the message was deleted, and identifies the redo log file name from which the deleted message must be recovered
- **Redo Log Number**: The redo log number identifies the archived redo log file from which the deleted message is to be recovered.
- **Available on Disk?**: If checked, the redo log file from which messages are recovered is online. If it is offline, the redo log file cannot be read and the messages cannot be recovered.

**Note**: If the **Database Instance ID** and **Redo Log Number** both have a 0 value for a message, and the **Available On Disk?** column is checked for that message, this message can be recovered. In this case, the 0 values indicate that this message has not yet been through the garbage collection process of the Housekeeper server.

9. Select any number of messages and click **Recover**. The same message can be recovered multiple times if the message appears in the recoverable messages list based on the search criteria.

10. Click **OK** when the confirmation page displays. Recovered messages return to the user’s inbox. If an error page displays, no messages were recovered. If a warning page displays, some messages were recovered, while others were not.

The SMTP server in the Oracle Internet Directory service registry is used to deliver the recovered messages to the user’s Inbox. The received date of the recovered message is changed to the date that the recovered message is received.

### Managing Oracle Mail Domains

Domains identify e-mail addresses as being from a specific company. E-mail **domains** can have subdomains that can be administered separately even if they are on the same system. The advantages to administering subdomains on the same system separately are:

- Convenience in accommodating subdomains with different maintenance schedules, which is typical for subdomains in different geographic regions
- Ease of administering subdomains with different default attributes, which is common for subdomains belonging to different organizations

Using the Oracle WebMail client, an administrator can perform domain management tasks, such as modifying default attributes for new users, managing domain settings, and creating domains.

**Note**: Only system administrators can create domains. Ensure that a system administrator has been created prior to attempting to create domains.
This section includes the following topics:

- Creating Domains
- Modifying Domain Settings

Creating Domains

Oracle Mail domains are created using the Oracle WebMail client. The base domain is created automatically during installation of the Oracle Collaboration Suite Infrastructure. E-mail domain names can be different than the base domain. For example, you can create e-mail subdomains of company.com named a.company.com, b.company.com, and c.company.com.

To create additional domains:

1. Open the Oracle WebMail client.

   **See Also:** "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client

2. Click the Administration tab. The Domain subtab displays by default.

3. Click Create Domain.

   **Note:** If you do not have system administrator privileges, this link will not display in the user interface (UI).

4. Click the name of the installation for which you want to create the new domain.

5. Select a domain from the Parent Domain list.

6. Enter the new domain name in the Domain field.

7. Click Create Domain to display the Domain Settings page.

8. Click Submit to display a confirmation page.

Modifying Domain Settings

**Note:** Preferences modified for a domain apply only to entries created after the modifications. For example, if the default mail quota for the oracle.com domain is changed to 60 megabytes (MB), only users newly created in that domain have the new 60 MB quota. Existing users in that domain retain their old mail quota.

To modify domain settings:

1. Open the Oracle WebMail client.

   **See Also:** "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client

2. Click the Administration tab. The Domain subtab displays by default.

3. Click Domain Settings.
4. Select an installation from the **Installation** list.
5. Select a domain from the **Domain** list.
6. Click **Submit**.
7. Modify domain attributes in the following fields, as necessary:
   - **Location in Public Namespace**: A valid distinguished name within the list server to which distribution lists are synchronized. This specifies the distinguished name of the **Lightweight Directory Access Protocol (LDAP)** container in Oracle Internet Directory, which contains all distribution lists in a public namespace for client lookup.
     
     For example:
     ```
     cn=List,dc=foo,dc=com,cn=um_system,cn=EMailServerContainer,cn=Products,cn=OracleContext
     ```

   - **Objectclasses for Creation in Public Namespace**: Enter a list of LDAP objectclasses used while creating distribution lists in the public namespace. The list of LDAP objectclasses must include the **groupofnames** or **groupofuniquenames** parameter.
     
     For example:
     ```
     groupofuniquenames=domainRelatedObject
     ```

   - **Naming Attribute for Creation in Public Namespace**: Contains the naming attribute to be used while creating distribution lists in the public namespace.
     
     For example:
     ```
     domain
     ```

   - **Flashback Mail Recovery**: Enables or disables **flashback mail recovery** for e-mail users. This attribute does not affect the flashback mail recovery capability for administrators using the PL/SQL interface.

8. Click **Submit** to apply the changes.

---

**Managing Distribution Lists**

Distribution lists are managed using the Oracle WebMail client. Management tasks include:

- Create, delete, or show **distribution lists** or list members
- Modify distribution list properties
- Show all distribution lists to which a member belongs

Additionally, routing control of incoming mail and certain List Server parameters configurable using Oracle Enterprise Manager 10g Application Server Control Console can be used to further manage how messages are delivered to distribution lists. In some cases, distribution lists can contain many hundreds or even thousands of users, which could potentially interfere with e-mail service.
Limits to the number of recipients in an e-mail envelope (this is applicable to all e-mail traffic, not just messages sent to distribution lists) can be established, in addition to batching recipients and setting a number of e-mails that can be processed concurrently.

See Also:
- "Configuring Advanced Routing Control Settings for Incoming Mail" on page 8-16
- "Oracle Mail List Server" on page F-25 for a list of List Server parameters

This section discusses various management tasks and provides distribution list attributes and parameters.

See Also: "oesdl" on page D-2 for information about managing distribution lists from the command line

This section includes the following topics:
- Setting Default Distribution List Attributes
- Distribution List Parameters
- Creating a Distribution List
- Modifying Distribution List Properties
- Modifying Default Distribution List Parameter Values
- Deleting a Distribution List
- Managing Distribution List Members
- Showing All Distribution Lists to Which a User Subscribes

Setting Default Distribution List Attributes

Distribution list attributes include:
- Group type, described in Table 2-1
- Subscription type, described in Table 2-2
- Posting type, described in Table 2-3

To set the default attributes of new distribution lists in a particular domain:

1. Open the Oracle WebMail client.

   See Also: "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client

2. Click the Administration tab.
3. Click Default New List in the Domain subtab.
4. Select an installation from the Installation list.
5. Select a domain from the Domain list.
6. Click Submit.
7. Modify the following attributes, described in Table 2-4:
Managing Distribution Lists

- Collaboration Suite Database
- Owner
- Topic
- Editor's List
- Moderator's List
- Auto Reconfirm
- Group Type
- Group Subscription Type
- Post Type
- Maximum Message Size
- Invite Text
- Information Text
- Merge Tag
- Edit/View Member Privilege
- Enable Digests
- Enable Bounce Processing

---

**Note:** For the Group Type, Group Subscription Type, Post Type, Edit/View Member Privilege, Enable Digest, and Enable Bounce Processing parameters, in a domain hierarchy, if any of these parameters are set in any parent domain, and the child domain does not have any values set, the value of the attribute is inherited from the parent domain.

For example, if the foo.com domain has **Edit/View Member Privilege** set as Members, Owner, Provers, Moderators, Editors, and if us.foo.com, a child domain of foo.com, does not have a value set for this parameter, Oracle WebMail displays the settings of the parent domain, if available.

If you clear the value in us.foo.com by selecting the blank option from the **Edit/View Member Privilege** list and save your settings, the next time you view, you will see that the settings for this parameter are those of the parent domain, if there are any present for the parent domain.

Also, if foo.com does not have a value for one of these parameters, but the .com default distribution list settings do have values set, the us.foo.com default distribution list settings will reflect that, if it does not have values of its own.

If in the entire parent hierarchy of us.foo.com, this value is blank, Oracle WebMail will display a blank value.

---

A distribution list group type is set by the distribution list owner during list creation and controls distribution list attributes. Examples of distribution list attributes include what headers are included on mail delivered to a distribution list, or whether the list is
Managing Distribution Lists

moderated. The distribution list owner can change the group type after the list is created.

Table 2–1 describes the different group types.

Table 2–1  Distribution List Group Types

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Announcement</td>
<td>Automatic replies or DSNs are not delivered to the sender. This group type is useful for making announcements to a group of recipients where the sender is not concerned with knowing if a message was delivered to individual recipients or if a recipient has set an automatic reply.</td>
</tr>
<tr>
<td>Discussion</td>
<td>Distribution list group type used for discussions among a group of people. Messages posted to this distribution list have a Reply-To header added, which is set to the distribution list mail ID itself. Thus, replying to such a message will send the reply back to the distribution list. Automatic replies and DSNs are delivered to the sender of a message (unless bounce processing is enabled for the list, in which case automatic replies or DSNs are sent to a special address list_ID-bounce@domain and are processed by the bounce processor in the List Server).</td>
</tr>
<tr>
<td>Edited</td>
<td>Distribution list group type that controls who can post mail to the list. Only users from a configurable list of editors can post mail to this list. Automatic replies and DSNs are delivered to the sender of a message (unless bounce processing is enabled for the list, in which case automatic replies or DSNs are sent to a special address listid-bounce@domain and are processed by the bounce processor in the List Server).</td>
</tr>
<tr>
<td>Moderated</td>
<td>All messages posted to this distribution list group type are sent to list moderators (specified in the Group Moderators List attribute). At least one moderator must approve any message within 3 days for the message to be posted to the distribution list. Automatic replies and DSNs are delivered to the sender of a message (unless bounce processing is enabled for the list, in which case automatic replies or DSNs are sent to a special address listid-bounce@domain and are processed by the bounce processor in the List Server).</td>
</tr>
</tbody>
</table>

Subscription types control who can subscribe to a distribution list, as described in Table 2–2.

Note: These subscription types do not apply to external distribution lists. For more information about external distribution lists, see “External Distribution Lists” on page 3-35.

Table 2–2  Distribution List Subscription Types

<table>
<thead>
<tr>
<th>Type</th>
<th>Subscription</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open</td>
<td>No approval required; any user can subscribe.</td>
</tr>
<tr>
<td>Restricted</td>
<td>The list owner, or one member of a list of appointed approvers, must approve any request to subscribe to this distribution list.</td>
</tr>
<tr>
<td>Closed</td>
<td>Subscription requests are not processed. Users can only subscribe by invitation of the distribution list owner.</td>
</tr>
</tbody>
</table>

Table 2–3 describes the distribution list posting type, which restricts whether nonmembers can post messages to the list.
Additionally, a server-side rule can be created to restrict certain users from posting messages to a particular list.

**See Also:** Chapter 9, "Oracle Mail Server-Side Rules" for more information about creating server-side rules

### Distribution List Parameters

Distribution lists are created using the Oracle WebMail client. When a new list is created, various parameters are set, giving the new list various attributes, such as archiving and posting attributes.

*Table 2–4* describes distribution list parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Acceptable Values</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distribution Name</td>
<td>E-mail address of the new distribution list.</td>
<td>Any valid e-mail address</td>
<td>None</td>
</tr>
<tr>
<td>Owner</td>
<td>The e-mail address of the person who is to own the list.</td>
<td>A fully qualified e-mail address, such as <code>user@foo.com</code></td>
<td>None</td>
</tr>
<tr>
<td>Maximum Message Size (bytes)</td>
<td>The maximum allowable size of a message posted to the distribution list. Messages exceeding this value are rejected. Use a value of 0 to indicate unlimited size.</td>
<td>Any integer greater than or equal to 0</td>
<td>None</td>
</tr>
<tr>
<td>Topic</td>
<td>Single-line phrase describing the topic of discussions on this list.</td>
<td>String of text</td>
<td>None</td>
</tr>
<tr>
<td>Invite Text</td>
<td>Multiline text sent in e-mail to users invited by a list owner to join the list.</td>
<td>String of text</td>
<td>None</td>
</tr>
<tr>
<td>Editor’s List</td>
<td>List of users (e-mail addresses) for the editors of the list.</td>
<td>A fully qualified e-mail address, such as <code>user@foo.com</code></td>
<td>None</td>
</tr>
<tr>
<td>Moderator’s List</td>
<td>List of users (e-mail addresses) who are moderators of the list.</td>
<td>A fully qualified e-mail address, such as <code>user@foo.com</code></td>
<td>None</td>
</tr>
</tbody>
</table>

**Note:** These posting types do not apply for edited lists.
**Table 2–4 (Cont.) Distribution List Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Acceptable Values</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Group Approvers</strong></td>
<td>List of users (e-mail addresses) who are the subscription approvers of the list. Applied only if the distribution list subscription type is Restricted.</td>
<td>A fully qualified e-mail address, such as <a href="mailto:user@foo.com">user@foo.com</a></td>
<td>None</td>
</tr>
<tr>
<td><strong>Information Text</strong></td>
<td>Multiline owner-provided descriptive text about the list.</td>
<td>String of text</td>
<td>None</td>
</tr>
<tr>
<td><strong>Merge Tag</strong></td>
<td>A tag used for specifying mail merge and scheduler tags, enabling a list owner to support mail merge or scheduled mail delivery.</td>
<td>Select an Oracle Collaboration Suite Database from the list</td>
<td>None</td>
</tr>
<tr>
<td><strong>Collaboration Suite Database</strong></td>
<td>If specified, the Oracle Collaboration Suite Database on which the messages addressed to this list are queued until the List Server processes them. If not, then messages addressed to this list are queued wherever they are received.</td>
<td>Select an Oracle Collaboration Suite Database from the list</td>
<td>None</td>
</tr>
<tr>
<td><strong>Auto Reconfirm</strong></td>
<td>If set to True, requests to suspend or resume delivery from a distribution list trigger an e-mail from the list requiring a reply e-mail from the requester confirming the action. The default False value is recommended, because in the case of a suspend request, the requester may be unaware of the need to reconfirm the request and no longer be offline when the reconfirmation e-mail is delivered. In this case, suspension from the distribution list will not occur.</td>
<td>True or False</td>
<td>False</td>
</tr>
<tr>
<td><strong>Group Type</strong></td>
<td>Type of distribution list, as described in Table 2–1, “Distribution List Group Types”.</td>
<td>Discussion, Announcement, Edited, or Moderated</td>
<td>Discussion</td>
</tr>
<tr>
<td><strong>Group Subscription Type</strong></td>
<td>Type of subscription control placed on the list, as described in Table 2–2, “Distribution List Subscription Types”.</td>
<td>Open, Restricted, or Closed</td>
<td>Open</td>
</tr>
<tr>
<td><strong>Post Type</strong></td>
<td>Type of posting control placed on the list, as described in Table 2–3, “Distribution List Posting Types”.</td>
<td>Open or Subscriber</td>
<td>Open</td>
</tr>
<tr>
<td><strong>Unsubscribe Not Allowed</strong></td>
<td>If TRUE, allows only the list owner to unsubscribe a member from a list. If FALSE, anyone can unsubscribe.</td>
<td>True or False</td>
<td>False</td>
</tr>
<tr>
<td><strong>List State</strong></td>
<td>State of the list: active, inactive, or migrating:</td>
<td>Active, Inactive, or Migrating</td>
<td>Active Migrating</td>
</tr>
<tr>
<td><strong>Enable Digests</strong></td>
<td>If selected, enables the digest feature, in which posts to a list are held and only one e-mail message is sent to a list member at a member-specified frequency, containing all the posts to the list during the interim.</td>
<td>Not applicable (NA)</td>
<td>None</td>
</tr>
<tr>
<td><strong>Enable Bounce Processing</strong></td>
<td>If selected, when a DSN is received from any member of a list a specific number of times, the list owner receives a notification and can then unsubscribe the member from the list.</td>
<td>NA</td>
<td>None</td>
</tr>
</tbody>
</table>
### Table 2–4 (Cont.) Distribution List Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Acceptable Values</th>
<th>Default Value</th>
</tr>
</thead>
</table>
| Edit/View Member Privilege | Select from the list which type of user has the privilege to view and edit list members. | ■ Owner<br>
 ■ Owner, Approver, Moderator, Editor<br>
 ■ Members, Owner, Approver, Moderator, Editor<br>
 ■ All | Members, Owner, Approver, Moderator, Editor | | |
| Restrict Membership to Group’s Domain | If Yes, restricts distribution list membership only to those users within the domain of the distribution list. If No, users from outside the domain of the distribution list can be members. | Yes or No | Yes |
| Send Notification On Subscribe/Unsubscribe To | Indicates who receives notifications upon a successful subscription or unsubscription | None, Only Member, Only Owner, and Member | Owner and Member |
| Members from OiD Group | Select this option to tie the membership of the list to a group created in Oracle Internet Directory. All members of the Oracle Internet Directory group will be members of the new distribution list. Whenever members are added to the group in Oracle Internet Directory, those members will be automatically added to the distribution list. | NA | None |
| OiD Group | Select an Oracle Internet Directory group from the list. | NA | None |

See Also: Chapter 9, "Dynamic and Static Groups in Oracle Internet Directory" in Oracle Internet Directory Administrator’s Guide for more information about groups in Oracle Internet Directory.
Managing Distribution Lists

Creating a Distribution List

To create a list:

1. Open the Oracle WebMail client.

   See Also: "Managing Distribution Lists" on page 2-12 for more information

2. Click the Administration tab.

3. Click the List subtab.

4. Click Create a new list in the Distribution List Management section.

5. Select the domain from the Select Domain list.

6. Select Quick or List Server from the Distribution List Type list. The distribution list type defines the distribution list type.

7. Click Go.

8. Enter the information in the corresponding fields, as described in Table 2–4, "Distribution List Parameters".

9. Click Create.

 NA In the Suppress Headers in posts section, check the header types to be suppressed in mails distributed to the list.

 NA In the Archive List Properties section, give the following information:

   - Group Has Archive: If set to True, enter an archive name in the Archive Name field in the form ListArchive.list_name.

   - If you choose to archive list information, select either Create a new archive on newsstore or Use existing archive.

   - Select from the Access Control list whether anyone can view archived messages, or restrict access to list members only

 NA In the External List Properties section, select True from the Group is External list to make the list available externally.

 In the External Procedure field, enter a name for the external procedure used to resolve the list, in the following format:

 schema-name.procedure-name

 See Also: "External Distribution Lists" on page 3-35 for more information

Table 2–4 (Cont.) Distribution List Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Acceptable Values</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NA</td>
<td>In the Suppress Headers in posts section, check the header types to be suppressed in mails distributed to the list.</td>
<td>NA</td>
<td>None</td>
</tr>
<tr>
<td>NA</td>
<td>In the Archive List Properties section, give the following information:</td>
<td>NA</td>
<td>False</td>
</tr>
<tr>
<td></td>
<td>- Group Has Archive: If set to True, enter an archive name in the Archive Name field in the form ListArchive.list_name.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- If you choose to archive list information, select either Create a new archive on newsstore or Use existing archive.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Select from the Access Control list whether anyone can view archived messages, or restrict access to list members only</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NA</td>
<td>In the External List Properties section, select True from the Group is External list to make the list available externally.</td>
<td>NA</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>In the External Procedure field, enter a name for the external procedure used to resolve the list, in the following format:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>schema-name.procedure-name</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

See Also: "Managing Distribution Lists" on page 2-12 for more information
Modifying Distribution List Properties

To edit list properties:

1. Open the Oracle WebMail client.

   See Also: "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client

2. Click the Administration tab.

3. Click the List subtab.

4. Click Edit/View List properties in the Distribution List Management section.

5. Select the domain of the list from the Select Domain list.

6. In the Search Criteria field, enter the list name, or enter an asterisk (*) to display all available lists.

7. Click the name of the list you want to modify.

8. Edit the properties you want to change.

9. Click Modify.

Modifying Default Distribution List Parameter Values

An administrator can modify the default distribution list parameter values one sees when creating a new list. Modifying these parameter values is done at the domain level.

To modify default list parameter values:

1. Open the Oracle WebMail client.

   See Also: "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client

2. Click the Administration tab.

3. Click the Domain subtab.

4. Click Default New List.

5. Select the installation from the Installation list.

6. Select the domain from the Domain list and click Submit to display the Default New List Attributes page.

7. Enter the parameter values you want to set as defaults.

   See Also: Table 2–4, "Distribution List Parameters" for a comprehensive list of distribution list parameters and descriptions for each

8. Click Submit to commit the changes, or use your browser’s back button to return to the previous page.
Deleting a Distribution List

To delete a list:

1. Open the Oracle WebMail client.
   
   See Also: "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client

2. Click the Administration tab.
3. Click the List subtab.
4. Click Delete list(s) in the Distribution List Management section.
5. In the Search Criteria field, enter the list name, or enter an asterisk (*) to display all available lists.
6. Select the domain of the list from the Select Domain list.
7. Click Go.
8. Select the list you want to delete.
9. Click Delete.
10. Click Return to Distribution List Management to return to the Distribution List Management page.

Managing Distribution List Members

To add or delete users from a distribution list:

1. Open the Oracle WebMail client.
   
   See Also: "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client

2. Click the Administration tab.
3. Click the List subtab.
4. Click Membership Management.
5. Click Add/Remove member(s) to display the Choose a List to Manage Member page.
6. In the Search Criteria field, enter the list name, or enter an asterisk (*) to display all available lists.
7. Select the domain of the list from the Select Domain list.
8. Click Go to display the Add/Remove member(s) page.
9. Click the list in the Name column you want to manage.
10. Enter or remove fully qualified e-mail address or aliases in the following fields:
    - Members (user): Users on this system that are members of this list. Select users from the User(s) list and use the Move, Move All, Remove, and Remove All buttons to move users to and from the Selected User(s) list.
    - Members (list): Other lists that are members of this list
Managing Aliases

- **Members (alias)**: Aliases that are members of this list
- **Members (foreign)**: Users foreign to this system who are members of this list

11. Click **Modify** to apply changes.
12. Click **Cancel** to return to the Distribution List Management page.

### Showing All Distribution Lists to Which a User Subscribes

To show all lists to which a user subscribes:

1. Open the Oracle WebMail client.

   **See Also**: "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client

2. Click the **Administration** tab.
3. Click the **List** subtab.
4. Click **Miscellaneous Functions**.
5. Click **Show all memberships of a user**.
6. Enter the user's name in the **User Name** field.
7. Select the domain of the user from the **Select Domain** list.
8. Click **Show Memberships** to display a list of distribution lists to which the user subscribes.
9. Click **Return to Distribution List Management** to return to the Distribution List Management page.

### Managing Aliases

Aliases are shorter or more descriptive names you can use when sending messages to long user IDs or list names. Aliases are pointers that redirect messages to the intended receiver.

For example, if Jane Doe changes her name to Jane Roe, an alias can be created so that messages sent to her original account, jane.doe@acme.com, are automatically redirected to her new account, jane.roe@acme.com. This alias prevents her from losing messages sent to her old user ID.

Using the Oracle WebMail client, you can create, modify, and delete aliases.

This section includes the following topics:

- Creating a New Alias
- Editing Alias Attributes
- Deleting Aliases

### Creating a New Alias

To create a new alias:

1. Open the Oracle WebMail client.
Managing Aliases

2. Click the Administration tab.
3. Click the Alias subtab to display the Alias Management page.
4. Click Create New Alias.
5. Select a domain from the Select Domain list.
6. Click Go to display the Create New Alias page.
7. Enter alias attributes in the following fields:
   - **Alias Name**: Enter a name by which the user ID will be referred. The alias name can either be just a name, such as dave, or it can be a fully qualified user or list ID, such as dave@foo.com.
   - **Alias Target**: Enter the fully qualified user or list ID to which the alias refers.
   - **Description**: Optionally, enter a description of the alias.
8. Click Create to display a confirmation page.
9. Click Return to Alias Management.

**Editing Alias Attributes**

To edit attributes of an existing alias:
1. Open the Oracle WebMail client.

   **See Also**: "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client

2. Click the Administration tab.
3. Click the Alias subtab to display the Alias Management page.
4. Click Edit Alias Properties.
5. Select the domain containing the alias from the Select Domain list.
6. Enter the alias name in the Search Criteria field. Enter an asterisk (*) to perform a wildcard search.
7. Click Go.
8. Click the alias you want to edit.
9. Edit the attributes, as necessary.
10. Click Modify to display a confirmation page.
11. Click Return to Alias Management.

**Deleting Aliases**

To delete an alias:
1. Open the Oracle WebMail client.

   **See Also**: "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client

   **See Also**: "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client
See Also: "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client

2. Click the Administration tab.
3. Click the Alias subtab to display the Alias Management page.
4. Click Delete Alias to display the Choose Alias to Delete page.
5. Enter the alias name in the Search Criteria field. Enter an asterisk (*) to perform a wildcard search.
6. Select the domain containing the alias from the Select Domain list.
7. Click Go.
8. Select the alias or aliases you want to delete.
9. Click Delete to display a confirmation page.
10. Click Return to Alias Management.

Managing News Objects

If a Network News Transport Protocol (NNTP) server is configured on an Oracle Collaboration Suite installation, an administrator can manage available peer servers and newsgroups using the Oracle WebMail client.

See Also:
- "NNTP Server" on page 3-41 for more information about configuring NNTP servers
- "oesng" on page D-6 and "oespr" on page D-9 for information about managing newsgroups and peers from the command line

This section includes the following topics:
- Managing Peer Servers
- About Newsgroups
- Managing Newsgroups

Managing Peer Servers

Use the Oracle WebMail client to add, edit, or delete peer servers, as the following sections describe:

See Also: "About News Servers" on page 3-42 for more information about peers

- Adding Peer Servers
- Editing Peer Server Properties
- Deleting Peer Servers

Adding Peer Servers
To add a peer server:
1. Open the Oracle WebMail client.  
   
   **See Also:** "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client

2. Click the Administration tab.

3. Click the News subtab to display the Peer Server Management page.

4. Click Add.

5. Enter information in the following fields:
   - **Installation(s):** An Oracle Collaboration Suite installation for which this peer is to be configured in which newsgroups have been created, and an NNTP server has been configured. The default is `um_system`.
   - **Hostname:** Fully qualified Internet host name of the peer, used by the NNTP inbound process to recognize an incoming connection as a peer connection.
   - **Port:** NNTP port on which the peer listens, used by the NNTP outbound process to connect to the peer. The default is 119.
   - **Accepted Newsgroup(s):** Names of newsgroups (wildcards are acceptable) for which feed is accepted from this peer. If any groups are specified, messages are accepted only if addressed to one or more of them.
   - **Rejected Newsgroup(s):** Names of newsgroups (wildcards are acceptable) for which feed is rejected from this peer. If any groups are specified, messages are rejected if addressed to one or more of them. This is checked after **Accepted Newsgroup(s)**. If a newsgroup appears in both **Accepted Newsgroup(s)** and **Rejected Newsgroup(s)**, it is rejected.
   - **Feed Newgroups:** Names of newsgroups for which feed is offered to this peer. If any groups are specified, then only messages posted to any of these groups are offered.

6. Click Submit to add the peer server and display a confirmation page. Click Return to Peers to return to the Peer Server Management page.

   Click Cancel to return to the previous page.

**Editing Peer Server Properties**

To edit a peer server:

1. Open the Oracle WebMail client.  
   
   **See Also:** "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client

2. Click the Administration tab.

3. Click the News subtab to display the Peer Server Management page.

4. Select an installation from the **Installation(s)** list.

5. Click Go.

6. Click the icon in the **Edit** column of the peer server for which you want to edit properties.
Managing News Objects

7. Edit the properties, as necessary.

8. Click Submit to commit the changes or Cancel to return to the previous page.

Deleting Peer Servers

To delete a peer server:

1. Open the Oracle WebMail client.

   See Also: "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client.

2. Click the Administration tab.

3. Click the News subtab to display the Peer Server Management page.

4. Select an installation from the Installation(s) list.

5. Click Go.

6. Select the peer server you want to delete.

7. Click Delete.

8. Click Yes to delete the peer server or No to return to the Peer Server Management page.

About Newsgroups

Note: Newsgroups cannot be viewed in Oracle WebMail.

A newsgroup is a collection of messages discussing a particular subject, posted to an Internet site and redistributed through Usenet, a worldwide network of news discussion groups. There are two types of newsgroups, public and private:

- Public newsgroups have worldwide distribution, are maintained at many news sites, and are intended to contain nonsensitive information. The NNTP service exchanges newsgroup articles among news sites.

  If your Oracle Collaboration Suite installation hosts more than one domain, public newsgroups are shared, which greatly reduces the storage space required for news articles. An inbound server always services all public newsgroups configured for an Oracle Collaboration Suite installation.

- Private newsgroups belong to and are visible in only one domain, where they are intended as internal discussion groups. Access to private newsgroups is permitted only if the inbound server has the local domain parameter set to that domain. An inbound server instance cannot host private newsgroups for more than one domain. For example, an inbound server instance with the local domain set to acme.com serves all public newsgroups in addition to only those private newsgroups that belong to the acme.com domain.

Newsgroups are organized into subject hierarchy. The first few letters of the newsgroup name indicates the major subject category; subcategories are represented by a subtopic name. Users can post to existing newsgroups and respond to previous posts, while only administrators can create newsgroups. Some newsgroups have a moderator, a designated person who decides which postings to allow or to remove.
Three attributes are associated with newsgroups:

- Name
- Description
- Posting allowed

Managing Newsgroups

Use the Oracle WebMail client to add, edit, or delete private and public newsgroups.

This section includes the following topics:

- Adding Private Newsgroups
- Editing Private Newsgroup Properties
- Deleting Private Newsgroups
- Adding Public Newsgroups
- Editing Public Newsgroup Properties
- Deleting Public Newsgroups

Adding Private Newsgroups

To add a private newsgroup:

1. Open the Oracle WebMail client.

   See Also: "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client

2. Click the Administration tab.

3. Click the News subtab.

4. Click Private Newsgroup Management.

5. Select a domain on which the newsgroup will reside from the Domain list.

6. Click Add to display the Create/Edit Newsgroup page.

7. Enter information in the following fields:

   - **Newsgroup Name**: A string of text that is the name of the newsgroup
   - **Owner**: A fully qualified e-mail address of the person who is to be the newsgroup owner
   - **Description**: A string of text that briefly describes the newsgroup
   - **Moderated Newsgroup**: Select either Yes or No from the list depending upon whether the newsgroup is to be moderated. The default value is No.
   - **Moderator(s)**: Fully qualified e-mail addresses of newsgroup moderators if the newsgroup is moderated
   - **Posting Allowed**: Select either Yes or No from the list depending upon whether posting to the newsgroup is allowed. The default value is Yes.
   - **Collaboration Suite Database**: Select from the list the database upon which news is stored for this newsgroup.
Managing News Objects

- **Article Retention Day(s):** Enter a number to specify the numbers of days an article is to be stored on the database.

8. Click **Submit** to add the newsgroup and display a confirmation page. Click **Return to Private Newsgroups** to return to the Private Newsgroup Management page.

   Click **Cancel** to return to the previous page.

**Editing Private Newsgroup Properties**

To edit private newsgroup properties:

1. Open the Oracle WebMail client.

   **See Also:** "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client

2. Click the **Administration** tab.

3. Click the **News** subtab.

4. Click **Private Newsgroup Management**.

5. Select the domain on which the newsgroup resides from the **Domain** list.

6. To limit the number of newsgroups listed, enter a newsgroup name—or a partial name with an asterisk (*) as a wildcard—in the **Filter** field.

7. Click **Go**.

8. Click the icon in the **Edit** column of the newsgroup for which you want to edit properties.

9. Edit the properties, as necessary.

10. Click **Submit** to apply the changes and display a confirmation page. Click **Return to Private Newsgroups** to return to the Private Newsgroup Management page.

   Click **Cancel** to return to the previous page.

**Deleting Private Newsgroups**

To delete a private newsgroup:

1. Open the Oracle WebMail client.

   **See Also:** "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client

2. Click the **Administration** tab.

3. Click the **News** subtab.

4. Click **Private Newsgroup Management**.

5. Select the domain on which the newsgroup resides from the **Domain** list.

6. To limit the number of newsgroups listed, enter a newsgroup name—or a partial name with an asterisk (*) as a wildcard—in the **Filter** field.

7. Click **Go**.

8. Select the newsgroup you want to delete.
9. Click **Delete**.

10. Click **Yes** to delete the newsgroup or **No** to return to the Private Newsgroup Management page.

### Adding Public Newsgroups

To add a public newsgroup:

1. Open the Oracle WebMail client.

   **See Also:** "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client

2. Click the **Administration** tab.

3. Click the **News** subtab.

4. Click **Public Newsgroup Management**.

5. Click **Add** to display the Create/Edit Newsgroup page.

6. Enter information in the following fields:
   - **Newsgroup Name**: A string of text that is the name of the newsgroup
   - **Owner**: A fully qualified e-mail address of the person who is to be the newsgroup owner
   - **Description**: A string of text that briefly describes the newsgroup
   - **Moderated Newsgroup**: Select either **Yes** or **No** from the list depending upon whether the newsgroup is to be moderated
   - **Moderator(s)**: Fully qualified e-mail addresses of newsgroup moderators if the newsgroup is moderated
   - **Posting Allowed**: Select either **Yes** or **No** from the list depending upon whether posting to the newsgroup is allowed
   - **Collaboration Suite Database**: Select from the list the database upon which news is stored for this newsgroup
   - **Article Retention Day(s)**: Enter a number to specify the numbers of days an article is to be stored on the database

7. Click **Submit** to add the newsgroup and display a confirmation page. Click **Return to Public Newsgroups** to return to the Public Newsgroup Management page.

   Click **Cancel** to return to the previous page.

### Editing Public Newsgroup Properties

To edit a public newsgroup:

1. Open the Oracle WebMail client.

   **See Also:** "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client

2. Click the **Administration** tab.
3. Click the News subtab.

4. Click Public Newsgroup Management.

5. To limit the number of newsgroups listed, enter a newsgroup name—or a partial name with an asterisk (*) as a wildcard—in the Filter field and click Go.

6. Click the icon in the Edit column of the newsgroup for which you want to edit properties.

7. Edit the properties, as necessary.

8. Click Submit to apply the changes and display a confirmation page. Click Return to Public Newsgroups to return to the Public Newsgroup Management page.

   Click Cancel to return to the previous page.

**Deleting Public Newsgroups**

To delete a public newsgroup:

1. Open the Oracle WebMail client.

   See Also: "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client

2. Click the Administration tab.

3. Click the News subtab.

4. Click Public Newsgroup Management.

5. To limit the number of newsgroups listed, enter a newsgroup name—or a partial name with an asterisk (*) as a wildcard—in the Filter field and click Go.

6. Select the newsgroup you want to delete.

7. Click Delete.

8. Click Yes to delete the newsgroup or No to return to the Public Newsgroup Management page.
This chapter discusses the different servers of the Oracle Mail system.

A typical installation of Oracle Mail will have either Post Office Protocol (POP) or Internet Message Access Protocol (IMAP) servers running but not both. It is good practice to have two instances of each server running for availability. Note, however, an instance of a server consumes resources, such as memory, processing, and database connections. Not all of the processes must be running, either, as would be the case if an installation has only clients that access stored messages using IMAP servers. In this case, POP servers would be unnecessary and could be turned off and disabled.

In most cases, set all parameter values at the target level. Notable exceptions are the Housekeeper server and the SMTP Outbound server.

This chapter includes the following topics:

- Oracle Collaboration Suite Database
- Managing Oracle Mail Servers and Instances
- Protocol Servers
- Housekeeper Server
- List Server
- NNTP Server

### Oracle Collaboration Suite Database

Oracle Mail uses the [Oracle Collaboration Suite 10g Database](Oracle Collaboration Suite Database) (Oracle Collaboration Suite Database) to store user folders and messages. The Oracle Collaboration Suite Database can be configured to store folders and messages for users in different domains. Messages destined for many accounts are stored only once, and links to the messages are set for all recipients. Single Oracle Collaboration Suite Databases can store mail for one domain or several different domains, while a large domain can be supported by multiple Oracle Collaboration Suite Databases.

Users can have one or more folders. These folders can be private, public, or shared. Private folders are visible only to the owner. Public folders are visible to all users in the owner’s domain. Shared folders are visible to specified users and specified distribution lists.

### Modifying Oracle Collaboration Suite Database Connection Parameters

The Oracle Collaboration Suite Database parameters are used by the Oracle Mail servers to connect to the Oracle Collaboration Suite Database.
To modify Oracle Collaboration Suite Database default parameters:

1. Open the Application Server Control Console for Collaboration Suite.

   **See Also:** "Oracle Enterprise Manager 10g Application Server Control Console for Collaboration Suite" on page 1-3 for information about accessing the Application Server Control Console for Collaboration Suite.

2. Click the application server instance where Oracle Mail is installed.

3. Click **Mail Application** in the **System Components** section to display the Mail Application page.

4. Click a server in the **Name** column, such as **IMAP Server**, **POP Server**, or **List Server**.

5. In the **Target** section, click **Collaboration Suite Database Connection Parameters**.

6. Select the Oracle Collaboration Suite Database for which you want to make changes.

7. Modify the parameters listed in **Table 3–1** you want to change.

8. Click **Apply**.

**Table 3–1  Oracle Collaboration Suite Database Connection Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Timeout (seconds)</strong></td>
<td>Enter a nonnegative number</td>
<td>Number of seconds before increasing the pool. The default value is 3600.</td>
</tr>
<tr>
<td><strong>Increment</strong></td>
<td>Enter a nonnegative number</td>
<td>Number of Oracle Collaboration Suite Database connections to be added to the connection pool. The default value is 1.</td>
</tr>
<tr>
<td><strong>Minimum</strong></td>
<td>Enter a nonnegative number</td>
<td>Minimum number of Oracle Collaboration Suite Database connections in the connection pool. The default value is 1.</td>
</tr>
<tr>
<td><strong>Maximum</strong></td>
<td>Enter a nonnegative number</td>
<td>Maximum number of Oracle Collaboration Suite Database connections in the connection pool. The default value is 10.</td>
</tr>
<tr>
<td><strong>Alternate Connect String</strong></td>
<td>String</td>
<td>Depending upon which server’s Oracle Collaboration Suite Database connection parameters are being modified, the alternate connect string is used by that server to connect to the Oracle Collaboration Suite Database chosen in Step 6.</td>
</tr>
</tbody>
</table>

The Oracle Collaboration Suite Databases shown on this page are the ones that are associated with this server or its instances on the Default Settings and Instance Settings pages.

**See Also:** "Modifying Server Instance Default Parameter Settings" on page 3-7 or "Modifying Parameter Settings for a Specific Server Instance" on page 3-8 for information about associating specific Oracle Mail servers with Oracle Collaboration Suite Databases.
Managing Oracle Mail Servers and Instances

This section discusses how to start, stop, restart, refresh, and modify servers and instances using the Oracle Enterprise Manager 10g Application Server Control Console for Collaboration Suite.

Starting an Oracle Mail server starts all the instances constituting that server type, such as IMAP and POP.

Stopping an Oracle Mail server sends a command to the server instances to shut down. Whenever instances are created or certain parameter values are changed, the server must be stopped prior to any such action.

System maintenance, such as upgrading the server hardware or software, is another reason an administrator should stop a server. The Oracle Mail server instances cannot be running while this kind of upgrade is being performed.

Restarting an Oracle Mail server first stops the server and then restarts it. An administrator can restart a server after particular parameters have been modified in order to apply the changes.

Refreshing an Oracle Mail server notifies running instances to reread the configuration. Changed configuration values take effect but only for certain parameters, such as Process Log Level. Current instances do not stop. For example, the IMAP log level can be changed, the IMAP server refreshed, and the new log level will take effect without any current user sessions getting disconnected.

This section includes the following topics:

- Log Files
- Enabling and Disabling Servers
- Starting, Stopping, Restarting, or Refreshing All Server Instances
- Creating a Server Instance
- Deleting a Server Instance
- Modifying Server Instance Default Parameter Settings
- Modifying Parameter Settings for a Specific Server Instance

Log Files

Oracle Mail server logs files are located in the \$ORACLE_HOME/oes/log/server_type directory. For example, List Server logs are found in the \$ORACLE_HOME/oes/log/list directory. Each running server instance creates a log directory for itself when it starts and then writes to a log file in that directory.

For example, if a List Server instance is running on a UNIX platform, and the operating system process ID for the process is 12345, the log file for the process will be \$ORACLE_HOME/oes/log/list/12345/12345.log.

The maximum size to which a log file can grow is configured by the Maximum Log Size parameter for a particular server. If a log file reaches the maximum size, it is renamed and a new log file is created. The old file is renamed by appending a number to the file name, such as 12345.log.000.

The renaming process cascades to older files. The names of older files are changed by increasing the value of the appended number. Example 3–1 shows a list of the log files in the log directory of the SMTP Outbound server.
Example 3–1  List of SMTP Outbound Server Log Files

% cd $ORACLE_HOME/oes/log/um_system/smtp_out/13067
% ls
13067.log   13067.log.002  13067.log.005  13067.log.008
13067.log.000  13067.log.003  13067.log.006  13067.log.009
13067.log.001  13067.log.004  13067.log.007

In the preceding example, log file renaming has occurred many times. The server instance is currently writing to 13067.log, the next most recent log file is named 13067.log.000, and the oldest log information is in the file named 13067.log.009.

The number of old log files to keep is configured by setting the Maximum Number of Log Files server parameter. Once the maximum number of log files is reached due to log file renaming, the oldest file is deleted.

In Example 3–1, if the Maximum Number of Log Files parameter is set to 10, and the size of the file named 13067.log grows to the maximum log size, the file named 13067.log.009 will be deleted, all remaining files will have their names changed, and a new 13067.log file will be created.

Log files for Oracle Mail servers are also found in the $ORACLE_HOME/opmn/logs directory. These log files contain debug and error output from the servers. Usually, it is not necessary to look at these files, but they can be useful when you are investigating problems with servers.

Example 3–2 shows where the administrator changes to the opmn log directory and lists the Oracle Mail server log files.

Example 3–2  Oracle Mail Server Log Files Listed in the opmn Log Directory

% cd $ORACLE_HOME/opmn/logs
% ls -1 email*
bash-2.05$ ls -1 email*
email~email_housekeeper~111669348732673252~1
email~email_imap~11166933915459529~1
email~email_imap~111669641725581757~1
email~email_listserver~111669349628087514~1
email~email_smtp_in~111669352320380482~1
email~email_smtp_in~111669739031461932~1
email~email_smtp_out~111669352925661397~1
email~email_smtp_out~111670781734121085~1
email~email_virus_scrubber~111669353532515101~1

Example 3–3 shows the type of debug output available in these files.

Example 3–3  Debug Output

% tail -18 email~email_smtp_in~111669352320380482~1
--------
05/06/25 13:44:40 Start process
--------
successfully added instance 111669352320380482[0,1000,0,1000]
good; added service  [ESSMI]
nslisten succeeded!
good; added registrar  [(DESCRIPTION=(ADDRESS=(PROTOCOL=IPC)(KEY=OCS_ROMMUM300.appserver.acme.com))))]
good; mapped instance to all registrars
good; mapped service 0 to all registrars
complete addr is
Enabling and Disabling Servers

A server must be enabled before it can be started. Disabling a server prevents it from being started.

To enable or disable a server:

1. Open the Application Server Control Console for Collaboration Suite.

   **See Also:** "Oracle Enterprise Manager 10g Application Server Control Console for Collaboration Suite" on page 1-3 for information about accessing the Application Server Control Console for Collaboration Suite

2. Click the application server instance where Oracle Mail is installed.

3. Click *Mail Application* in the *System Components* section to display the Mail Application page.

4. Select a server to enable or disable.

5. Click *Enable* or *Disable*.

---

**Note:** Disabling a server that is currently running will first stop the server, then disable it.

---

**See Also:**

- "Enabling an Oracle Mail Server" on page D-19 for information about enabling a server from the command line
- "Disabling an Oracle Mail Server" on page D-20 for information about disabling servers from the command line

Starting, Stopping, Restarting, or Refreshing All Server Instances

To start, stop, restart, or refresh all instances of a particular server:

1. Open the Application Server Control Console for Collaboration Suite.

   **See Also:** "Oracle Enterprise Manager 10g Application Server Control Console for Collaboration Suite" on page 1-3 for information about accessing the Application Server Control Console for Collaboration Suite

2. Click the application server instance where Oracle Mail is installed.
3. Click **Mail Application** in the **System Components** section to display the Mail Application page.

4. Select a server to start, stop, or refresh.

5. Click **Start**, **Stop**, **Restart**, or **Refresh**.

   Click **Restart** to apply any changes made to any server instance parameters. **Restart** shuts down all instances of the selected server before starting them up again. This will result in a brief interruption of e-mail service.

   Click **Refresh** to apply changes made to log levels or debug flags. **Refresh** does not shut down instances of the server and will not interrupt any service.

---

**Note:** The refresh icon located on this page refreshes the information on this page, not any servers.

---

**See Also:** "Starting All Instances of an Oracle Mail Server" on page D-21 for information about starting all server instances from the command line

### Creating a Server Instance

To create a server instance:

1. Open the Application Server Control Console for Collaboration Suite.

   **See Also:** "Oracle Enterprise Manager 10g Application Server Control Console for Collaboration Suite" on page 1-3 for information about accessing the Application Server Control Console for Collaboration Suite

2. Click the application server instance where Oracle Mail is installed.

3. Click **Mail Application** in the **System Components** section to display the Mail Application page.

4. Select the server for which the new instance is to be created.

5. Click **Stop** to stop the server.

6. Click the server in the **Name** column to display the page for that server.

7. Click **Create**. This creates a new server instance that inherits the default parameters.

   Optionally, click **Create Like** to create a new server instance with the same parameters as an existing, previously selected server instance.

8. Click the newly created instance to modify the parameter values.

9. Click **Apply** when finished.

10. Click **Clear Instance Settings** to clear parameter settings for all process instances listed.

11. Return to the Mail Application page.

12. Select the server for which the new instance was created.

13. Click **Start** to bring up the server.
Deleting a Server Instance

Caution: Deleting an Oracle Mail server instance may disable some or all e-mail processes.

To delete a server instance:

1. Open the Application Server Control Console for Collaboration Suite.

   See Also: "Oracle Enterprise Manager 10g Application Server Control Console for Collaboration Suite" on page 1-3 for information about accessing the Application Server Control Console for Collaboration Suite

2. Click the application server instance where Oracle Mail is installed.

3. Click Mail Application in the System Components section to display the Mail Application page.

4. Select the server from which the instance is to be deleted.

5. Click Stop to stop the server.

6. Click the server in the Name column to display the page for that server.

7. Select the server instance you want to delete.

8. Click Delete.

Modifying Server Instance Default Parameter Settings

All new server instances that are created inherit the default parameter values for that server type, unless the instance is created using the Create Like button. The parameters, both default and replicated, can later be modified for specific server instances.

Notes:

- In most cases, administrators should modify parameters only at the target level to reduce the chances of creating conflicts between two instances of the same server. Two notable exceptions to this are the Housekeeper server and the SMTP Outbound server.

- Servers must be restarted or refreshed whenever parameters are modified.
To modify default server instance parameter settings:

1. Open the Application Server Control Console for Collaboration Suite.

See Also: "Creating a Server Instance" on page 3-6

2. Click the application server instance where Oracle Mail is installed.

See Also: "Oracle Enterprise Manager 10g Application Server Control Console for Collaboration Suite" on page 1-3 for information about accessing the Application Server Control Console for Collaboration Suite

3. Click Mail Application in the System Components section to display the Mail Application page.

4. Click a server in the Name column, such as IMAP Server, POP Server, or List Server to display the page for that server.

5. Click Default Settings in the Target section.

6. Modify the parameters you want to change or click Revert to reset the parameters to their default values.

   Click Cancel to cancel any changes and return you to the server page.

7. Click Apply to apply changes.

8. Restart the server to apply any changes prior to creating any new server instances.

See Also: "Starting, Stopping, Restarting, or Refreshing All Server Instances" on page 3-5

Modifying Parameter Settings for a Specific Server Instance

Notes:

- Servers must be restarted whenever instance parameters are modified in order for the changes to be applied.

- Whenever a setting is cleared at the instance level, the corresponding value from the default parameter settings page is used. This inheritance occurs for all Oracle Mail servers and Oracle WebMail.

To modify parameters for a specific server instance:

1. Open the Application Server Control Console for Collaboration Suite.

See Also: "Oracle Enterprise Manager 10g Application Server Control Console for Collaboration Suite" on page 1-3 for information about accessing the Application Server Control Console for Collaboration Suite

2. Click the application server instance where Oracle Mail is installed.
3. Click Mail Application in the System Components section to display the Mail Application page.

4. Click a server in the Name column, such as IMAP Server, POP Server, or List Server to display the page for that server.

5. Click the server instance you want to modify.

6. Modify the parameters you want to change or click Revert to reset the parameters to their default values.

   Click Cancel to cancel any changes and return you back to the server page.

7. Click Apply to apply changes.

8. Restart the server to apply any changes.

   See Also: “Starting, Stopping, Restarting, or Refreshing All Server Instances” on page 3-5

Protocol Servers

The scalable protocol server programming framework maintains a pool of worker threads that handle the work for the clients. In addition, a pool of database connections are shared across client connections. Incoming client requests have worker threads assigned to them. Worker threads read client commands, obtain database connections, and carry out operations. Once the database connections are released back to the pool, the threads return to the worker thread pool.

A system can contain multiple mail stores, and the IMAP and POP servers can be configured to create database connection pools to more than one mail store. Administrators use the IMAP and POP server parameters to control connection pool sizes.

This section includes the following topics:

- IMAP and POP Servers
- SMTP Server

IMAP and POP Servers

The Internet Message Access Protocol (IMAP) (the current version is IMAP4) provides functionality to manipulate mail messages and mail folders stored on the server and to enable an offline client to resynchronize with the server. IMAP also has primitives enabling optimization of online performance, especially for large MIME messages.

The Post Office Protocol (POP) (the current version is POP3) provides mail manipulation services for smaller Internet nodes where it can be impractical to maintain a message transport system or undesirable to keep an Internet connection open for long periods of time. Messages are temporarily stored on the server until they are downloaded to a client system.

Note: Either the IMAP server or the POP server will be enabled in a given installation. Disable the unused server.

This section includes the following topics:

- IMAP and POP Server Architecture
Protocol Servers

- IMAP and POP Session Data Flow
- Oracle WebMail Client Session Data Flow
- IMAP and POP Server Instance Parameters
- Managing IMAP and POP Servers

IMAP and POP Server Architecture
The IMAP and POP servers obtain the benefits of multithreading, database connection sharing, and load balancing by using the framework. These benefits enable the servers to support thousands of concurrent user connections while using very few system resources.

Many operating systems limit the number of file descriptors and sockets that a single instance can open. These limits can make it necessary to run more than one instance of an IMAP or POP server, in which case the listener distributes the load between them. Administrators must verify the correctness of the operating system parameter controlling the file descriptors for such instances.

See Also: Oracle Collaboration Suite Installation Guide for Solaris Operating System for more information about operating system parameters

IMAP and POP Session Data Flow
As a user connects, either through various clients, such as Microsoft Outlook or Mozilla Thunderbird, or the Oracle WebMail client, it is important to understand the connection flow and the components the clients are accessing during login and during an individual session.

All IMAP-compliant and POP-compliant clients are able to access the Oracle Mail server. These clients must be directly installed on the end-user client's system and configured by that user.

The access method flow is described, as follows, and shown in Figure 3–1:

1. The client starts an application, such as Microsoft Outlook or Mozilla Thunderbird. The client must be configured to connect to the system where IMAP and POP are listening.
2. The user is prompted to enter a user name and password.
3. Authentication of the login information is checked against the Oracle Collaboration Suite Infrastructure through the IMAP server connection for validation. A connection is opened from the LDAP connection pool of the IMAP server. Once authentication is validated, the LDAP connection is released back to the original connection pool.
4. The user IMAP connection is passed to the database connection pool for access to the user e-mail account.
5. Once a connection has been established, a download of the user's INBOX begins. Any new incoming messages are also posted to the INBOX for sorting.
6. When the INBOX download is complete, the client releases the database connection back to the database connection pool, but maintains an authenticated cached connection to the IMAP instance.
7. Now when there is a call to the database, such as when a user opens a message or opens a folder, a new connection to the database is established to respond to the request. Once the request is satisfied, the database connection is released.
Oracle WebMail Client Session Data Flow

The Oracle WebMail client runs on the Oracle Collaboration Suite Applications tier. It is not necessary for the user to download any information, except for a cookie to the local client. Besides entering a URL in a Web browser, no local configuration is necessary. However, the authentication method is similar to that of other clients, except that the Oracle WebMail client caches the user preferences. The access method is through Oracle Java Mail API (OJMA) and is not, by default, using the IMAP server. IMAP can be configured to use IMAP through the oc4j.properties file under the $ORACLE_HOME/j2ee/OC4J_OCSClient/config directory.

The access method flow is described, as follows, and shown in Figure 3–2:

1. The client starts a browser and enters a given URL. This URL connects to the Applications tier where the Oracle WebMail client is configured.
2. The user is prompted to enter a user name and password. Once committed, the client calls the ESDS application programming interface (API).
3. The ESDS API uses the authentication information to check against the Oracle Collaboration Suite Infrastructure for validation. The connection is opened through the ESDS LDAP connection pool. Once authentication is validated, the LDAP connection is closed.
4. Once authenticated, the connection is passed to the OJMA connection pool for direct access to the user e-mail account.
5. Once a connection has been established, a download of the user’s INBOX begins. Any new incoming messages are also posted to the INBOX for sorting.
6. When the INBOX download is complete, the database connection is released back to the database connection pool, but maintained as an authenticated user by OJMA.
7. Now when there is a call to the database, such as when a user opens a message or opens a folder, a connection from the pool is opened by OJMA and the request is satisfied. Once the request is satisfied, the database connection is released.
**IMAP and POP Server Instance Parameters**

*See Also:* "Oracle Mail IMAP Server" on page F-6 and "Oracle Mail POP Server" on page F-18 for detailed information about IMAP and POP server instance parameters

**Managing IMAP and POP Servers**

*See Also:* "Managing Oracle Mail Servers and Instances" on page 3-3 for instructions on creating, deleting, and modifying server instances

**SMTP Server**

The Simple Mail Transfer Protocol (SMTP) enables e-mail messages to be sent between servers, and is used by most Internet e-mail systems. Mail clients use SMTP to send messages to a mail server, and use either POP or IMAP to retrieve messages.

The SMTP server handles all inbound and outbound mail, implements the SMTP protocol, and interacts with the domain name server (DNS) and the Oracle Internet Directory server for information about hosts and users.

The SMTP server is also responsible for delivering e-mail messages to archive servers based on configured archive policies.

*See Also:* "Oracle Mail Archive Policies" on page 8-26 for more information about archive policies

This section includes the following topics:

- Various SMTP Configurations
- SMTP Message Flow
- SMTP Inbound Server Architecture
- SMTP Outbound Server Architecture
- SMTP Address Rewriting Rules
Various SMTP Configurations
The flexible architecture of Oracle Mail enables users to set up a single or multitier configuration appropriate for specific a site.

This section includes the following topics:

- **Single Node Setup**
- **Single Oracle Collaboration Suite Database Setup**
- **Multiple Oracle Collaboration Suite Database Setup**

**Single Node Setup** A single node setup has one Oracle Collaboration Suite Database and one SMTP server running on the same host, supporting a small numbers of users.

**Single Oracle Collaboration Suite Database Setup** A single Oracle Collaboration Suite Database setup divides two servers into two tiers:

- The tier where the Oracle Collaboration Suite Database resides
- The Oracle Collaboration Suite Applications tier where SMTP and other protocol servers reside

This configuration provides fault tolerance and the flexibility to run multiple SMTP servers with distributed loads by running the servers behind a network director. Alternatively, it can have multiple MX records for the domain.

**Multiple Oracle Collaboration Suite Database Setup** A multiple Oracle Collaboration Suite Database is a scaled version of a single Oracle Collaboration Suite Database setup that supports a large user base. The multiple database setup consists of a set of hosts, each running an Oracle Collaboration Suite Database, and the Applications tier, which includes a set of hosts running the SMTP server and other protocol servers. Each SMTP inbound server can accept and deliver mail to multiple databases. The SMTP outbound server performs queue processing against a single database and delivers to multiple databases. It is possible to have one database just to receive the mail and the rest supporting the user base for added fault tolerance and reduced contention.

Each SMTP server serves only one Oracle Collaboration Suite Database, and each Oracle Collaboration Suite Database must have an SMTP server. The Oracle Collaboration Suite Databases on the SMTP hosts are used as SMTP queues and do not contain users.

**SMTP Message Flow**
The SMTP inbound server is responsible for handling the incoming SMTP connection. It receives incoming messages, queries the Oracle Internet Directory server to find and authenticate the addresses, rewrites addresses based on the rewriting rules, and applies antispam rules. If all the steps are successful, the SMTP message transfer agent (MTA) accepts the message and inserts it into the corresponding queue based on the destination address, as shown in Figure 3–3.

If the message recipient is a user outside of the Oracle Collaboration Suite system, the message is stored in the relay queue to await further processing. If the recipient is local, the message is stored in the local delivery queue. The Local Domains parameter contains the list of local domains used to determine whether an address is local.
local delivery module picks up the message later, applies the rules, and delivers it to
the user’s inbox.

If administrators do not want to process the messages immediately, they can be stored
in the submission queue and marked as submitted or unprocessed. Messages created
by the software developer’s kit (SDK) applications are also placed in the submission
queue and marked as submitted. Messages in the submission queue are picked up by
the SMTP outbound server.

For relay messages, the SMTP outbound server queries the DNS server, applies any
rules to the messages, and sends them out using SMTP. For submitted messages,
processing by the address rewriting and DNS resolution module happens first.
Subsequently, the SMTP outbound server sends them to the local delivery queue or to
the Internet, depending on whether the messages recipients are local.

During address resolution, the server determines whether the message is addressed to
a distribution list handled by the List Server. If so, the server places the message in the
queue for the List Server, which then picks up the message, expands the distribution
list, and delivers the message.

Messages for users on a different Oracle Collaboration Suite Database are placed in the
relay queue. The outbound server picks up and delivers the messages to the SMTP
inbound server for the other Oracle Collaboration Suite Database.

If the recipient is determined to be local, the message is stored in the local delivery
queue. To determine if an address is local, the Local Domains parameter is used. This
parameter contains the list of domains that are considered local.

If the recipient is an outside user, either on another Oracle Collaboration Suite
Database or on the Internet, the message is stored in the relay queue to await further
processing by the SMTP outbound server.

See Also: "SMTP Address Rewriting Rules" on page 3-17 and
"List Server" on page 3-33 for more information

The SMTP server is also responsible for delivering e-mail messages to archive servers
based on configured archive policies. To enable archive delivery, set the Archive
Processing parameter to Enabled in both SMTP inbound and outbound servers and
the List Server. This parameter determines whether the servers will check all messages
for archive eligibility.

---

Note: The Archive Processing parameter must contain the same
value for all the Applications tiers to ensure that archive message
processing is consistent. In addition to the Archive Processing
parameter, also set Archive Queue Processing to Enabled for the
SMTP outbound server. This parameter allows the SMTP Outbound
server to generate and deliver archive messages.

See Also: "Oracle Mail Archive Policies" on page 8-26 for more
information about enabling the archive feature
**Figure 3–3 SMTP Message Flow**

---

**SMTP Inbound Server Architecture**

The SMTP inbound server listens for client requests, processes incoming messages, and either delivers them locally or places them into queues for further processing.

The Oracle Net listener listens for incoming client requests on the SMTP port (default 25) and transfers connections to the SMTP server. The SMTP server maintains three thread pools to perform its tasks:

- Worker thread pool, through which it handles client requests
- Oracle Internet Directory server connection pool, through which it performs user authentication and address resolution
- Database connection pools to the configured Oracle Collaboration Suite Databases, through which it delivers local messages
Upon receipt of a connection request, the SMTP server picks up a worker thread from the pool to handle the request and:

- It performs name resolution on the incoming message using a connection from the Oracle Internet Directory.
- If the SMTP server is enabled for archiving, it determines whether archiving is needed for sender or recipient addresses. If message archiving is enabled, the message is placed in the archive queue for further processing.
- It applies antivirus and antispam rules.
- It applies recipient rewriting rules to the e-mail addresses to determine whether the message is to be delivered locally, sent to another Oracle Collaboration Suite Database, or sent out to the Internet.
- The SMTP MTA accepts the message and inserts it into the corresponding queue based on the destination address.
- It terminates the SMTP connection to the client for all but the local recipients and the worker thread continues to process the message and perform local delivery.

**Note:** If the recipient is an SMTP distribution list, the message is placed in the submission queue to be processed. The SMTP outbound server expands SMTP distribution lists and performs delivery to the expanded lists.

**SMTP Outbound Server Architecture**

The SMTP outbound queue processor processes messages in the submission, local, and relay queues. It has a main thread for each queue that periodically polls the database for messages in its queue. Whenever there are messages to process, a new thread is spawned to process the mail.

The outbound queue processor also maintains two other thread pools:

- The Oracle Internet Directory server connection pool, through which the outbound queue processor performs address authentication. If `SMTP_auth` is turned on, this thread pool is also used for user authentication prior to sending out a message.
- The database connection pool to the mail store, through which the outbound queue processor delivers local messages.

The size of all of these thread pools can be set through the Application Server Control Console for Collaboration Suite.

**See Also:** "Modifying Parameter Settings for a Specific Server Instance" on page 3-8 for more information about setting server parameters

When a thread is started to process a message from one of the queues, it picks up a database connection from the pool and gets connections from the Oracle Internet
Directory pool as needed. After the mail is processed, the database and Oracle Internet Directory threads are returned to the pool.

Messages in the submission queue are treated as not yet processed, and so must go through the antivirus and antispam rules and rewriting rules to determine their destination. After processing, the messages are either placed in the local delivery queue or in the relay queue.

If the recipient is a user outside of Oracle Collaboration Suite, the message is stored in the relay queue to await further processing by the SMTP outbound server. If the recipient is on an Oracle Collaboration Suite Database different from the database that was used to insert the incoming message, and if the SMTP inbound server is configured to perform delivery to this database, the message is copied and delivered into this database using SQL*Net. If the SMTP inbound server is not configured to deliver to the recipient's Oracle Collaboration Suite Database, the message is placed in the relay queue to await further processing by the SMTP outbound server.

Messages in the local delivery queue are destined for a local mailbox, so the queue processes or applies local rewriting and other rules, if any, and inserts the mail into the user’s inbox in the database using a connection from the database pool.

Relay messages require further processing because their recipients are either on a different local message store or outside the e-mail system. Relay messages first go through the sender rewriting rules, then the system rules are invoked for event relay and external filter processing. If the system rule processing and external filter processing are successful, the DNS resolution takes place. The SMTP outbound queue processor then sends the relay messages to another Oracle Collaboration Suite Database in the system or to the Internet using SMTP, depending on whether the message recipients are local or not.

If the delivery of an e-mail fails, the message is returned into the queue and delivery is retried after intervals defined by the `minqueueage` parameter. If the attempted redeliveries are unsuccessful during the interval equal to the `queuetimeout` parameter, a delivery failure message is sent to the sender.

**SMTP Address Rewriting Rules**

The SMTP address rewriting rules enable you to check and correct the addresses of an e-mail message before sending it to its final recipient destinations. Rules resolve a focused or internal format address into a mailer-host-user triplet that can be delivered. Table 3–2 lists and describes mailer, host, and user parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mailer</td>
<td>Specifies the Oracle Mail SMTP server daemons used for delivery. <strong>Note:</strong> This is the only mailer available. Creating alternative mailers is not a feature of this application.</td>
</tr>
<tr>
<td>Host</td>
<td>Specifies either a fully qualified host name, such as <code>hostname.acme.com</code>, or a domain name, such as <code>foo.com</code>.</td>
</tr>
<tr>
<td>User</td>
<td>Specifies the recipient user name.</td>
</tr>
</tbody>
</table>

To execute and complete name resolution, the SMTP inbound server parses each rule for every address in the message envelope during mail delivery.

This section includes the following topics:

- Components of Rewriting Rules
Rule Execution Guidelines

Oracle Mail Rewriting Rules

Creating an Oracle Mail Address Rewriting Rule

Components of Rewriting Rules Headers for the message and the envelope are distinctly different. The envelope headers are generated by the receiving e-mail application, rather than by the sender. Received: headers are the envelope headers, and relate only to the envelope From and envelope To fields.

The envelope From header is created from the MAIL FROM entry in the received message. For example, when a sending computer puts MAIL FROM: jsmith@foo.com in the message, the receiving e-mail application generates the envelope From field content as jsmith@foo.com.

Similarly, the envelope To is derived from an incoming message line, such as RCPT TO: john.smith@foo.com. The information for envelope To and envelope From is stored in a different location from the header.

Mail is routed based solely on the envelope To data rather than on the message To: or From: headers supplied by the sender. These headers contain no significant envelope information and can misrepresent who sent the mail to whom. An example of a message header as is illustrated in Figure 3–4.

Figure 3–4 Message Header

A handshake between two SMTP systems executing transactions through port 25 involves a series of action dialogs for each message being delivered. These messages can be seen on the receiving or sending systems only by running in debug mode, as illustrated in Example 3–4. The example illustrates why the routing of mail ignores the Message From and Message To headers, which can be faked, and relies instead on the envelope data.

Example 3–4 Example of Original Header

HELO acme.org
250 mail.rico.net Hello ernie.com [104.65.21.123], pleased to meet you
MAIL FROM: forged-address@foo.org
250 forged-address@foo.org... Sender ok
RCPT TO: john.smith@foo.com
250 john.smith@foo.com... Recipient OK
DATA
354 Enter mail, end with "." on a line by itself
From: another-forged-address@moreover.com
To: (your address suppressed for stealth mailing and annoyance)
.
250 OAA08757 Message accepted for delivery

Example 3–5 shows how the header illustrated in Example 3–4 is seen by the message recipient.
Example 3–5  Resulting Header as Seen by the Recipient

Received: from foo.org ([104.128.23.115]) by mail.rico.net (8.8.5)
From: another-forged-address@moreover.org
To: (your address suppressed for stealth mailing and annoyance)

Notice that the only true data seen by this recipient is in the Received line, which was taken from the RCPT TO entry actually sent. The apparent sending addresses need not have any relationship to the physical facts. They are taken from the data of the message MAIL FROM and RCPT TO: lines exactly as entered by the sender, with no necessary relationship to what is factual.

The preceding examples illustrate why the MAIL FROM: and RCPT TO: headers are not reliable in mail, because they can easily be forged.

Rule Execution Guidelines  Address rewriting rules are applied sequentially, beginning with rule 1. All rules are applied, unless a result starts with a dollar sign ($) and at sign (@), which immediately stops rule execution and ignores any remaining rules. If a rule has a syntax error or cannot be executed, it is ignored.

A rule is applied to its own output in a loop until the application of the rule does not yield anymore changes in the result. The next rule in the sequence is then applied.

After all the rules have been executed, an Oracle Internet Directory resolution is performed on the result. If the Oracle Internet Directory resolution returns a changed address due to an alias (for example, the address rewriting rules are applied to the changed address), the Oracle Internet Directory resolution is performed again. When the Oracle Internet Directory resolution rule does not yield any more changes, the rule execution process is done.

Oracle Mail Rewriting Rules  To understand rewriting rules, you must understand their components: a left-hand side (LHS), a right-hand side (RHS), and a description used in this format:

Pattern (LHS), Result (RHS), Description

Table 3–3 lists descriptions of the rewriting rule components.

Table 3–3  Rewriting Rule Components

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pattern (LHS)</td>
<td>Specifies the pattern to be changed.</td>
</tr>
<tr>
<td>Result (RHS)</td>
<td>Specifies that whenever the Pattern (LHS) is seen, it is changed with this result.</td>
</tr>
<tr>
<td>Description</td>
<td>Specifies the administrator’s rule notation, and is not used in address name resolution. Anything after the last comma does not require quotation marks.</td>
</tr>
<tr>
<td>Comma (,)</td>
<td>Separates the LHS, RHS, and Description. No spaces are allowed between the commas, nor before the first comma.</td>
</tr>
</tbody>
</table>

When the Pattern (LHS) is compared against the address and finds a match, the Result (RHS) replaces that match in the address. The comparison is not case-sensitive. If no match is found, then this rule is skipped and the next rule is applied. A rule can be applied to an address resulting from applying a previous rule.

Tokens and Matching
When processing an address for rewriting by a rule, the SMTP daemon first separates the address into parts called tokens and stores them into a buffer called the workspace.
A rule’s Pattern (LHS) is also divided into tokens, which are then compared to the tokens in the workspace. If the two sets of tokens are identical, it is a match, and the result of the left-hand side comparison is true.

**LHS Operator Descriptions**

If rules always had to match addresses exactly, too many rules would be required, which would render their usage unproductive. Instead, operators such as wildcards can also be used to match arbitrary text in the workspace. To make the entire Pattern (LHS) match, wildcard operators match as little as possible. Figure 3–5 shows an example of rewriting rule.

**Figure 3–5  Rewriting Rule Example**

<table>
<thead>
<tr>
<th>LHS</th>
<th>RHS</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$^+$.$, $1.$.$2@$uuh$ost,</td>
<td>Changing the first.last to first.last@$uuh$ost</td>
<td></td>
</tr>
</tbody>
</table>

The following LHS operators are used as wildcards or token identifiers:

- **$^*$** = zero or more tokens, and prefers zero, or the fewest possible, to satisfy a Pattern (LHS) match
  
  For example:
  
  fred.jones resolved by the Pattern (LHS) rule
  Result (RHS) rule = fred.jones@\$uuh\$ost

- **$^+$** = one or more tokens, and prefers one, or the fewest possible, to satisfy a Pattern (LHS) match

  To illustrate, consider passing the address john.jones@home.ORG to the Pattern (LHS), as shown in Figure 3–6:

  **Figure 3–6  Changing Uppercase to Lowercase**

<table>
<thead>
<tr>
<th>LHS</th>
<th>RHS</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$^*$ @ $^+$.$ORG, $1.$.$2.org,</td>
<td>Changing the uppercase to lowercase</td>
<td></td>
</tr>
</tbody>
</table>

  For example:
  
  john.jones@home.ORG resolved by the Pattern (LHS) rule,
  
  Result (RHS)= john.jones@home.org
  $^*$ (matches zero or more) = john.jones
  @ matches exactly
  $^+$ (matches one or more) = home

- **$^-** = exactly one token

  john rewritten by the right-hand side token\$rhs $^- = -$\rightarrow john
  
  If the result was john@\$uuh\$ost, then the rule would not match.

**RHS Operator Descriptions**

The following list describes the various RHS operators:

- **$1,\$.\$2** identifies Pattern (LHS) tokens to be passed over into the Result (RHS). These are copied by position from the Result (RHS) location.
- lhs $\ast$.\$\ast$ where rhs $\$1.\$2$
- $\$\$: Indicates that the rule should be applied only once.
- rhs john rewritten by $\$1 = john$
- $\$@$: Exactly none. Rules are not applied beyond this point if the $\$@$ operator is reached during the rewriting rule processing.
- $\$!$: Reject: A DSN will be sent if the SMTP outbound server is rewriting
- $\$\%$: Discard: The address is discarded. No DSN is sent if the SMTP outbound server is rewriting.

Creating an Oracle Mail Address Rewriting Rule  Oracle Mail uses two types of address rewriting rules:

- Sender rewriting rules: Apply only to senders of messages that are relayed out by the SMTP outbound server
- Recipient rewriting rules: Apply to all incoming and outgoing recipient addresses

Rules can be written using the Application Server Control Console for Collaboration Suite and are executed in the order in which they are entered.

Examples of Rewriting Rules
The following example takes the From: (sender) and the To: (recipient) addresses and rewrites them using the rewriting rules.

- Sender Rewriting Rules
  
  $\$\*+\$.com,$1@uuhost.com, "This changes john.doe@foo.com to john.doe@uuhost.com"
  
  Rule:
  1. Match anything before the at sign (@) and take the one token after the at sign (@) with the .com at the end and change it.
  2. Keep the user name and pass it to the RHS through $\$1$, which is in direct order or the first token from the LHS, john.doe and pass the @ sign as is, but change the $\$2$ token (second token) to uuhost.com.

  The receiving SMTP daemon accepts this message, and accepts john.doe@uuhost.com as the sender of the message. It is important to remember that the header information is never changed from its original entries.

- Recipient Rewriting Rules
  
  $\$\ast$.\$\ast$uuhost,\$1.$2foo.com, "This changes fred.jones@uuhost to fred.jones@foo.com"
  
  Rule:
  1. Capture both the first name and the last name of any address that has uuhost after the at sign (@).
  2. Bring those tokens over as $\$1$ and $\$2$ respectively, and keep a period (.) between them.
  3. After the at sign (@), replace uuhost with foo.com.

- Rewriting an E-Mail Address
The following example shows how to rewrite an e-mail address using `fred.jones@uuhost`. The address points to `uuhost`, which is a UNIX to UNIX copy (UUCP) system name. The message is sent using the UUCP software which requires the address form of `uuhost!username` and that the current address be rewritten for UUCP. Consider the following example:

```
$*@uuhost,uuhost!$1,"Changing from to UUCP address"
```

Using the rewriting rule shown in Figure 3–7, you can change this address to a more compatible Internet address, such as `fred.jones@foo.com`.

![Figure 3–7 Message Flow through Rewriting Rules](image)

The operators used in Figure 3–7 are as follows:

- `$*` token in Pattern (LHS) resolves as anything after the exclamation point (!).
- `$*` = `fred.jones`.

The comma (,) is the separator between the LHS, RHS, and Description.

The `$1` or first token in LHS string `$*$` moves to the RHS as is.

Message headers are not rewritten during SMTP address name resolution. The address is parsed and rewritten by the delivery daemon rewriting rules, and passed as a logical address to the receiving daemon, which then parses and resolves it.

### SMTP Server Parameters

See Also:

- "Oracle Mail SMTP Inbound Server" on page F-34 for detailed information about SMTP inbound server parameters
- "Oracle Mail SMTP Outbound Server" on page F-44 for detailed information about SMTP outbound parameters

### Managing SMTP Servers

If message archiving is enabled on your Oracle Mail installation, create a server instance of the SMTP outbound server that is dedicated to the handling of archived messages.

See Also:

- "Managing Oracle Mail Servers and Instances" on page 3-3 for instructions on creating, deleting, and modifying SMTP server instances
- "Enabling Message Archiving" on page 8-29 for information about creating and configuring an SMTP outbound server instance for message archiving
SMTP Routing Control

See Also: "Antispam Methods" on page 6-5 for more information about routing control

Housekeeper Server

The Housekeeper server is a background process that works inside the Oracle Collaboration Suite Database and performs periodic tasks, such as garbage collection, which cleans up deleted message bodies. Additional tasks include performing Oracle Text index synchronization and optimization for enabling message body search, and moving message bodies to tertiary storage tablespaces.

During Oracle Mail installation, a Housekeeper instance is created by default to perform basic garbage collection. Once the server process finishes its assigned task, it sleeps for a configured amount of time before waking up to restart the tasks.

The Housekeeper server can also be configured to start and stop running certain tasks dynamically from the command line, enabling the administrator to control the exact time when certain tasks are started.

See Also: "Dynamically Starting and Stopping Housekeeper Tasks" on page D-22 for instructions on dynamically starting and stopping Housekeeper tasks from the command line

The Housekeeper server consumes data produced by other Oracle Mail servers. For example, the pruning garbage collection task processes all the messages produced by the IMAP expunge command and filters out those messages that are still referenced by users. Additionally, the collection task processes the rest of the pruned result and removes all message bodies. Housekeeper metric information enables administrators to track the progress of its tasks.

The Housekeeper process can also be configured to enable LogMiner-based mail recovery. Once this feature is enabled, vital information about all deleted messages is kept in the database, allowing these messages to be recovered at a later time.

Note: Enabling LogMiner recovery may lead to Housekeeper process performance degradation.

The Housekeeper log files are located in two places: the Oracle Collaboration Suite Database and the Applications tier. The log file on the Oracle Collaboration Suite Database contains information about the progress of housekeeping tasks; the log file on the Applications tier contains information about the status of the process.

The Housekeeper server is designed to perform eight distinct and separate tasks:

- Three operational tasks:
  - Statistics Cleanup
  - Process Control Message Cleanup
  - Tertiary Storage
- Five additional tasks:
  - Expiration
  - Pruning
- Collection
- Index Synchronization
- Text Optimization

This section includes the following topics:

- Configuring Housekeeper Tasks
- Housekeeper Server Parameters
- Managing Housekeeper

**Configuring Housekeeper Tasks**

For the Housekeeper server to perform all eight of the aforementioned tasks, either eight separate instances of the Housekeeper server can be configured, or tasks can be combined. At a minimum, three separate instances must be configured in order to perform all eight tasks.

Regardless, Oracle recommends that for any size installation, three separate instances of the Housekeeper server be configured to perform the following three tasks:

- **Collection**: Deleting an instance of a message or the message itself is an expensive operation for the database in terms of resource consumption. Therefore, for performance reasons, when you delete a message you actually tag the message to be permanently deleted later. The Housekeeper server, in the background, performs the collection and cleanup of deleted messages from the Oracle Collaboration Suite Database.

  See Also: "Process Control Message Cleanup" on page 3-25 for more information about additional Housekeeper tasks that can be combined with the garbage collection instance

- **Index Synchronization**: Index synchronization is the process of looking at each message in detail (message bodies, headers, and attachments) to facilitate searching. It is another expensive operation for the database in terms of resource consumption. Therefore, for performance reasons, messages stored in the Oracle Collaboration Suite Database that must be indexed are done so by the Housekeeper server in the background.

  See Also: "Creating a Housekeeper Server Instance to Index Text" on page 3-29 for more information

- **Tertiary Storage**: Users often keep messages in their production Oracle Collaboration Suite Database for long periods of time. The Oracle Collaboration Suite Database has tertiary storage, which is a separate set of tablespaces designed to store these older messages. An administrator can configure these tablespaces on less expensive or slower disks, because they will be accessed less often. The Housekeeper server, in the background, moves messages of a specified age to tablespaces in tertiary storage.

  See Also: "Tertiary Storage" on page 3-31 for information about configuring a Housekeeper server instance for tertiary storage

This section includes the following topics:

- Process Control Message Cleanup
- Oracle Text
- Tertiary Storage

### Process Control Message Cleanup

As mentioned previously, a Housekeeper server instance configured for garbage collection is created by default upon installation of Oracle Mail. In addition to garbage collection, configure this instance to perform process control message cleanup.

Different Oracle Mail servers sometimes use advanced queuing to facilitate interprocess communication. The Housekeeper server can be configured to clean these messages, improving Oracle Mail performance.

---

**Note:** This procedure combines the Process Control Message Cleanup operation mode with the Pruning and Collection tasks.

---

To enable process control message cleanup:

1. Open the Application Server Control Console for Collaboration Suite.

   **See Also:** "Oracle Enterprise Manager 10g Application Server Control Console for Collaboration Suite" on page 1-3 for information about accessing the Application Server Control Console for Collaboration Suite

2. Click the application server instance where Oracle Mail is installed.

3. Click **Mail Application** in the **System Components** section to display the Mail Application page.

4. Select the Housekeeper server and click **Stop** to bring down the server.

5. Click **Housekeeper** to display the process page.

6. Click the default Housekeeper server instance configured for garbage collection to display the parameters for that particular instance.

7. Select **Process Control Message Cleanup** from the **Operation Mode** list.

8. Select **Enabled** from the **Pruning** and **Collection** lists in the **Housekeeping Operations** section.

9. Ensure that all other Housekeeping Operations are disabled.

10. Enter 60 in the **Frequency of Execution of Housekeeper Process** field.

11. The **Age Threshold** parameter units are measured in minutes when process control message cleanup is configured. Because few of these messages are generated on a daily basis, 30 is an acceptable value for this parameter.

12. Select **On Startup** from the **Run Task** list.

13. Optionally, enable the **Support Log Miner Recovery** parameter to recover messages with LogMiner.

   **See Also:** "Setting Up LogMiner to Recover Mail" on page 3-26

14. Click **Apply**.

15. Return to the Mail Application page.
16. Select the Housekeeper server and click Start to start the server.

Setting Up LogMiner to Recover Mail To set up mail recovery, you must enable supplemental logging for the Oracle Collaboration Suite Database and configure the Housekeeper server to record the messages being deleted into the redo logs.

Setting up LogMiner involves the following tasks:

■ Oracle Collaboration Suite Database Tasks
■ Enabling Supplemental Logging
■ Configuring the Housekeeper Server to Record Deleted Messages

Oracle Collaboration Suite Database Tasks
Perform the following tasks on the Oracle Collaboration Suite Database to set up LogMiner:

1. Ensure that the database is in archivelog mode.
2. Specify the archive log destination in the init.ora file, as follows:
   
   ```
   log_archive_dest_1='location=full_path'
   ```
3. Specify the archive log format in the init.ora file, as follows:
   
   ```
   log_archive_format=arch_%t_%s_%r.arc
   ```

Enabling Supplemental Logging
To enable supplemental logging for the Oracle Collaboration Suite Database:

1. Start SQL*Plus and log in as sys, as follows:
   
   ```
   $ sqlplus sys/sys_password
   ```
2. Enter the following SQL command:
   
   ```
   SQL > alter database add supplemental log data (primary key,unique index) columns;
   ```

Configuring the Housekeeper Server to Record Deleted Messages
The following procedure is an abbreviated form of that described in "Process Control Message Cleanup" on page 3-25. The following procedure only configures the Housekeeper to record deleted messages.

To configure the Housekeeper process to record the messages being deleted into the redo logs:

1. Open the Application Server Control Console for Collaboration Suite.

   See Also: "Oracle Enterprise Manager 10g Application Server Control Console for Collaboration Suite" on page 1-3 for information about accessing the Application Server Control Console for Collaboration Suite

2. Click the application server instance where Oracle Mail is installed.
3. Click Mail Application in the System Components section to display the Mail Application page.
4. Click Housekeeper.
5. Click the Housekeeper instance where the collection parameter is configured.
6. Enable the **Support Log Miner Recover** parameter in the **General Parameters** section.

7. Click **Apply**.

8. Return to the Mail Application page.

9. Click **Start**.

---

**Oracle Text**

Integrating **Oracle Text** and Oracle Mail extends the e-mail server functionality, enabling text search in e-mails, e-mail theme generation, and e-mail formatting functions such as highlight and markup.

Oracle Text integration support is installed by default when Oracle Mail is installed. However, if the database user `ctxsys` is not present at the time of installation, the Oracle Text installation will fail.

---

**Note:** This feature is only available when the Oracle Collaboration Suite Database is Oracle Database 10g Enterprise Edition.

---

The user attribute **Text Indexing** enables users to perform server-side search on mail message bodies.

**See Also:** "Managing Oracle Mail Users" on page 2-1 to enable a user for message body search or change this attribute value for all new users created by default

Oracle Mail support for Oracle Text provides both a Java SDK and a PL/SQL SDK for application integration. Applications can interface with the SDKs to use or extend Oracle Text functionalities.

Except for zipped attachments, Oracle Mail message bodies and attachments can be indexed and later searched for text strings, themes, gists, or formatting, such as highlight and markup. To be searchable, the contents of a mail message body must be indexed by the Oracle Text server. If indexing is enabled, Oracle Mail puts candidate messages into a queue for Oracle Text to index. The created index is later usable for performing a message body search.

Text indexing enables searching message bodies for content, using IMAP clients that support message body searching or using the Oracle Ultra Search component of Oracle Collaboration Suite. This feature is available only to users whose accounts are text-enabled.

Applications that integrate with Oracle Mail can use Oracle Text indexing through the PL/SQL and Java APIs.

**See Also:** Chapter 1 "PL/SQL API" Reference in *Oracle Mail Application Developer’s Guide* for more information about using Oracle Mail APIs to find themes and gists in e-mail messages

---

This section includes the following topics:

- Enabling E-mail Body Searching for Various Languages
- Verifying Oracle Text Installation
- Creating a Housekeeper Server Instance to Index Text
Enabling Text Indexing for a User

Enabling E-mail Body Searching for Various Languages  The text index for e-mail body searching is created with the Oracle Text BASIC_LEXER, which supports English and most western European languages that use white space delimited words. For other languages that are not supported by Oracle Text BASIC_LEXER, such as Chinese, Japanese, and Korean, e-mail body search does not function.

To enable message search for Chinese, Japanese, or Korean:

1. Stop the Housekeeper process using the Application Server Control Console for Collaboration Suite.

   See Also:  "Starting, Stopping, Restarting, or Refreshing All Server Instances" on page 3-5 for information about stopping a process

2. Run the following SQL commands as database user es_mail:

   SQL> @recreate_text_index.sql

3. Select and enter the text lexer for indexing messages from the list, as shown in the following example. The script will rebuild the text index using the selected lexer.

   SQL> @recreate_text_index

   Use this script to customize or update the index used for text searching. Choose a lexer and a default character set for mail messages.

   LEXER: a lexer is a program component responsible for recognizing words in a document for a specific language. Choose one of the following representing the primary language used in the system.

   1 - chinese lexer   for Chinese
   2 - japanese lexer  for Japanese
   3 - korean lexer    for Korean
   4 - default lexer   for other languages
   (this is the default if no input is received)

   Enter the desired lexer number[4]: 4

   DEFAULT CHARACTER SET: when a mail message body or a text attachment of a mail message does not contain a character set tag in the header, the system uses this default character set to recognize the mail message for indexing. Choose one of the following representing the primary character set that client mail programs use in this environment. Note that this is NOT necessarily the character set used in the mail database. For a list of recommended default character sets for popular languages, refer to the text file default_charset.txt present in the same directory.

   1 - US-ASCII (US7ASCII)          2 - UTF-8 (AL32UTF8, default)
   3 - SHIFT_JIS (JA16SJIS)         4 - EUC-JP (JA16EUC)
   9 - GB18030 (ZHS32GB18030)      10 - BIG5 (ZHT16MSWIN950)
   11 - BIG5-HKSCS (ZHT16HKSCS)    12 - WINDOWS-1250 (E8MSWIN1250)
   13 - WINDOWS-1251 (E8MSWIN1251) 14 - WINDOWS-1252 (E8MSWIN1252)
   15 - WINDOWS-1253 (E8MSWIN1253) 16 - WINDOWS-1254 (E8MSWIN1254)
   17 - WINDOWS-1255 (E8MSWIN1255) 18 - WINDOWS-1256 (E8MSWIN1256)
   19 - WINDOWS-1257 (E8MSWIN1257)
Enter the default character set number[2]: 2
Setting default character set and re-creating the text index...
(this may take a while, please wait...) Setting default character set...
Creating text index...

PL/SQL procedure successfully completed.

Done.
SQL> exit

4. Ensure that a Housekeeper server instance is configured for Oracle Text indexing using the Application Server Control Console for Collaboration Suite.

5. Start the Housekeeper process using the Application Server Control Console for Collaboration Suite.

See Also: "Starting, Stopping, Restarting, or Refreshing All Server Instances" on page 3-5 for information about starting a process

Note: Indexing is limited to only one lexer.

Verifying Oracle Text Installation Before text indexing can be used, Oracle Text must be installed and configured. Oracle Text is installed by default when Oracle Database 10g Enterprise Edition is installed. The Oracle Mail support for Oracle Text installation fails if the database user ctxsys is not present at the time of installation.

To verify that the Oracle Text option was installed and configured on the Oracle Collaboration Suite Database, run the following SQL query as sysdba:

SQL> select comp_id, version, status from dba_registry;

If Oracle Text was installed correctly, an output similar to the following displays:

<table>
<thead>
<tr>
<th>COMP_ID</th>
<th>VERSION</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONTEXT</td>
<td>10.1.0.4.0</td>
<td>VALID</td>
</tr>
</tbody>
</table>

If Oracle Text was not installed and configured on the Oracle Collaboration Suite Database, it must be configured manually.

See Also: Oracle Collaboration Suite Installation Guide for Solaris Operating System for further instructions on installing and configuring Oracle Text

Creating a Housekeeper Server Instance to Index Text Oracle Text periodically processes a message queue filled by a Housekeeper server instance.

Text search performance can be improved by periodically optimizing the existing Oracle Text index. Because many indexed messages are deleted or moved, the Oracle Text index bits are no longer consecutive, slowing down searching. Search time can be reduced by periodic cleanup of the Oracle Text index, removing entries that refer to deleted or moved messages.
Optimization can be done by the Housekeeper server. Assign a new Housekeeper instance to do this unless performance requires optimization to be done at the same frequency as indexing.

To create a Housekeeper server instance to queue messages for text indexing:

1. Open the Application Server Control Console for Collaboration Suite.

   **See Also:** "Oracle Enterprise Manager 10g Application Server Control Console for Collaboration Suite" on page 1-3 for information about accessing the Application Server Control Console for Collaboration Suite.

2. Click the application server instance where Oracle Mail is installed.

3. Click Mail Application in the System Components section to display the Mail Application page.

4. Select the Housekeeper server and click Stop to bring down the server.

5. Click Housekeeper to display the Housekeeper page.

6. Click Create to create a new Housekeeper server instance.

7. Click the new Housekeeper server instance to display its parameter page.

8. Select Enabled from the Text Synchronization and Text Optimization lists in the Housekeeping Operations section.

9. Ensure that all other Housekeeping Operations are disabled.

10. In the Frequency of Execution of Housekeeper Process field in the General Parameters section, enter how often the Housekeeper should queue messages for indexing, in minutes.

    For example, if the Housekeeper should queue messages for indexing every 2 hours, enter 120 in the field.

    **Note:** Indexing too frequently will result in increased database server load and degraded search performance, but indexing too infrequently will cause more new messages to be unavailable for search. The recommended frequency is 1 to 2 hours.

11. Click Apply.

12. Return to the Mail Application page.

13. Select the Housekeeper server and click Start to bring up the server.

**Enabling Text Indexing for a User**

**See Also:** "Modifying E-mail User Attributes" on page 2-4 to enable text indexing for users.
Tertiary Storage

Administrators can configure Oracle Mail to move messages to tertiary storage based on the age of the message. This process frees up valuable space on the primary disk for newer, more frequently accessed messages, and enables users to still access messages in tertiary storage, as before.

Message stores tend to grow constantly. Mail continually enters the store, and while many messages are deleted, more are saved. Generally, older messages are accessed less, so storing them on less expensive, slower disks while keeping them accessible to users may be an acceptable way to reduce costs. Depending on the storage mechanisms used for tertiary storage, users should not be aware that their older messages have been moved to a different physical disk.

Tertiary storage in Oracle Mail is enabled through the Housekeeper. The Housekeeper can be set to move older messages to a tablespace named ESTERSTORE, which is reserved for tertiary storage of old messages. The age of messages to be moved to tertiary storage is set through the Age Threshold Housekeeper general parameter.

Note: For the name of mail store tablespaces and their default storage parameters, refer to the $ORACLE_HOME/oes/install/sql/tblspc.sql script.

Tertiary storage can be initially planned as part of an Oracle Mail system, or it can be implemented later. By default, the ESTERSTORE tablespace is created on the same disk as all other tablespaces during the initial Oracle Mail installation.

Table 3–4 gives the four considerations in determining how tertiary storage tablespace is handled.

<table>
<thead>
<tr>
<th>If Tertiary Storage Is:</th>
<th>Then ESTERSTORE Tablespace:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Never enabled for the system</td>
<td>Remains empty.</td>
</tr>
<tr>
<td>Enabled for Oracle Mail</td>
<td>Is set up on a disk different from the primary mail store, either before or after Oracle Mail installation.</td>
</tr>
<tr>
<td>To be implemented for a new Oracle Mail system</td>
<td>Is created on a disk different from the primary mail store, before installation of Oracle Mail.</td>
</tr>
<tr>
<td>To be implemented for an existing Oracle Mail system</td>
<td>Is moved, with the es_tbody table, from its default location on the same disk as the primary mail store onto a separate disk.</td>
</tr>
</tbody>
</table>

See Also: Oracle Database Administrator’s Guide for more information about creating and moving tablespaces.

This section includes the following topics:

- Moving the ESTERSTORE Tablespace
- Enabling Tertiary Storage

Moving the ESTERSTORE Tablespace To move the ESTERSTORE tablespace after Oracle Mail has already been installed:

1. Back up the database.
2. Identify the data files for ESTERSTORE tablespace.
For example, the following query of the data dictionary view DBA_DATA_FILES lists the data file names of the ESTERSTORE tablespace:

```sql
select file_name from dba_data_files
where tablespace_name='ESTERSTORE';
FILE_NAME
------------------------------------------
/usr/app/oracle/product/mailstore/dbf/erstore.dbf
```

3. Take the ESTERSTORE tablespace offline.
   ```sql
   alter tablespace esterstore offline normal;
   ```

4. Copy the data files for the ESTERSTORE tablespace using the operating system, to a different disk.

5. Use the `ALTER TABLESPACE` statement with the `RENAME DATAFILE` clause to change the file names for the ESTERSTORE tablespace to a new location.
   ```sql
   alter tablespace esterstore rename datafile
   '/usr/app/oracle/product/mailstore/dbf/erstore.dbf' to
   'file_name_in_new_location';
   ```

6. Bring the ESTERSTORE tablespace online.
   ```sql
   alter tablespace esterstore online;
   ```

**See Also:** Oracle Database Administrator’s Guide

### Enabling Tertiary Storage

After the ESTERSTORE tablespace has been created, create and configure an instance of the Housekeeper server to enable tertiary storage:

---

**Note:** This procedure combines the Tertiary Storage operation mode with the Expiration task.

---

1. Open the Application Server Control Console for Collaboration Suite.
   **See Also:** "Oracle Enterprise Manager 10g Application Server Control Console for Collaboration Suite" on page 1-3 for information about accessing the Application Server Control Console for Collaboration Suite

2. Click the application server instance where Oracle Mail is installed.

3. Click Mail Application in the System Components section to display the Mail Application page.

4. Select the Housekeeper server and click Stop to bring down the server.

5. Click Housekeeper to display the Housekeeper page.

6. Click Create to create a new Oracle Mail Housekeeper instance.

7. Click the new Housekeeper instance to display its parameter page.

8. Select Tertiary Storage from the Operation Mode list in the Housekeeping Operations section.

9. Select Enabled from the Expiration list in the Housekeeping Operations section.
   When Expiration is enabled, each folder deletes messages older than the number of days specified in the Age Threshold parameter.
10. Ensure all other Housekeeping Operations are disabled.

11. In the **Frequency of Execution of Housekeeper Process** field, enter how often the Housekeeper should perform tertiary storage, in minutes.

   For example, if the Housekeeper process performs tertiary storage once a day, enter 1440 (24*60).

12. In the **Age Threshold** field, enter the age, in days, of messages you want to move to tertiary storage. The default is 30 days.

   For example, if you enter 60 in this field, messages that are 60 days old are moved to tertiary storage.

13. Select **On Startup** from the **Run Task** list.

14. Click **Apply**.

15. Return to the Mail Application page.

16. Select the Housekeeper server and click **Start** to bring up the server.

   The Housekeeper process periodically moves messages of the appropriate age into tertiary storage.

---

**Housekeeper Server Parameters**

**See Also:** "Oracle Mail Housekeeper" on page F-2 for detailed information about Housekeeper parameters

**Managing Housekeeper**

**See Also:** "Managing Oracle Mail Servers and Instances" on page 3-3 for instructions on creating, deleting, and modifying Housekeeper instances

---

**List Server**

List servers enable public distribution list management as well as integration with other messaging services or applications.

Users can own and administer public distribution lists as a way to distribute information to groups of people or as a discussion forum. If desired, restrictions can be placed on membership, requiring prior approval, and on outgoing messages, requiring screening by one or more moderators who control what messages are sent out. For example, a distribution list administrator may screen out advertisements.

The **List Server** is installed with Oracle Mail, with default values set for all List Server parameters. Administrators can modify these values to meet performance or feature requirements. For example, a distribution list with a large number of members requires changing the Oracle Internet Directory Query Entry Return Limit parameter. It must be configured to return a large number of entries to enable the list resolution API to return all the members. This parameter can be configured through the Oracle Internet Directory administration tool **oidadmin**.

**See Also:** Chapter 4, "Directory Administration Tools" in Oracle Internet Directory Administrator’s Guide for information about how to access oidadmin
APIs provided with the List Server enable users to customize distribution lists and messages sent out to a distribution list. For example, marketing campaigns can send special nontransferable offers readable only by the intended recipients. As another example, a user can query a sales information database to create a distribution list of all customers who have made purchases in the past three months. Customers on that distribution list can then receive e-mail coupons with discounts based on the amount of their purchases.

This section includes the following topics:

- List Server Mail Interface
- Archiving Distribution List Posts
- External Distribution Lists
- Distribution List Digests
- Distribution List Bounce Processing
- Multiple Language Responses
- Mail Merge
- List Server Parameters
- Managing List Servers

**List Server Mail Interface**

The List Server features a mail interface that enables distribution list members and owners to perform certain tasks. Depending on the distribution list type and parameters, members and owners can subscribe, unsubscribe, suspend, resume, or invite members to a distribution list. The command messages are sent to a particular e-mail address of the form `list_name-admin@domain`. For example, if a distribution list name is `list@foo.com`, commands are sent to `list-admin@foo.com`.

**See Also:** Oracle WebMail online Help for a complete list of commands with syntax, description, and examples

**Archiving Distribution List Posts**

A distribution list owner can have all posts sent to a distribution list stored as messages in an archive in the NNTP server archives. Such an archive operates as a newsgroup and can be browsed using a standard news client.

An administrator must specify archiving as a property of the distribution list in order to archive messages, as described in Table 2-4, "Distribution List Parameters" on page 2-16.

When a distribution list is archived, a newsgroup is created with a name reflecting the original distribution list. For example, the name of the NNTP archive newsgroup for the distribution list `abc@foo.com` becomes the following:

`ListArchive.abc`

Once a distribution list is created, the domain administrator can begin archiving, which affects only e-mails sent after the archive property is set for a distribution list. No messages prior to that time are archived.
Distribution list archives must have the post parameter disabled. An e-mail is added to the archive only when an e-mail is delivered to the distribution list. E-mails cannot be added to an archive by any other mechanism.

Distribution list archives must be local to the domain of the distribution list. Global newsgroups cannot be associated with a distribution list as an archive.

Administrators can set expiration periods for distribution list archives, such as one month, meaning that messages are only stored in the archive for one month before being deleted. The expiration policy for a distribution list’s archive is the corresponding newsgroup’s expiry attributes.

External Distribution Lists

External distribution lists provide a way for the membership of a distribution list to be stored outside of Oracle Collaboration Suite, while using the List Server to deliver e-mails to such a distribution list. A distribution list owner or domain administrator can configure a distribution list to be external by enabling the external list option in the distribution list properties page, as described in Table 2-4, ”Distribution List Parameters” on page 2-16. A PL/SQL procedure for resolving the addresses of the distribution list members must be created on the Oracle Collaboration Suite Database to which the List Server is connected.

The PL/SQL procedure must have the following syntax:

```sql
procname(session_ID IN NUMBER,
msg_obj IN MAIL_MESSAGE_OBJ,
list_ID IN VARCHAR2,
return_count IN NUMBER,
count OUT NUMBER,
recipients OUT RECIPIENTS_TABLE)
```

- The `session_ID` and `msg_obj` parameters can be used by the PL/SQL procedure developer to call the MAIL_MESSAGE PL/SQL API and fetch any relevant information about the message being processed.

**See Also:** "MAIL_MESSAGE Package" in Chapter 1 of Oracle Mail Application Developer’s Guide for more information about the MAIL_MESSAGE package

- `list_ID` is the e-mail address of the list being resolved.
- `return_count` indicates whether the procedure should return the number of recipients in the list or the recipients itself. A value of 1 indicates the count is to be returned and 0 indicates that the recipients are to be returned.
- The count of the recipients are returned in the `count` variable if the value of `return_count` is 1.
The recipients are returned in the recipients table with one row for each recipient if the value of return_count is 0.

The List Server calls the procedure twice while resolving an external distribution list. Initially, the value passed for the return_count parameter is 1. It receives, in return, the count OUT NUMBER parameter, containing just the number of recipients in the list, and not the list of recipient addresses.

Subsequently, the value passed for the return_count parameter is 0, which causes the procedure to return a table of recipients in the recipients OUT parameter. Each row of that table contains the full e-mail address of a recipient.

Example
The following is an example of how to create the get_cust_list PL/SQL procedure.

1. Open the Application Server Control Console for Collaboration Suite.

   See Also:  "Oracle Enterprise Manager 10g Application Server Control Console for Collaboration Suite" on page 1-3 for information about accessing the Application Server Control Console for Collaboration Suite

2. Click the application server instance where Oracle Mail is installed.

3. Click Mail Application in the System Components section to display the Mail Application page.

4. Click List Server to display the List Server page.

5. Navigate to the list cust_list@acme.com.

6. Edit the properties of the list.

7. Select True in the list box for the Group Is External field.

8. Set the External Procedure parameter to get_cust_list.

9. Connect as es_mail to the Oracle Collaboration Suite Database to which the List Server is connected and create the following PL/SQL procedure:

   ```sql
   procedure get_cust_list(session_id IN NUMBER, 
   msg_obj IN MAIL_MESSAGE_OBJ, 
   listid IN VARCHAR2, 
   return_count IN NUMBER, 
   count OUT NUMBER, 
   recipients OUT RECIPIENTS_TABLE) 
   l_hdr varchar2(2000); 
   l_cnt number; 
   begin 
   -- First get the sender of the message being processed. 
   mail_message.get_header(session_id, msg_obj, 'From', l_hdr); 
   -- Query the table to get the customer count based on the sender's region. 
   if (instr(lower(l_hdr), 'sales_us@foo.com', 1, 1) > 0) 
     then select count(*) into l_cnt from customer_list where region='US'; 
   else 
     select count(*) into l_cnt from customer_list where region!= 'US'; 
   end if;
   ```
-- If the count is requested, then return the count.

    if (return_count = 1)
        then count := l_cnt;
    else

-- Create a recipients_table object.

        recipients := recipients_table();
        recipients.extend(l_cnt);

-- Query the table to get the customer list based on the sender's region.

    if (instr(lower(l_hdr), 'sales_us@foo.com', 1, 1) > 0)
        then select mailid from customer_list where region='US'
            bulk collect into recipients;
    else
        select mailid from customer_list where region!='US'
            bulk collect into recipients;
    end if;

end if;
end if;
end;

The previous example assumes that cust_list@acme.com is a list of customers maintained in a database table by a different application. This procedure uses a table called customer_list, described in Table 3–5.

Assuming that the customer_list table is populated with the customer e-mail IDs and their regions, if the user sales_us@foo.com sends a message to the list, the message is delivered to all the customers in the us region. Mail from any other e-mail address to this list is delivered to all customers on the list, regardless of region.

### Table 3–5  customer_list Table

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Data Type</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>mailid</td>
<td>varchar2 (256)</td>
<td>E-mail ID of a customer</td>
</tr>
<tr>
<td>region</td>
<td>varchar2 (256)</td>
<td>Geographical region of the customer</td>
</tr>
</tbody>
</table>

---

**Note:** The signature of the external lists procedure has changed in this release. To continue to use the Oracle Collaboration Suite Release 2 (9.0.4) signature for external lists, add a flag -external_list_904 in the Process Flags parameter of the List Server and restart the List Server.

---

**Distribution List Digests**

The List Server includes a mail digest feature for distribution lists. This feature enables a member of a distribution list to receive a single message containing all posts in a day or a week to a specific distribution list, rather than receive the individual messages as they are sent.

Distribution list owners control whether digests are enabled on the lists they own or not. If digests are enabled for a distribution list, a member can choose to receive a daily
or a weekly digest, by changing the setting through the Oracle WebMail client or by setting the frequency option in the subscribe command (described in "List Server Mail Interface" on page 3-34).

All mail digests are sent in HTML format with a table of contents listing all the postings in that digest. Users can navigate to the specific post by clicking the subject of the post in the table of contents.

If the distribution list is also configured for archiving, a member can choose not to receive any messages. The user will still be able to browse through the archives of the distribution list and not receive any of the messages sent to the list. By default, a user will receive all messages sent to the distribution list as they are delivered.

**Distribution List Bounce Processing**

It is possible that certain members of a distribution list (especially those in different domains) are invalid or do not exist. In such cases, a DSN is generated when a message is sent to one of these users and this DSN is sent to the sender of the message.

The List Server can be configured to automatically handle these DSNs. If the distribution list owner enables bounce processing for a list (using the Oracle WebMail client), the List Server receives all DSNs and a record is maintained.

Once the number of bounces for a particular e-mail address reaches a preconfigured threshold, the owner of the distribution list is notified of this, along with the action the owner can take to remove the invalid recipient mail ID from the list. The distribution list owner can then unsubscribe the user from the list.

**Multiple Language Responses**

With Oracle Collaboration Suite 10g, all responses sent out by the List Server to users (in response to commands or requests for message moderation, for example), are delivered in the preferred language of the recipient.

**Mail Merge**

Mail merge enables customized mail to be delivered to every member of a distribution list. Distribution list owners or domain administrators must decide on a mail merge tag for a list and set it in the distribution list properties page. The mail merge tag can be a single word or a group of words. This feature can be enabled for a distribution list by providing a value for the merge tag property of the list, as described in Table 2–4, "Distribution List Parameters" on page 2-16. Table 3–6 lists the two types of mail merge that the List Server supports.
For standard mail merge, use the mail merge tag appropriate to a corresponding section of the mail. For example, if the distribution list’s mail merge property is `orcl`, and the mail is addressed with the recipient’s full name, the mail looks like the following:

```
Dear <orcl>recipient_full_name</orcl>,
...
...
```

For PL/SQL mail merge, if you have a PL/SQL `getSalary` function that returns an individual’s salary, given his mail address, you can use it in the mail. For example, you can embed the function call in the mail you send to a list of employees, letting them know their salaries, as follows:

```
Dear <orcl>recipient_full_name</orcl>,
Your salary is <orcl>getSalary(recipient_mail_address)</orcl>.
...
```

**Note:** Database links are not supported for any of the List Server PL/SQL callouts (either for PL/SQL mail-merge or for external distribution lists). The procedures for both of these features must reside on the queue database (the database to which the list server is connected). These procedures can then, in turn, refer to procedures on other databases using database links. The server itself does not support database links.

```
Dear <orcl>recipient_full_name</orcl>,
Your salary is <orcl>getSalary(recipient_mail_address)$dblink</orcl>. 
...
```

**Example**

**Note:** The following example assumes that distribution lists and users have been set up correctly with the List Server process configured and running.
The following example shows how to create the `get_sal` PL/SQL procedure:

1. Open the Application Server Control Console for Collaboration Suite.

   **See Also:** "Oracle Enterprise Manager 10g Application Server Control Console for Collaboration Suite" on page 1-3 for information about accessing the Application Server Control Console for Collaboration Suite.

2. Click the application server instance where Oracle Mail is installed.

3. Click Mail Application in the System Components section to display the Mail Application page.

4. Navigate to the list `all_emp@acme.com`.

5. Edit the properties of the list and set the Group merge tag parameter to mail merge.

6. Connect as `es_mail` to the mail store supported by the List Server and create the following PL/SQL procedure:

   ```sql
   CREATE OR REPLACE FUNCTION get_sal(email IN VARCHAR2) RETURN VARCHAR2
   mon varchar2(10);
   tmp number;
   ret varchar2(4000);
   begin
   -- get the month and salary value for the user
   select month, salary into mon, tmp from emp_payroll where employee=email;

   -- concatenate to form a string
   ret := mon || ' is $' || tmp;

   return ret;
   end;
   ```

The procedure assumes that some application puts employee payroll information into a database table. Table 3–7 lists the columns contained in the `emp_payroll` table in the previous example.

### Table 3–7 Example emp_payroll Table

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Data Type</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>employee</td>
<td>varchar2(1000)</td>
<td>Mail ID of an employee</td>
</tr>
<tr>
<td>month</td>
<td>varchar2(10)</td>
<td>Month for which the salary is stored</td>
</tr>
<tr>
<td>salary</td>
<td>number</td>
<td>Salary of the employee</td>
</tr>
</tbody>
</table>

Following is an example of a message with mail merge tags embedded in it. This sends a mail to each recipient in the distribution list `all_emp@acme.com` with each person’s salary details.

Dear `<mailmerge>recipient_full_name</mailmerge>`,

Your salary for the month of `<mailmerge>get_sal(recipient_mail_address)</mailmerge>` been credited to your account.

Thanks
Payroll
Scheduled Mail Delivery

Scheduled mail delivery enables administrators to schedule mail delivery to occur at a particular time, such as during low traffic hours, possibly minimizing server loads during peak usage hours. Otherwise, delivery of very large messages or of mailings to distribution lists with large numbers of subscribers can degrade performance.

This feature can be enabled by providing a value for the mail merge property of the distribution list. Specify the delivery time for a message by putting the schedule mail delivery tag anywhere in the mail. The following example illustrates this, using orcl as the tag for the mail merge property of the distribution list:

```
<orcl>send_schedule=DD-MON-YYYY hh24:mi [+/+TZH:TZM]</orcl>
```

```
<orcl>send_schedule=23-JUN-2003 21:45 -08:00</orcl>
```

Note: +/- before TZH:TZM is required.

Table 3–8 lists parameter descriptions for the send_schedule delivery tag.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DD</td>
<td>The date</td>
</tr>
<tr>
<td>MON</td>
<td>The three letter abbreviation for the month</td>
</tr>
<tr>
<td>YYYY</td>
<td>The year</td>
</tr>
<tr>
<td>hh24</td>
<td>The time in a twenty-four hour period</td>
</tr>
<tr>
<td>mi</td>
<td>The time in minutes</td>
</tr>
<tr>
<td>TZH</td>
<td>The optional time zone hour offset</td>
</tr>
<tr>
<td>TZM</td>
<td>The optional time zone minute offset</td>
</tr>
</tbody>
</table>

If TZH and TZM are not specified, the List Server uses the sender’s time zone to schedule delivery of the mail.

List Server Parameters

See Also: "Oracle Mail List Server" on page F-25 for detailed information about List Server parameters

Managing List Servers

See Also: "Managing Oracle Mail Servers and Instances" on page 3-3 for instructions on creating, deleting, and modifying List Server instances

NNTP Server

Network News Transport Protocol (NNTP) is used to distribute, query, post, and retrieve news articles from the Internet using a reliable stream-based mechanism. NNTP enables news-reading clients to select news articles from a central database, enabling subscribers to retrieve only the articles they want to read. The net news model provides indexing, cross-referencing, and message expiration. For
server-to-server interaction, NNTP is designed to efficiently transmit net news articles over a reliable communication channel. Receiving and sending news articles is an interactive mechanism so that articles already present are not retransmitted.

The Oracle Mail NNTP server can be used immediately upon installation and configuration of Oracle Collaboration Suite. In addition, the NNTP server uses the Oracle Collaboration Suite Database as an article repository and the Oracle Collaboration Suite Infrastructure directory service to store operational parameters. All protocol exchanges are performed over a stream-based connection.

During installation, default values are set for all Oracle Mail NNTP server parameters. Administrators can modify these values to meet performance or feature requirements of their site.

This section includes the following topics:

■ About News Servers
■ Controlling News Storage
■ Article Caching for Performance
■ NNTP Processes
■ NNTP Server Parameters
■ Managing NNTP Servers

About News Servers

One or more news servers used by the same community of users is called a news site. Such sites can exchange news articles, transmitting locally posted articles to other sites to provide (and serve) a wider audience. News servers that exchange news articles are called peers.

News articles collected into similar-topic groupings are called newsgroups, such as articles about sailing or articles about Oracle Database. A peer can be configured to download articles only for particular newsgroups.

Users of news services exchange information by posting and reading news messages. Posting means a news user composes a message in a standard newsreader and sends it to the news server for storage, after which other users can read it.

The NNTP service maintains a list of peer servers, the newsgroups each peer server is configured to receive, and a list of newsgroups that the NNTP service delivers. The administrator for each newsgroup specifies the peers to be fed articles from that newsgroup. Once peers and newsgroups are configured and the feed rules are set, the service is ready for posting, reading, and feeding news.

The NNTP inbound server receives news articles from clients and posts them to the Oracle Collaboration Suite Database.

The NNTP outbound server takes articles from the Oracle Collaboration Suite Database and exchanges those articles with various peers.

Controlling News Storage

News articles are stored in the Oracle Collaboration Suite Database. Inbound and outbound servers connected to the Oracle Collaboration Suite Database only handle newsgroups created in that database. News articles automatically expire in strict accordance with the Housekeeper process.
The NNTP service also creates a history record to track articles already received for which new entries are rejected by the server. Having a long expiry history avoids repeated entry of the same article into the mail store. History records are also subject to expiry and collection by the Housekeeper service.

The storage needed for NNTP service depends on the volume of incoming traffic and the expiry policy of the server instances, such as how long articles are retained. Each article’s expiration date and history record are established when it is stored, and cannot later be changed.

**Article Caching for Performance**

You can configure the NNTP inbound server to cache articles in memory, improving performance for articles that are requested repeatedly, because no new Oracle Collaboration Suite Database access is needed. Caching can only be done for articles less than 4 KB in size. You can adjust the total cache size to accommodate the number of articles you want to cache, to provide newsreaders with quicker response times for popular articles.

**NNTP Processes**

There are two types of newsgroup exchanges, which are known as feeds:

- **Inbound**: The NNTP server receives the feed
- **Outbound**: The NNTP server transmits the feed

The processes required for NNTP service are shared between the inbound and outbound servers.

This section includes the following topics:

- NNTP Inbound Server
- NNTP Outbound Server

**NNTP Inbound Server**

The NNTP inbound server has two functions:

- Incoming feed: accepts news articles and waits for connections from remote hosts
- Read or post: accepts and waits for connections from newsreading clients and enables them to post or read news articles

The NNTP inbound server identifies the connecting host for each connection it receives. For a peer, the server prepares to receive the news feed. If the connecting host is not a peer, it is a newsreader and only has permission to read and post articles.

When a newsgroup is configured, administrators can specify the number of peers that must be sent articles for that newsgroup. Based on the number of peers specified, the NNTP inbound server creates queues of incoming messages that must be passed on to other peers.

**NNTP Outbound Server**

The NNTP outbound server periodically connects to peer news servers configured to receive news feeds and offers a list of new articles queued for sending. Peer server parameters determine what is offered and what is acceptable or rejected by the peer.

See Also: "Managing Peer Servers" on page 2-24 for more information
The NNTP outbound server maintains a list specifying the newsgroups for each peer server. When the outbound server contacts a peer and provides a list of new articles, the remote host’s response determines which articles are sent.

**NNTP Server Parameters**

*See Also:* "Oracle Mail NNTP Inbound Server" on page F-12 and "Oracle Mail NNTP Outbound Server" on page F-15 for detailed information about NNTP server parameters

**Managing NNTP Servers**

*See Also:* "Managing Oracle Mail Servers and Instances" on page 3-3 for instructions on creating, deleting, and modifying NNTP server instances
This chapter discusses the Oracle Collaboration Suite 10g WebMail (Oracle WebMail) client and how it is managed.

This chapter includes the following topics:

- Oracle WebMail Client Overview
- Oracle WebMail Tool Kit Default Settings
- Oracle WebMail Client Properties
- Oracle WebMail Client Log Files Location
- Oracle Mail Portlet API

Oracle WebMail Client Overview

The Oracle WebMail client is a thin client that gives users a simple and fast means to access messages and other self-service features through a Web browser. A user points his browser to a predetermined URL to log in to his e-mail account and sees the inbox rendered dynamically.

All programs execute in the Oracle Application Server, including the logic to render a user’s folders, messages, public directory, and personal address book. There is no processing or data storage on the desktop. The browser acts merely as a keyboard and screen.

Oracle WebMail provides a standard Web mail solution, along with a tool kit that can extend and modify this standard solution.

The Oracle WebMail client runs on the Oracle Collaboration Suite Applications tier. The user does not have to download any information or software, as they do when using fat clients, such as Microsoft Outlook or Netscape Messenger. Other than entering a URL in a browser (which can be bookmarked), no configuration of the user’s local computer is necessary.
Note: Initially, default Oracle WebMail settings are such that attachments are not cached on the client’s disk, for security and privacy reasons. Additionally, due to an issue in Microsoft Internet Explorer, this prevents users from opening attachments inline using that browser.

For example, clicking a text attachment and selecting Open from the subsequent attachment dialog will fail. The default text editor application for the user will start and complain that the file could not be found.

Caching settings are all defined and configurable in the $ORACLE_HOME/um/client/config/um_sso.conf file. Administrators can alter caching behavior (although they may sacrifice security for the functionality described in the preceding paragraph) by adjusting values in that file (the file contains informative instructions indicating which lines to comment or uncomment to achieve different behavior).

Note, however, that if administrators enable Secure Sockets Layer (SSL), they must relax caching settings in this configuration file or attachments will not be downloadable at all using Internet Explorer.

---

Oracle WebMail Tool Kit Default Settings

Oracle WebMail is designed to provide a number of ways to customize the application to fit specific needs, from changing the look-and-feel using modifications to the UIX pages, to changing application page flow.

State File
The state file contains XML defining the navigation behavior of the Oracle WebMail client. This file facilitates defining state transitions in the client (when the user moves from one state to another) and managing the end state to present to the user.

The location of the state file for the Oracle WebMail client is determined by the toolkit.statefile property:

```
toolkit.statefile=%ORACLE_HOME%/um/client/config/statefile.xml
```

Note: Percent symbols (%) in the oc4j.properties file are substituted to reflect the real directory path during installation.

The toolkit.statefile property is set in the $ORACLE_HOME/j2ee/OC4J_OCSClient/config/oc4j.properties file.

---

Oracle WebMail Client Properties

This section includes the following topics:

- Oracle WebMail oc4j.properties File Properties
Oracle WebMail Client Properties

- Service Registry Dependency
- Configuring SSL Between Oracle WebMail and Oracle Internet Directory

Oracle WebMail oc4j.properties File Properties

Table 4–1 describes the Oracle WebMail client properties in alphabetical order. Values given for the properties indicated for database and LDAP connection pooling while using OJMA, and for database connection pool parameters, are just examples and should actually be determined based on the number of users, and system load.

To edit these properties, change their values in the $ORACLE_HOME/j2ee/OC4J_OCSClient/config/oc4j.properties file.

Note: Oracle WebMail client properties can also be edited in the $ORACLE_HOME/opmn/config/opmn.xml file.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Acceptable Values</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>client.corporate.url</td>
<td>Link to the corporate logo that is displayed in the application.</td>
<td>Any URL that points to a corporate logo</td>
<td><a href="http://otn.oracle.com/products/cs/index.html">http://otn.oracle.com/products/cs/index.html</a></td>
</tr>
<tr>
<td>client.faxsubtab</td>
<td>Configure to show a subtab for fax messages on the message list page.</td>
<td>Show or Hide</td>
<td>Show</td>
</tr>
<tr>
<td>client.image.corporate</td>
<td>Path to image to customize Oracle WebMail with corporate logo.</td>
<td>Any URL that points to an image</td>
<td>/um/images/ocs_brand_header.gif</td>
</tr>
<tr>
<td>client.image.product</td>
<td>Path to location of the product logo in Oracle WebMail.</td>
<td>Any URL that points to an image</td>
<td>/um/images/mail_subbrand.gif</td>
</tr>
<tr>
<td>client.ldapsearch.maxresult</td>
<td>Maximum number of results returned from a search of Oracle Internet Directory from Oracle WebMail. End users whose searches return more matches than this are notified that additional results exist, but that only this maximum number are shown.</td>
<td>Any integer</td>
<td>500</td>
</tr>
<tr>
<td>client.mail.attachment.defaultname</td>
<td>File name to be used when attachment has no associated file name.</td>
<td>A file name using the 27.3 naming convention</td>
<td>UnnamedAttachment.txt</td>
</tr>
<tr>
<td>client.mail.attachment.downloadlongfilename</td>
<td>These parameters are used in the ViewAttachment.java file and should not be modified without first contacting Oracle Support.</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>client.mail.attachment.downloadmaxencodedlen</td>
<td></td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>client.mail.enforceencodedHTMLfonts</td>
<td>If true, original fonts are to be used for HTML.</td>
<td>true or false</td>
<td>true</td>
</tr>
<tr>
<td>client.mail.messagetransport</td>
<td>If SMTP, messages are sent through the SMTP server; database uses direct database interaction.</td>
<td>SMTP or database</td>
<td>SMTP</td>
</tr>
</tbody>
</table>
Oracle WebMail Client Properties

### Table 4–1 (Cont.) Oracle WebMail Client Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Acceptable Values</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>client.mail.sharedfoldercacheacherefresh</td>
<td>Configure to refresh the shared folder cache. Enter -1 to never refresh; 0 to always refresh; and a number n to refresh no more than once every n seconds.</td>
<td>-1, 0, or n</td>
<td>600</td>
</tr>
<tr>
<td>client.mail.showsharedfoldersinlists</td>
<td>Configure to show shared folders in lists. Enter -1 to never show shared folders; 0 to show folders immediately; and a number n to wait for the nth time before showing the list.</td>
<td>-1, 0, or n</td>
<td>0</td>
</tr>
<tr>
<td>client.mail.translate.INBOX</td>
<td>If true, the INBOX folder is automatically translated to the user’s locale. If false, the INBOX is displayed in English.</td>
<td>true or false</td>
<td>true</td>
</tr>
<tr>
<td>client.message.charset.default</td>
<td>Default character set to use for outgoing messages.</td>
<td>Any valid character set</td>
<td>UTF-8</td>
</tr>
<tr>
<td>client.message.charset.default.iana</td>
<td>Default character set to use when sending a message. For backward compatibility, the non-IANA property client.message.charset.default can be defined, and it will take precedence.</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>client.message.view.charset.default.iana</td>
<td>Default character set to use when viewing a message if Oracle WebMail is unable to determine the character set. For backward compatibility, the non-IANA property client.message.view.charset.default can be defined, and it will take precedence.</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>client.privacystatement.url</td>
<td>Link to the privacy statement.</td>
<td>Any valid URL</td>
<td><a href="http://www.oracle.com">http://www.oracle.com</a></td>
</tr>
<tr>
<td>client.voicesubtab</td>
<td>Configure to show a subtab for voice messages on the message list page.</td>
<td>Show or Hide</td>
<td>Show</td>
</tr>
<tr>
<td>jdbc.connection.debug</td>
<td>If true, enables debugging JDBC connections.</td>
<td>true or false</td>
<td>false</td>
</tr>
<tr>
<td>jvm.command.line.option</td>
<td>Set the JVM heap size.</td>
<td>-Xmx512m</td>
<td></td>
</tr>
<tr>
<td>mail.debug</td>
<td>If true, enables debugging OJMA API for Oracle Mail.</td>
<td>true or false</td>
<td>false</td>
</tr>
<tr>
<td>MaxTelephonePinDigits</td>
<td>Maximum number of digits in voice-mail PINs.</td>
<td>Any integer</td>
<td>12</td>
</tr>
<tr>
<td>MinTelephonePinDigits</td>
<td>Minimum number of digits in voice-mail PINs.</td>
<td>Any integer</td>
<td>7</td>
</tr>
<tr>
<td>oracle.mail.admin.ldapDebug</td>
<td>Enables debugging for the administration ESDS API.</td>
<td>true or false</td>
<td>false</td>
</tr>
<tr>
<td>oracle.mail.admin.policy.indexoldmessages</td>
<td>This parameter controls whether existing user messages are indexed or not. If true, text indexing of existing messages is enabled. Use this parameter in conjunction with the Text Indexing user parameter set in Oracle WebMail.</td>
<td>true or false</td>
<td>false</td>
</tr>
</tbody>
</table>
### Oracle WebMail Client Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Acceptable Values</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>oracle.mail.admin.ui.ojma</td>
<td>Enables debugging for the administration OJMA API.</td>
<td>true or false</td>
<td>false</td>
</tr>
<tr>
<td>Debug</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A valid value is one of the following:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- ISO2022-JP-OUTLOOK: ISO-2022-JP compatible with Microsoft Outlook. Half-width Kana letters are encoded using full-width equivalents. This is the default setting. Oracle recommends this option if a majority of users or their associates use Microsoft Outlook.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- ISO2022-JP-OUTLOOK-HWKANA: ISO-2022-JP compatible with Microsoft Outlook. Half-width Kana letters are encoded as is. This option allows the recipient to view half-width Kana letters in the original message if their client supports them.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This property must be added to the oc4j.properties file manually.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>oracle.mail.client.prefs.</td>
<td>Enables access to automatic reply features and options. If true, enables automatic reply functions for end users.</td>
<td>true or false</td>
<td>true</td>
</tr>
<tr>
<td>autoreply</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>oracle.mail.client.prefs.</td>
<td>Every incoming message receives an automatic reply with the original message copied. Requires oracle.mail.client.prefs.autoreply to be enabled.</td>
<td>true or false</td>
<td>true</td>
</tr>
<tr>
<td>autoreply.echo</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>oracle.mail.client.prefs.</td>
<td>Enables the user to select the reject option in Oracle WebMail. With this option enabled, the server rejects all incoming messages. Requires oracle.mail.client.prefs.autoreply to be enabled.</td>
<td>true or false</td>
<td>true</td>
</tr>
<tr>
<td>autoreply.reject</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>oracle.mail.client.prefs.</td>
<td>Enables the reply option in Oracle WebMail. With this option enabled, every sender receives one automatic reply regardless of the amount of messages sent by that sender. Requires oracle.mail.client.prefs.autoreply to be enabled.</td>
<td>true or false</td>
<td>true</td>
</tr>
<tr>
<td>autoreply.reply</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>oracle.mail.client.prefs.</td>
<td>Enables the vacation option in Oracle WebMail. With this option enabled, every incoming message receives an automatic reply with the original message copied. Requires oracle.mail.client.prefs.autoreply to be enabled.</td>
<td>true or false</td>
<td>true</td>
</tr>
<tr>
<td>autoreply.vacation</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 4-1 (Cont.) Oracle WebMail Client Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Acceptable Values</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>oracle.mail.client.prefs.autoreplymimesizelimit</td>
<td>Limits the size of automatic reply MIME messages.</td>
<td>Any integer</td>
<td>-1</td>
</tr>
<tr>
<td>oracle.mail.client.prefs.maxattachmentsize</td>
<td>Set the maximum size limit in bytes of an e-mail attachment.</td>
<td>Any integer</td>
<td>5000000</td>
</tr>
<tr>
<td>oracle.mail.client.prefs.maxMessagesShown</td>
<td>Sets the maximum number of messages shown in Oracle WebMail.</td>
<td>Any integer</td>
<td>1000</td>
</tr>
<tr>
<td>oracle.mail.client.prefs.readreceipt.response</td>
<td>Sets the read-receipt options when a user receives a message that requests a read-receipt notification.</td>
<td>disable, prompt, automatic</td>
<td></td>
</tr>
<tr>
<td>oracle.mail.sdk.esmail.cache_inactivity_timeout</td>
<td>Number of seconds to wait for a connection before the ESDS client connection pool times out.</td>
<td>Any integer values OJMA connection pool settings</td>
<td>300</td>
</tr>
<tr>
<td>oracle.mail.sdk.esmail.connection_max_limit</td>
<td>Maximum number of connections in the Oracle mail sdk es_mail connection pool.</td>
<td>Any integer values OJMA connection pool settings</td>
<td>10</td>
</tr>
<tr>
<td>oracle.mail.sdk.esmail.connection_min_limit</td>
<td>Determines the initial or minimum number of connections created in the connection pool. Oracle recommends keeping this limit as low as possible to avoid holding on to unused database connections.</td>
<td>Depends on factors, such as the number of users and system load</td>
<td>1</td>
</tr>
<tr>
<td>oracle.mail.sdk.esmail.db_timing</td>
<td>Set to true to get database timing information. By enabling this property, you can view the Active count (total number of active connections) and Cache count (total number of connections) in the database connection pool.</td>
<td>true or false</td>
<td>false</td>
</tr>
<tr>
<td>oracle.mail.sdk.esmail.driver_type</td>
<td>Determines the type of JDBC driver to be used for the database connection pool.</td>
<td>oci8, thin (recommended in non-Oracle Real Application Clusters environment)</td>
<td>oci8</td>
</tr>
<tr>
<td>oracle.mail.sdk.esmail.encryption</td>
<td>Disables password encryption, which is mandatory in Oracle Collaboration Suite. Can be disabled for better performance.</td>
<td>true or false</td>
<td>true</td>
</tr>
<tr>
<td>oracle.mail.sdk.esmail.ldap_debug</td>
<td>If true, enables debugging OJMA API for Oracle Internet Directory.</td>
<td>true or false</td>
<td>false</td>
</tr>
<tr>
<td>oracle.mail.sdk.esmail.ojma_debug</td>
<td>Controls the debug output from the OJMA layer.</td>
<td>true or false</td>
<td>false</td>
</tr>
</tbody>
</table>
Table 4–1  (Cont.) Oracle WebMail Client Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Acceptable Values</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>oracle.mail.sdk.esmail.timing</td>
<td>Set to true to get timing information for various e-mail operations, such as listing folders, opening a folder, and copying messages.</td>
<td>true or false</td>
<td>false</td>
</tr>
<tr>
<td>oracle.ocsclient.smtp.host</td>
<td>Note: This property overwrites the value in the service registry.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>oracle.ocsclient.smtp.port</td>
<td>Note: This property overwrites the value in the service registry.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>toolkit.clientdir</td>
<td>Directory under $ORACLE_HOME/j2ee/OC4J_OCSClient/applications/UMClientApp/um_client where the UIX pages reside. Default value should not be changed.</td>
<td>Any valid path under $ORACLE_HOME/j2ee/OC4J_OCSClient/applications/UMClientApp/um_client where the UIX pages reside</td>
<td></td>
</tr>
<tr>
<td>toolkit.controller.type</td>
<td>Parameter used by the application controller. Default value should not be changed.</td>
<td>uix</td>
<td></td>
</tr>
<tr>
<td>toolkit.controller.URL</td>
<td>URL for accessing the client framework controller.</td>
<td>A valid URL that accesses the client framework controller /templates/um/trafficcop</td>
<td></td>
</tr>
<tr>
<td>toolkit.debugmode</td>
<td>Whether to debug the OESContext.</td>
<td>TRUE or FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>toolkit.helpdir</td>
<td>Relative URL path to the online Help files.</td>
<td>Any valid path to directories containing the associated files /um/help/</td>
<td></td>
</tr>
<tr>
<td>toolkit.imagedir</td>
<td>Relative URL path to the images files.</td>
<td>Any valid path to directories containing the associated files /um/images/</td>
<td></td>
</tr>
<tr>
<td>toolkit.jslibdir</td>
<td>Relative URL path to the javascript files.</td>
<td>Any valid path to directories containing the associated files /um/scripts/</td>
<td></td>
</tr>
<tr>
<td>toolkit.logdirectory</td>
<td>Path to the directory containing the Oracle WebMail client log files.</td>
<td>A valid file path containing the log files %ORACLE_HOME%/um/log</td>
<td></td>
</tr>
<tr>
<td>toolkit.logfilecount</td>
<td>Number of log files to rotate.</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>toolkit.logfilename</td>
<td>Name of the Oracle WebMail client log file.</td>
<td>WebMail_Client</td>
<td></td>
</tr>
<tr>
<td>toolkit.logfilesize</td>
<td>Maximum size of the log file in bytes before rotation.</td>
<td>1000000</td>
<td></td>
</tr>
<tr>
<td>toolkit.loghostclient</td>
<td>Name for the Oracle WebMail Client host.</td>
<td>%machinehost%</td>
<td></td>
</tr>
</tbody>
</table>
Since Oracle Collaboration Suite 10g Release 10.1.1, Oracle WebMail no longer requires administrators to specify SMTP configuration information (specifically, hostname and port) in the oc4j.properties file. Instead, Oracle WebMail retrieves the information from the service registry in Oracle Internet Directory. If overwriting the SMTP host and port is necessary, Table 4–2 lists two properties that can be added to the oc4j.properties file (and remove all existing instances of these properties, if any), such that all SMTP configuration can be centrally managed through the service registry.

### Table 4–2  Overwriting SMTP Host and Port Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Acceptable Values</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>oracle.ocsclient.smtp.host</td>
<td>Host name of the SMTP server.</td>
<td>Any valid host name</td>
<td>NA</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This property overwrites the value in the Oracle Internet Directory service registry.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>oracle.ocsclient.smtp.port</td>
<td>Port number of the SMTP server.</td>
<td>Any integer</td>
<td>NA</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This property overwrites the value in the Oracle Internet Directory service registry.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Configuring SSL Between Oracle WebMail and Oracle Internet Directory

Oracle WebMail relies on Oracle Internet Directory for authentication, through Oracle Application Server Single Sign-On, to look up users in the directory, and to access the user’s address book. The connection between Oracle WebMail and Oracle Internet Directory can be secured by configuring Secure Sockets Layer (SSL).

To configure SSL for the connection between Oracle WebMail and Oracle Internet Directory, add the following properties to the oc4j.properties file:

```
oracle.mail.ldap.connectssl=true
oracle.mail.ldap.sslport=4031
```

Oracle WebMail Client Log Files Location

Oracle WebMail log files are located in the $ORACLE_HOME/um/log/Webmail_Client directory, by default. Oracle WebMail logging is configured by properties in the oc4j.properties file for the OC4J_OCSClient application.

In this file:

- `toolkit.loghostclient` maps to a field in the log files to indicate what computer generated the log file.
- `toolkit.loglevel` indicates the amount of logging to do, and can be set to one of the following values: `internalerror`, `error`, `warning`, `notification`, or `trace`.
- `toolkit.debugmode` controls whether or not debug information is logged for use of the ESDS API by the Oracle WebMail client code.

Oracle Mail Portlet API

Oracle Mail Portlet API is provided for Oracle Application Server Portal (OracleAS Portal) to access e-mail user information. A user can log in to OracleAS Portal and get unread e-mail and voice mail message counts, as well as header information of the most recently received e-mails from the Inbox. A user can also customize the mail portlet to prioritize messages and set up filters. The portlet also provides links to the Oracle WebMail client to view messages in detail.

All programs execute in the Oracle Application Server, including the logic to render a user’s Inbox folder and message headers. There is no processing or data storage on the desktop. The portlet acts merely as a screen.

Oracle Mail Portlet API runs on the Oracle Collaboration Suite Applications tier. The user does not have to download any information or software. Oracle Mail Portlet API can be accessed only through OracleAS Portal with server-to-server authentication. No configuration of the user’s local computer is necessary.

Table 4–3 describes the Oracle Mail Portlet API properties.

To edit these properties, change their values in the $ORACLE_HOME/j2ee/OC4J_Mail/config/oc4j.properties file.

---

**Note:** Values given for the properties indicated for database and LDAP connection pooling while using OJMA, and for database connection pool parameters, are just examples and should actually be determined based on the number of users, and system load.
Table 4–3 Oracle Mail Portlet API Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Acceptable Values</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>oracle.cabo.image.laf.browser.lightAccentColorOffset</td>
<td>Renders the color of Oracle WebMail and should not be modified.</td>
<td></td>
<td>362914</td>
</tr>
<tr>
<td>oracle.mail.portlet.debug</td>
<td>If true, specifies the Oracle WebMail title link as https.</td>
<td>true or false</td>
<td>false</td>
</tr>
<tr>
<td>oracle.mail.portlet.httpsToWebmail</td>
<td>Number of seconds to wait for a connection before the esds client connection pool times out.</td>
<td>Any integer</td>
<td>300</td>
</tr>
<tr>
<td>client.mail.spellcheck.dictionaries</td>
<td>Path to the directory containing spell checker dictionaries.</td>
<td>Path to any valid spell checker dictionary</td>
<td>%ORACLE_HOME%/um/client/spellcheck/dictionaries</td>
</tr>
<tr>
<td>oracle.mail.ws.debug</td>
<td>If true, enables debugging e-mail display Web services.</td>
<td>true or false</td>
<td>false</td>
</tr>
<tr>
<td>oracle.ocsclient.directory.cache.enable</td>
<td>If true, Directory Cache is enabled and periodically updated. If false, Directory Cache remains in pass-through mode.</td>
<td>true or false</td>
<td>true</td>
</tr>
<tr>
<td>oracle.ocs.ldappool.incrementsize</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>oracle.ocs.ldappool.initialize</td>
<td>5</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>oracle.ocs.ldappool.maxsize</td>
<td>10</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>oracle.ocs.ldappool.minsize</td>
<td>5</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>oracle.ocs.ldappool.proxydn</td>
<td>cn=EmailServerContainer,cn=Products,cn=OracleContext</td>
<td>cn=EmailServerContainer,cn=Products,cn=OracleContext</td>
<td></td>
</tr>
<tr>
<td>oracle.ocs.ldappool.reconnecttime</td>
<td>30</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td>oracle.ocs.ldappool.shrinkinterval</td>
<td>1800</td>
<td>1800</td>
<td></td>
</tr>
<tr>
<td>oracle.ocs.ldappool.timeoutinterval</td>
<td>30</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td>oracle.um.ctf.sessiontracker.reportinterval</td>
<td>Set Session Tracker attributes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: Changes made to the oc4j.properties file will also affect the Oracle Web Access Client.

Oracle Mail Display Web Services log files are located in the $ORACLE_HOME/opmn/logs directory.
This chapter discusses **Directory Cache**, a component of Oracle Mail that, when enabled, builds an in-memory cached copy of the corporate directory, enabling faster lookup of user information when using the Oracle WebMail client.

Additionally, when Directory Cache is enabled, **auto-complete** and **address resolution** features associated with Directory Cache are enabled.

This chapter discusses the following topics:

- About Directory Cache
- Enabling Directory Cache

### About Directory Cache

Directory Provider provides data access to the corporate directory (Oracle Internet Directory). It creates a *directory cache* upon startup, and allows direct connection to LDAP. While Directory Cache is being built, or if Directory Cache is disabled, it is said to be in *pass-through mode*.

Once the building of Directory Cache is complete, performance improves dramatically. The cache refreshes itself periodically, every 24 hours by default.

This section discusses the following topics:

- Directory Cache Search Behavior
- Directory Cache Default Behavior
- Location of Directory Cache Logs

### Directory Cache Search Behavior

The search behavior varies depending upon whether Directory Cache is enabled or not. Directory Cache is a *crawler*, and will span fields. However, during pass-through, queries work only on single fields.

For example, if the following searches are performed for a user that exists in Directory Cache, such as Andrew Edwards *andrew.edwards@acme.com*, the following results are returned:

- Search for *andre* will return Andrew Edwards from both the pass-through and the cache.
- Search for *andrew e* will return Andrew Edwards from the cache but will not return Andrew Edwards from the pass-through.

When searching in pass-through mode, the following attributes are used:
Enabling Directory Cache

The following attributes are indexed, for searching, in the cache:

givenname
sn
middlename
displayName
mail
dn

Directory Cache Default Behavior

Directory Cache refreshes itself periodically, every 24 hours by default.
During cache update, every query is retried three times when there are failures (with a one minute sleep). If the third query fails, errors are logged and the cache update is aborted until the next time.

Location of Directory Cache Logs

Directory Cache logs are contained in the container's log file, located in the $ORACLE_HOME/opmn/logs/directory.

Logs are set to INFO by default in Oracle WebMail. To get more detailed log messages, raise the log level in the oc4j.properties file for the Oracle WebMail client.

See Also: "Oracle WebMail Client Log Files Location" on page 4-9 for more information about setting log levels in Oracle WebMail

Enabling Directory Cache

To enable Directory Cache, set the following parameter in the $ORACLE_HOME/j2ee/OC4J_OCSClient/config/oc4j.properties file:

# to enable Directory Cache
oracle.oscclient.directory.cache.enable=true

In addition, the following parameter specifies how often Directory Cache refreshes its in-memory copy with the data from the live Oracle Internet Directory:

# how often the directory cache updates, in hours
oracle.oscclient.directory.updateinterval=24
This chapter discusses Oracle Mail security issues including antispam and antivirus solutions, Virus Scrubber, and virus management using PL/SQL scripts.

This chapter includes the following topics:

- Oracle Mail Security Overview
- SSL and TLS
- Antispam Methods
- Symantec AntiVirus Scan Engine
- Virus Scrubber
- Virus Scanning and Removal Using PL/SQL Scripts

**Oracle Mail Security Overview**

E-mail system security has many aspects and implications. Each component of the system has potential vulnerabilities in addition to possible breaches through user error or violation of documented security policies. Examples include careless password management or cooperation with deceptive phone calls purporting to be from information technology (IT) workers.

Security issues include:

- Components of the e-mail system to identify the areas to consider when designing a secure architecture
- Elements of security to consider in the design, such as password policies

This section includes the following topics:

- E-mail System Component Security
- Network Security
- Firewalls
- Nontechnical Considerations

**E-mail System Component Security**

Each core component of an e-mail system has unique security issues and vulnerabilities that you must address in designing your system and security policies. Security decisions must often balance the goals of maximum protection and unlimited access. Most decisions that increase security inevitably reduce the level of access for ordinary users.
This section discusses the following e-mail system core components:

- **Information Storage Database**
- **Oracle Collaboration Suite Applications Tier**
- **Identity Management Infrastructure**
- **Mail Clients**

**Information Storage Database**
The information storage database in an e-mail system consists of a database on which message bodies, message header information, and pointers to messages—for both incoming and outgoing messages—are stored. Oracle Mail employs the Oracle Collaboration Suite Database, an Oracle Database 10g database, to store all messages.

Table 6–1 describes the elements providing security in the message store.

<table>
<thead>
<tr>
<th>Message Store Element</th>
<th>Security Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Database 10g</td>
<td>Traditional database security prevents unauthorized access.</td>
</tr>
<tr>
<td>Data access management</td>
<td>Normal database authentication mechanisms protect e-mail, too, and can be restricted to specific accounts or trusted users.</td>
</tr>
<tr>
<td>Signed e-mail and S/MIME support</td>
<td>Mail clients can provide e-mail security with digital signatures and S/MIME, part of an overall security strategy supported by Oracle to preserve message integrity.</td>
</tr>
</tbody>
</table>

**Oracle Collaboration Suite Applications Tier**
In the Oracle Collaboration Suite Applications tier, more security vulnerabilities arise because this is the access point for most users. Security concerns and ease of use for end users must be balanced to build a workable implementation.

Because protocol servers, such as IMAP, POP, or SMTP, are potential targets for attack by hackers looking for security weaknesses, you should enable only the protocols you require. Where appropriate, enforce authentication for all client connections, and consider using SSL for the underlying network connection. For SMTP, authentication can prevent inbound mail traffic. In this case, ensure that the antispam, antirelay, and antivirus controls are configured appropriately to minimize the risks posed by incoming mail traffic.

For HTTP servers, only minimum information should be available through any Web servers giving access through Web clients. Secure access to any URL except for the thin client. To protect the security of e-mail data and passwords, enable SSL access only through the thin clients.

Providing adequate security of the Oracle Collaboration Suite Applications tier, particularly the SMTP server, can be problematic because by design, SMTP accepts and routes inbound traffic to its destination. While this design makes mail exchange possible, it also provides possible avenues of attack. Restrictions in the openness of the SMTP server should be weighed against the loss of usability.

SMTP mail is inherently insecure because it enables users to negotiate directly with receiving and relaying SMTP servers. Sophisticated users can create messages that will trick a naive recipient into believing that they came from somewhere else. Constructing such a message so the trickery cannot be detected by an expert is more difficult, but not so much as to deter a determined and knowledgeable hacker.
Consequently, as knowledge of Internet mail increases, so does the knowledge that, at
the transport level, SMTP mail inherently cannot be authenticated, nor can integrity
checks be provided. Real mail security lies only in end-to-end methods that secure
message bodies by using digital signatures, such as PGP or S/MIME.

Identity Management Infrastructure

The identity management infrastructure controls and manages all aspects of directory,
authentication, and single sign-on operations.

Database security rules protect the underlying Oracle Database instance. Middle tier
and storage servers, as well as Web clients, must access this information to operate.
Access is required though LDAP and possibly HTTP/HTTPS, and access to these
protocols should be limited to only those servers truly requiring such access.

If Web clients are deployed on the public Internet, the single sign-on components
should be implemented on servers separate from the rest of the infrastructure. This
separation makes it possible to provide protection for these components behind
firewalls.

Because end-user passwords are managed by the infrastructure, password policies,
such as enforcing acceptable password sizes, randomness, and frequency of change,
should be maintained.

Unused or inactive mailboxes should be routinely cleaned or locked to minimize the
risk of unauthorized use.

Mail Clients

Most mail clients have configuration options enabling support for increased levels of
security when connecting to the server. For example, support for connections over SSL
and protocol authentication can require special configuration. Ensure that users are
aware of risky behaviors, such as storing passwords in ordinary files on PCs, and the
configuration options or changes required to minimize those risks.

Simple Authentication and Security Layer (SASL) provides authentication support to
connection-based protocols.

Configuring SASL for Oracle Mail includes using the Oracle Internet Directory
administration tool and the Application Server Control Console to configure various
parameters.

See Also:

- "Modifying Parameter Settings for a Specific Server Instance" on
  page 3-8 for information about modifying server parameters
- Appendix F, "Oracle Mail Server Parameters and Log Files" for
definitions of the various SASL parameters for the following
  servers:
  IMAP
  POP
  List Server
  SMTP Inbound
  SMTP Outbound

Network Security

Security features of the product enable separate components to be configured securely.
The more restrictive access to an organization’s network is the messaging system’s
security. Ensuring that the rest of your intranet is secure reduces the chances of unauthorized attempts to access components of the messaging system.

Firewalls

Firewalls play a large role in protecting the security of your implementation. Firewalls must be configured appropriately, with more than one firewall in place, and regularly monitored for intrusion. It is important not to assume that everything is safe because you have deployed a firewall.

You must determine what protocols to enable at the various points in your network. This decision often requires evaluating the trade-off between providing wide access to legitimate users and yet still protecting vulnerabilities from unauthorized use.

At a minimum, sending and receiving e-mail messages from the Internet requires that you enable inbound and outbound connections through port 25, the default SMTP connection socket. For other protocols, such as IMAP and POP, determine whether enabling public Internet access is worth the risks and cost. The risks include unauthorized access, and the costs include extra configuration and administration to maintain this infrastructure. In a typical enterprise, such access is not required, and all protocol tiers can be well protected within an intranet environment. Access for non-office-based workers can be managed through a separate virtual private network (VPN) or remote access infrastructure.

If you enable access through any of these protocols from the Internet, security can be improved by using authentication and SSL. Authentication provides some protection to the protocols, and SSL aids data encryption of network traffic.

The information storage database should be located behind any firewall implementation, with minimal access through SQL*Net from the middle-tier processes in other parts of the demilitarized zone (DMZ).

You should close down all firewall access other than explicitly required port and host connections. Closely managing and minimizing potential security vulnerabilities is a key part of any secure configuration.

Never assume that implementing a secure configuration means no new vulnerabilities and risks can arise. Watch for security updates from Oracle and security updates affecting Internet protocols to ensure that you maintain a secure environment.

Nontechnical Considerations

Any security implementation is only as good as its users’ awareness of security issues. Many security breaches are the result of simple human factors allowing intruders to gain access to user accounts through human deception. Administrators must keep the following factors in mind:

- Understand who has access to sensitive information
- Understand that database administrators can generally access trusted level information
- Implement password policies: minimum lengths, frequent changes
- Remove unused accounts
- Do not start unused services: run only what you need

Establish security policies for each level of security that applies to different parts of your system, including who has access to them and how to respond to security breaches.
SSL and TLS

**Secure Sockets Layer (SSL)** is a protocol for transmitting private information over the Internet. SSL works by using a public key to encrypt data that is transferred over the SSL connection from e-mail clients to the e-mail server. SSL secures traffic to the IMAP and SMTP servers, preventing anyone from accessing data on the network, including plain text password exchanges.

Many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs requiring an SSL connection start with `https:` instead of `http:`.

The primary goal of the **Transport Layer Security (TLS)** protocol is to provide privacy and data integrity between two communicating applications. The protocol is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. At the lowest level, layered on top of some reliable transport protocol, such as TCP, is the TLS Record Protocol. The TLS Record Protocol provides connection security that has two basic properties:

- The connection is private
- The connection is reliable

TLS enables the communication between either client and server, server to server, or both to be secured (more so than traditional SMTP which passes most of its data in clear text over its communication channel).

The security is negotiated between the two sides, so enabling it for a server does not force all other parties to use it, which is important because many mail servers might not support it or require it. Essentially, TLS allows users to use the best available security on their server.

**See Also:** "Securing Oracle Mail" in Chapter 2 of *Oracle Collaboration Suite Security Guide* for more information about enabling SSL for Oracle Mail

Antispam Methods

The NNTP and SMTP servers support a variety of **antispam** methods to prevent users and domains from misusing the e-mail system. Examples include flooding the e-mail system with undesired, unsolicited messages, and using the server as a spam relay for other domains.

This section includes the following topics:

- **Third-Party Antispam Filters**
- **Routing Control for SMTP**
- **Routing Control for NNTP**
- **Wildcards**
- **Routing Control Parameters for NNTP and SMTP**

**Third-Party Antispam Filters**

A third-party antispam filter agent can be run in front of the SMTP server to check whether incoming messages are spam. After completing the spam check, the agent passes the mail to the SMTP server. Antispam filters are configured to either reject spam mails or to change or add headers to indicate that the mail could be spam.
This release of Oracle Mail does not process any specific spam headers. However, because the format and values of the new headers are known, a user can set up server-side or client-side rules to move spam mail out of the Inbox or delete spam mail based on certain criteria.

**Setting Up Third-Party Antispam Filters**
If the third-party spam filter and SMTP server are running on the same computer, the filter should listen to the default SMTP port 25. The SMTP server listens to a different port. When e-mails come into the system, the spam filter filters the mail and takes action on it. If the mail passes the spam check, it is sent to the SMTP server. The communication between the third-party spam filter and SMTP server must be done over SMTP protocol.

**Routing Control for SMTP**
The SMTP server supports antispam checks, which are more efficient than third-party antispam filters because they eliminate the costs of external agent execution and passing mail. Upon the result of these checks, messages are routed to various destinations, or are rejected, depending upon the configuration of the Oracle Mail installation.

Routing control checks are performed on each input from the sender to identify spam mails at an earlier stage. The checks do not analyze message contents, but all e-mails are checked for the following:

- Sender’s address
- Sender’s domain
- Recipient’s address
- Recipient’s domain
- IP address of the sending computer
- Domain of the sending computer

The server supports two types of settings: an acceptance list and a rejection list. The values in these lists are domains, IP addresses, and senders. The appropriate accept and reject list is checked against the SMTP command being processed.

Routing control checks are performed during the following operations:

- When the SMTP connection is opened
- When the client connects
- After each SMTP protocol command, in the following order:
  ```plaintext
  HELO/EHLO, MAIL FROM, RCPT TO
  ```

Typically, SMTP servers inside a firewall do not need to have routing control enabled. Outside the firewall, however, servers receiving inbound e-mail messages need antispam protection.

SMTP inbound and NNTP inbound servers have a global **Routing Control** parameter that is checked by each instance. If this value is set to **Disabled**, antispam checking does not occur and all other parameters for routing control are disabled.

If **Routing Control** is enabled, the following occurs:
1. The Internet Protocol (IP) address and domain name (based upon a DNS lookup of the IP address) of the requester are checked during the connection request to the server. The following parameters are checked:

- **Accept Connections from IP Addresses:** If the IP address is trusted, the process continues.
- **Reject Connections from IP Addresses:** If the IP address is here, the message is rejected and the connection is closed.
- **Accept Connections from Host Domains:** If the domain name of the computer is trusted, the process continues. The domain name is obtained through a reverse DNS lookup of the IP address.
- **Reject Connections from Host Domains:** If the domain name is in this list, the message is rejected and the connection is closed.
- **Prevent Service Denial Attack:** The number of messages plus the number of connection requests from this host within a time interval that is considered to be flooding.
- **Spam Flood Interval:** The time interval, in minutes, used in conjunction with the **Spam Maximum Flood Count** parameter to determine whether a host is spamming.
- **Spam Maximum Flood Count:** SMTP server signals flooding if the number of messages and connections from a single host exceeds the value of this parameter within the **Spam Flood Interval**.

2. The **HELO** or **EHLO** command is processed. This is the initial command processed before any work can begin on the SMTP server. When this command is entered, a domain name is passed as part of the command. The following parameters are set:

- **Accept Connections from IP Addresses:** If the IP address is trusted, the process continues.
- **Accept Connections from Host Domains:** If the domain name of the computer, obtained through reverse DNS lookup of the IP address, is trusted, the process continues.
- **Enable HELO DNS Check:** If this parameter is set, the domain name in the **HELO**/**EHLO** command is checked for existence in the DNS server. If it does not exist, the connection is rejected.

3. The information in the **MAIL FROM** command is verified. This command contains the e-mail address of the sender. This address can be checked for spam. The following parameters are set:

- **Accept Connections from IP Addresses:** If the IP address is trusted, the process continues.
- **Accept Connections from Host Domains:** If the domain name of the computer, obtained through reverse DNS lookup of the IP address, is trusted, the process continues.
- **Reject Connections from Sender Domains:** If the domain name part of the sender’s e-mail address is in this list, the message is rejected and the connection is closed.
- **Reject Connections from Sender:** If the sender’s e-mail address is in this list, the message is rejected and the connection is closed.
- **Accept Connections from Sender Domains:** If the domain part of the sender’s e-mail address is in the list, the process continues.
Antispam Methods

- **Accept Connections from Sender**: If the sender address is a trusted address, the process continues.

- **Enable Sender DNS Check**: If this is enabled, the domain in the sender’s address is checked to determine if it exists in the DNS server.

4. An additional check for flooding takes place. This is required because a single connection to a message transfer agent (MTA) can send multiple messages. A flood check is performed after each message is accepted.

- **Prevent Service Denial Attack**: The number of messages plus the number of connection requests from this host within a time interval that is considered to be flooding.

- **Spam Flood Interval**: The time interval, in minutes, used in conjunction with Spam Maximum Flood Count to determine whether a host is spamming.

  The default values for the preceding two parameters are as follows:

  - Spam Flood Interval=10
  - Spam Maximum Flood Count=10000

- **Spam Maximum Flood Count**: SMTP server signals flooding if the number of messages and connections from a single host exceeds the value of this parameter within the Spam Flood Interval.

5. The RCPT TO command is verified. This command contains the e-mail addresses of the recipients. This check is dependent on several parameters and differs depending on the mail destination. If the sending computer is trusted, the mail continues. Then each recipient is either a local user or the mail message must be relayed to another SMTP server. If the mail is to be delivered to a local user, a check for rejected recipients is made. If the mail is to be relayed, a check is performed to make sure the server is allowed to relay, or allowed to relay conditional upon the domain to which the mail is going, as well as if the connection was initially authenticated.

- **Accept Connections from IP Addresses**: If the IP address is trusted, the process continues.

- **Accept Connections from Host Domains**: If the domain name of the computer or the domain name sent as part of the connection request are trusted, the process continues.

- **Accept Connections from Sender Domains**: If the domain part of the sender’s e-mail address is in the list, the process continues.

- **Accept Connections from Sender**: If the sender address is a trusted address, the process continues.

- **Reject Recipient**: This parameter list is only used for local delivery mail messages. If the recipient name is in this list, the message is rejected and the connection is closed. This is useful for temporarily suspended accounts or restricted distribution lists.

- **Relay Allowed**: This parameter is only used for relay delivery of mail messages. The possible values are:
  - **True**: The recipient domain is checked to see if it is in the list of domains allowed to relay.
  - **False**: Relay messages are not allowed.
– **Auth**: If the sender is authenticated when it first connected to the SMTP server, the delivery continues.

- **Relay Domains Allowed**: This value only reads relay mail messages when the **Relay Allowed** parameter is set to **True**. This parameter provides a list of domains that the SMTP server allows to be relayed. If relaying for all domains is allowed, the parameter must be set to an asterisk (*).

**See Also**: "Configuring Routing Control for Incoming Mail" on page 8-8 for information about setting up routing control for the SMTP inbound server

**Routing Control for NNTP**

The NNTP server supports antispam checks, based on the following:

- Host domain
- Host Internet Protocol (IP)
- Sender mail address

Configuring routing control for NNTP is similar to configuring routing control for SMTP.

**See Also**: "Configuring Routing Control for Incoming News" on page 8-21 for information about setting up routing control for the NNTP inbound server

**Wildcards**

NNTP and SMTP wildcard support exists on prefixes for domains and suffixes for IP addresses, to allow subdomains and subnetworks with a single entry. Entries containing only an asterisk (*) on a line by itself means all domains or IP addresses.

For example:

Valid entries: *.foo.com (all subdomains of foo.com), *.*.foo.com, 99.99.99.* (any host with IP address having a prefix 99.99.99);

Invalid entries: *.foo.*.com (domain), 99.*.99.* (IP).

**Routing Control Parameters for NNTP and SMTP**

**Note**: For SMTP, Reject parameters take precedence over Accept parameters. Exception for parameters such as Accept IPs apply only to subsequent spam checks. For example, if user99@foo.com is present in Accept senders, any checks on the rcpt to: command are ignored. However, if the IP address of host1.foo.com is present in Accept IPs and is not present in Reject IPs, all connections from host1.foo.com are accepted and all further spam checks on mails from host1.foo.com are ignored.
Symantec AntiVirus Scan Engine

Oracle Mail is packaged with two Symantec filters that can be used with the Symantec AntiVirus Scan Engine (SAVSE). The SAVSE client software can be installed within the network and configured on the Applications tier, or Oracle Mail can be integrated directly over the network with a SAVSE server. Both filters provide additional virus protection for your mail and incoming news.

The difference between the two filters is the communication protocol each uses when communicating with the SAVSE.

The SAVSE can be configured with either the Internet Content Adaptation Protocol (ICAP) or the Native protocol.

---

**Note:** ICAP configuration only applies to the platforms that Symantec supports: Windows, Solaris, and Linux. For other platforms, use the Native protocol.

**See Also:** Symantec documentation for details about ICAP and Native communication protocols

This enables Oracle Mail to use the Symantec virus knowledge base to detect and cleanse infected messages at the SMTP level and the Oracle Collaboration Suite Database.

This section includes the following topics:

- **Editing SAVSE Filters**
- **Applying SAVSE Filters**

### Editing SAVSE Filters

Edit the SAVSE filters before applying them.

To edit filters:

1. Open the Oracle WebMail client.

   **See Also:** "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client

2. Click the **Administration** tab.
3. Click the **Policy** subtab.
4. Click the name of the filter in the **Name** column to display the Edit Filter page.
5. Select Yes or No from the **Active** drop down list. Yes activates the SAVSE filter.

6. Select Yes or No from the **External Process** drop down list. No enables SAVSE filter antivirus protection.

7. Select Yes or No from the **Capable of Message Modification** drop down list. YES enables the SAVSE filter to repair messages, based on the **FilterFlags** string.

The Oracle Collaboration Suite filter architecture must define whether a filter can return a modified or repaired version of a message. This is distinct from any specific behavior of a third party library such as SAVSE, which may also have its own configuration settings for modifying or repairing a messages, such as a policy that includes RepairOnly:1. Messages in Oracle Collaboration Suite will only be repaired if the filter is capable of message modification and the external library is also configured to perform such repair, either through its own configuration or the explicit settings of the **FilterFlags** field.

**See Also:** "Applying SAVSE Filters" on page 6-13 for definitions of the various filters

8. In the **External Administration URL** field, enter the URL to the SAVSE administration page on the local host where the SAVSE client software is installed.

9. Use **FilterFlags** to configure the interface to the Symantec side to which is added `Server:IP_address:port_number` to the list of parameters described in Table 6–2.

**ICAP Configuration:**

a. Enter one of the following in the **Filter Flags** field, on a single line:

- `(config=Server:IP_address:port_number;;FailRetryTime:60;;ReadWriteTime:180)(policy=RepairOnly:1)(tmpdir=directory_for_temporary_files)(lib=libsymcsapi.so.4.x.x)`

- `(config=Server:IP_address:port_number;;FailRetryTime:60;;ReadWriteTime:180)(policy=ScanOnly:1)(tmpdir=directory_for_temporary_files)(lib=libsymcsapi.so.4.x.x)`

- `(config=Server:IP_address:port_number;;FailRetryTime:60;;ReadWriteTime:180)(policy=AlwaysReportDefInfo:1)(tmpdir=directory_for_temporary_files)(lib=libsymcsapi.so.4.x.x)`

- `(config=Server:IP_address:port_number;;FailRetryTime:60;;ReadWriteTime:180)(policy=RepairOnly:1;AlwaysReportDefInfo:1)(tmpdir=directory_for_temporary_files)(lib=libsymcsapi.so.4.x.x)`

- `(config=Server:IP_address:port_number;;FailRetryTime:60;;ReadWriteTime:180)(policy=ScanOnly:1;AlwaysReportDefInfo:1)(tmpdir=directory_for_temporary_files)(lib=libsymcsapi.so.4.x.x)`

**See Also:** *Symantec AntiVirus Scan Engine Software Developer's Guide* for more information about the **config** and **policy** parameters and values
In the preceding examples:

* Specify a path to a directory in the `tmpdir` parameter for storage of temporary files while repairing a message

* Specify the name of the SAVSE client library file in the `lib` parameter

Table 6–2 lists the parameters in the preceding filter strings and descriptions for each.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ScanOnly:1</td>
<td>Scan for viruses but do not attempt repair.</td>
</tr>
<tr>
<td>RepairOnly:1</td>
<td>Attempt to repair infected files but do not delete files that cannot be repaired.</td>
</tr>
<tr>
<td>AlwaysReportDefInfo:1</td>
<td>If a clean file is scanned, a Problem Incident is created with only the virus definitions date and revision number.</td>
</tr>
<tr>
<td>FailRetryTime:seconds</td>
<td>If the client fails to connect to a Symantec AntiVirus Scan Engine, wait <code>seconds</code> before trying to connect to that server again (use only the other servers in the meantime, unless they have all failed recently). The default setting is 30.</td>
</tr>
<tr>
<td>ReadWriteTime:seconds</td>
<td>If after <code>seconds</code> no response is received from the scan engine (when data is being transmitted to the scan engine), or if the transmission of data does not complete (when data is being receiving from the scan engine), return an error message.</td>
</tr>
</tbody>
</table>

b. Copy the SAVSE client library file from the `Scan_Engine/Scan_Engine_SDK/Lib/platform/dynamic` directory on the host where the SAVSE client software is installed to the `$ORACLE_HOME/oes/lib` directory on the Applications tier.

Choose the directory for the platform on which the SAVSE client software is installed.

Native Configuration:

Use the following format if the SAVSE has the Native protocol installed and configured:

```
(host=host_name) (port=port_number) (repair=true or false)
```

In the preceding example, specify the IP address of the host where the SAVSE is running in the `host` parameter. Specify the port number of the SAVSE in the `port` parameter.

If `repair` is set to `true`, the SAVSE will attempt to repair an infected message. The repaired message is received by the server and inserted into the Oracle Collaboration Suite Database instead of the original infected message.

10. Click OK to apply any changes.
Applying SAVSE Filters

You can apply the SAVSE filters to act on messages at various stages in the delivery cycle of the message. The filters can be applied to incoming messages, outgoing messages, messages delivered within the local Oracle Mail domain, and all messages stored in the Oracle Collaboration Suite Database.

To apply SAVSE filters:

1. Open the Oracle WebMail client.

   See Also: "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client

2. Click the Administration tab.

3. Click the Policy subtab.

4. Click the Application link.

5. Click either Incoming, Outgoing, Local, or Collaboration Suite Database to display a list of Oracle Collaboration Suite Applications tier servers associated with that point in the delivery cycle of the message.
   - Incoming: Filter is applied to all incoming messages.
   - Outgoing: Filter is applied to all messages delivered outside the local Oracle Mail domain.
   - Local: Filter is applied to all messages delivered within the local Oracle Mail domain.
   - Collaboration Suite Database: Filter is applied to all messages stored in the Oracle Collaboration Suite Database.

6. Click the icon in the Configure Filters column. If you clicked Collaboration Suite Database in the preceding step, go to "Configuring Filters for an Oracle Collaboration Suite Database" on page 8-5 for a description of that page.

7. Click Apply Filter.

8. Select either SAVSE filter according to whether the SAVSE client software is installed on the Applications tier and configured with ICAP, or Oracle Mail is being integrated with SAVSE over the network where it is installed and configured with the Native protocol. Click the Policy subtab followed by the Definitions link to determine which filter to apply with which configuration.

9. In the Options section, select Yes from the Allow Message Modification list to enable the filter to modify messages.

10. In some cases, you may want to override the filter flags associated with one of the filters. To do this, click the icon adjacent to Filter Flags to list the values that will be overridden during filter application. The filter is then applied to all messages. Otherwise, the values for Filter Flags are inherited from the filter definition and the filter is only applied to messages that meet these criteria.

   See Also: "Editing SAVSE Filters" on page 6-10 for usage information of SAVSE filter flags

11. Click OK to apply the filter and return to the Configure Filters page. Applied filters are displayed.
12. To disable a filter, select a filter from the list to be unapplied and click **Unapply Filter**. A confirmation page displays. Click **Yes** or **No**.

13. In the **Advanced** section, click **Remove Instance Level Settings**.

14. If you apply any filters, you must restart the associated servers.
   - For incoming mail, restart the SMTP inbound, SMTP outbound, and NNTP inbound servers.
   - For outgoing mail, restart the SMTP outbound server and the List Server.
   - For local mail, restart the SMTP inbound and SMTP outbound servers and the List Server.
   - For mail stored on the Oracle Collaboration Suite Database, restart the Virus Scrubber.

**Virus Scrubber**

The Oracle Mail **Virus Scrubber** is a server process that scans for and cleans up virus-infected e-mail messages already in the Oracle Collaboration Suite Database. When rapid measures are required to immediately cleanse a system of virus-infected messages, the Virus Scrubber prescans an information storage database to isolate suspect messages contained within based on headers such as subjects or attachment names. Prescanning isolates suspect messages so that users are not able to access them and possibly cause damage. Prescanning never deletes a message. After prescanning, the Virus Scrubber uses the external scanner to individually scan the isolated messages. A message that is deemed clean or repaired by the virus detection software is restored to its original folder.

---

**Note:** Although prescanning is a faster way to isolate suspect messages in an information storage database than scanning all individual messages, it can quarantine clean messages.

---

If a message is identified as infected and not repairable, the administrator can either delete the message immediately or quarantine it to a special folder for later processing. For example, an infected message can be quarantined to wait for a future release of virus definitions that may be able to repair the message. Oracle Mail can be configured to send a message to either the mail recipient or sender notifying them that a message was identified as infected. Such notifications are useful to explain to users why their messages disappeared.

The Virus Scrubber is different from the SMTP-based virus scanner that filters out virus-infected messages before they enter the system. The Virus Scrubber is a necessary complement to the SMTP virus scanner, because new types of viruses continue to emerge before virus detection software can be updated to detect and repair them. There is always a possibility that by the time virus software is updated, some infected messages have already entered the system. The virus scanner can be used to retroactively rid the system of such viruses. This information store-based scanner can also be used to scan viruses coming in through a non-SMTP route such as IMAP append.

The Virus Scrubber and SMTP-based virus scanner rely on external virus detection and cleanup software from the Symantec AntiVirus Scan Engine. Oracle Collaboration Suite provides interface libraries for third-party virus tools to integrate with Oracle Mail. The third-party virus software must be installed properly for the Virus Scrubber server to be fully functional.
The Virus Scrubber log files are located in the following directories:

On UNIX:

$ORACLE_HOME/oes/log/install_name/vs/pid/pid.log

On Windows:

%ORACLE_HOME\oes\log\install_name\vs\pid\pid.log

Configuring the Virus Scrubber with the Oracle Enterprise Manager 10g Application Server Control Console for Collaboration Suite

To configure the Virus Scrubber using the Application Server Control Console for Collaboration Suite:

1. Open the Application Server Control Console for Collaboration Suite.

   **See Also:** "Oracle Enterprise Manager 10g Application Server Control Console for Collaboration Suite" on page 1-3 for information about accessing the Application Server Control Console for Collaboration Suite

2. Click the application server instance where Oracle Mail is installed.

3. Select the server for which the new instance is to be created.

4. Click **Stop** to bring down the server.

5. Click **Mail Application** in the **System Components** section to display the Mail Application page.

6. Click **Virus Scrubber**.

7. In the **Mail Collaboration Suite Database** section, choose an Oracle Collaboration Suite Database from the **Mail Collaboration Suite Database** list to display the default parameter settings for that particular Oracle Collaboration Suite Database.

8. In the **Thread Parameters** section, enter a number in the **Number of Threads** field to establish the number of connections to the database. The number chosen is dependent upon such factors as how much memory each thread uses and how many connections each thread makes, and whether a connection pool is being used. A large number of threads can affect resource performance.

9. In the **General Parameters** section, configure the process parameters listed in Table 6–3.

### Table 6–3 Virus Scrubber General Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Pre-Scan Mode | Disabled, Enabled, or Pre-scan Only | - **Disabled**: Only those messages that have been isolated by a previous prescan operation are sent through the filters for scrubbing;  
- **Enabled**: First, all messages are prescanned and messages that match the prescan criteria are isolated. Then, only those isolated messages are sent through the filters for scrubbing.  
- **Pre-scan Only**: All messages are prescanned only. Messages that match the prescan criteria are isolated. |
Pre-Scan Filter

The IMAP SEARCH command style conditions that are executed to identify the list of messages to pass through the third-party scanner. Messages matching this criteria are removed from the mailbox of the respective users until the third-party scanner verdict is harmless/not-affected.

All IMAP search commands except new, old, and recent can be used in the filter.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Interval</td>
<td>Enter a nonnegative number</td>
<td>Time interval between two successive scans.</td>
</tr>
<tr>
<td>(Minutes)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Repair Mode</td>
<td>Purge or Quarantine</td>
<td>Determines what action to perform to messages identified as infected. Select Purge to delete the infected messages immediately; Quarantine to save it to a special folder specified in following parameters.</td>
</tr>
<tr>
<td>Quarantine</td>
<td>String</td>
<td>If the repair mode is set to Quarantine, this parameter, in conjunction with Quarantine Destination Folder, uniquely identifies an IMAP folder where the message will be quarantined.</td>
</tr>
<tr>
<td>Destination E-mail Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quarantine</td>
<td>String</td>
<td>If the repair mode is Quarantine, this parameter, in conjunction with Quarantine Destination E-mail Address, uniquely identifies an IMAP folder where the message will be quarantined.</td>
</tr>
<tr>
<td>Destination Folder</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
When composing notification message templates to virus senders (or recipients), you can use macros that can be substituted with actual message-specific values when the Virus Scrubber generates and sends the notifications. Supported macros include:

- %internaldate%: Received date of the message
- %messagesize%: Message size in bytes
- %rfc822date%: The Date header value of the message
- %rfc822from%: The From header value of the message
- %rfc822subject%: The Subject header value of the message
- %rfc822to%: The To header value of the message
- %rfc822cc%: The CC header value of the message
- %rfc822sender%: The Sender header value of the message
- %rfc822replyto%: The Reply-To header value of the message
- %rfc822msgid%: The Message-ID header value of the message
- %xpriority%: The X-Priority header value of the message

For example, consider the following notification text:

A message you sent on %internaldate% to %rfc822to% with subject %rfc822subject% has been identified as virus-infected. Please run a virus scan on your computer immediately.

The actual notification message received by the recipient will have the preceding text with the macros substituted by the actual values from the virus infected message.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notification Message to Virus Sender</td>
<td>String</td>
<td>If a message is infected, the sender will be notified. The text entered in this parameter will be sent embedded in a standard mail.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When composing notification message templates to virus senders (or recipients), you can use macros that can be substituted with actual message-specific values when the Virus Scrubber generates and sends the notifications. Supported macros include:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>%internaldate%: Received date of the message</td>
</tr>
<tr>
<td></td>
<td></td>
<td>%messagesize%: Message size in bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>%rfc822date%: The Date header value of the message</td>
</tr>
<tr>
<td></td>
<td></td>
<td>%rfc822from%: The From header value of the message</td>
</tr>
<tr>
<td></td>
<td></td>
<td>%rfc822subject%: The Subject header value of the message</td>
</tr>
<tr>
<td></td>
<td></td>
<td>%rfc822to%: The To header value of the message</td>
</tr>
<tr>
<td></td>
<td></td>
<td>%rfc822cc%: The CC header value of the message</td>
</tr>
<tr>
<td></td>
<td></td>
<td>%rfc822sender%: The Sender header value of the message</td>
</tr>
<tr>
<td></td>
<td></td>
<td>%rfc822replyto%: The Reply-To header value of the message</td>
</tr>
<tr>
<td></td>
<td></td>
<td>%rfc822msgid%: The Message-ID header value of the message</td>
</tr>
<tr>
<td></td>
<td></td>
<td>%xpriority%: The X-Priority header value of the message</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For example, consider the following notification text:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A message you sent on %internaldate% to %rfc822to% with subject %rfc822subject% has been identified as virus-infected. Please run a virus scan on your computer immediately.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The actual notification message received by the recipient will have the preceding text with the macros substituted by the actual values from the virus infected message.</td>
</tr>
</tbody>
</table>

| Notification Message to Virus Recipient | String | If a message is infected, the recipient will be notified. The text entered in this parameter will be sent embedded in a standard mail. |
|                                        |        | See Notification Message to Virus Sender for a list of supported macros. |
10. Click Cancel to cancel any changes made, click Revert to set the parameter values back to the default, or click Apply to apply any changes made.

11. Restart the Virus Scrubber.

See Also: "Starting, Stopping, Restarting, or Refreshing All Server Instances" on page 3-5 for more information about restarting the process.

Virus Scanning and Removal Using PL/SQL Scripts

E-mail viruses typically have the form of an executable program, such as an e-mail attachment. The program is executed on the client computer when the attachment is opened by an unsuspecting user, causing various forms of damage to the computer or the network. Oracle Mail provides several different tools for virus protection, each of them suited for a different type of administration requirement.

The Oracle Mail server SMTP inbound process provides integration with third-party virus scanning software to scan each message that passes through the SMTP server. The server rejects the message upon arrival, preventing the virus e-mail from entering the e-mail system.
If third-party virus scanning software is not available, Oracle Mail server can still reject virus messages using server-side rules. Server-side rules reject incoming messages based on suspicious subject lines, attachment names or sender information.

**See Also:** "oesrl" on page D-24 for more information about how to create server-side rules using oesrl

If there is a virus outbreak before the SMTP server has a chance to upgrade itself to use the latest third-party software, some virus e-mail messages could already be present in a user's Inbox. The Virus Scrubber server can be used to scan the entire Oracle Collaboration Suite Database and repair or remove virus-infected e-mail messages once the third-party software is updated.

Oracle Mail has a simple PL/SQL utility package `MAIL_AV` that scans the message store based on simple message attributes, such as subject line and attachment names. To use this package, write a SQL*Plus script that uses this package or execute procedures in this package directly from SQL*Plus.

**See Also:** "oesctl and opmnctl" on page D-16 for more information about how to create server-side rules using oesctl

### Usage Examples

The following are summaries and usage examples for the procedures in the `MAIL_AV` package:

#### Quarantine

The quarantine procedure has the following syntax:

```sql
PROCEDURE quarantine (p_endday IN DATE,
                      p_dayrange IN NUMBER,
                      p_attribute IN NUMBER,
                      p_pattern IN VARCHAR2,
                      p_folder IN VARCHAR2);
```

The quarantine procedure identifies virus-infected messages using a given pattern and moves them to a designated folder. The caller of the procedure must have write authorization to the folder. Authentication is done by using `MAIL_SESSION` package.

**See Also:** Oracle Mail Application Developer's Guide for more information

The `p_endday` and `p_dayrange` parameters can be used to narrow down the virus search to within certain time frame. The `p_attribute` parameters takes one of the following three values:

- `MAIL_AV.ATTR_SUBJECT`
- `MAIL_AV.ATTR_ATTACHMENT`
- `MAIL_AV.ATTR_SENDER`

The `p_pattern` parameter is the identifying string for the virus. The `p_folder` parameter is the designated folder name to which virus-infected messages are moved.

The following example logs in as user `SYSADMIN`, and scans the entire mail server for messages with an attachment name containing `.exe` within the last seven days, and moves them to the `/infected` folder.

```sql
DECLARE
    sessionid number;
```
begin
    mail_session.login('sysadmin', <password>, <ldaphost>, sessionid);
    mail_av.quarantine(sysdate, 7, mail_av.attr_attachment, '.exe',
      '/sysadmin/infected');
end;
/

Quarantine II
The quarantine procedure can take on the following format enabling IMAP style search criteria:

PROCEDURE quarantine (p_criteria IN VARCHAR2,
    p_folder IN VARCHAR2);

This quarantine procedure form identifies virus-infected messages using an IMAP style search criteria for enhanced searching. All IMAP search commands are supported except new, old, and recent commands. The advantage of using this procedure not only includes the expanded list of search item, but also the ability to combine search criteria using logical operations such as and or or.

See Also: Internet RFC 2060: Internet Message Access Protocol, version 4, rev 1, for more information about IMAP search commands

Use the new form of quarantine procedure. The following script identifies and moves messages with subject *snow white* from *acme.com*, that have been sent since January 2002:

declare
    sessionid number;
begin
    mail_session.login('sysadmin', <password>, <ldaphost>, sessionid);
    mail_av.quarantine('SINCE 01-Jan-2002 SUBJECT "snow white" SENDER "aol.com"',
      '/sysadmin/infected');
end;
/

Restore
There are two procedures to restore quarantined messages to their original folders:

PROCEDURE restore (p_messageid IN NUMBER);
PROCEDURE restoreall;

The restore procedure takes a given message ID and restores it to its original folder. If the message ID does not exist, the procedure does nothing. The restoreall procedure restores all messages quarantined regardless of which designated folders are used to store the messages. These procedures are useful when a message is wrongly identified as a virus-infected message and must be restored to its recipients.
This chapter describes how to set up monitoring for the Oracle Mail component of Oracle Collaboration Suite. An Oracle Mail installation may be spread over dozens of computers.

Monitoring Oracle Mail can also be done using the oesmon and oeschart command-line utilities.

This chapter discusses the following topics:

- Monitoring Oracle Mail Using Oracle Enterprise Manager 10g Grid Control Console
- Purging Monitoring Data from the Oracle Collaboration Suite Database
- Using oesmon and oeschart

Monitoring Oracle Mail Using Oracle Enterprise Manager 10g Grid Control Console

The following instructions assume that Oracle Mail is already installed and that Oracle Enterprise Manager 10g Grid Control Console and Oracle Management Agent are already installed. Furthermore, the following instructions assume that you have detailed knowledge of how Oracle Mail is configured and where the different protocol servers are running.

In this section you will create targets that represent components of your Oracle Mail deployment. In addition, an Oracle Mail group target will be created. The group target will include all the component Oracle Mail targets.

This section discusses the following topics:

- Overview of Oracle Mail Target Types
- Identifying Oracle Mail Hosts and Databases
- About Oracle Mail Service Targets

Overview of Oracle Mail Target Types

Oracle Mail has several protocols with distinct services and servers for each type of protocol:

- IMAP
- SMTP inbound
- SMTP outbound
- POP
- Oracle WebMail

An Oracle Mail server refers to a specific process running on a specific host. As a result, the up or down metric for a server indicates whether or not the process is running. An Oracle Mail service refers to the service provided by a collection of processes. For a service, the up or down metric indicates whether or not a user can make use of that service.

These Oracle Mail services and servers are often spread over hosts and databases. Create the targets as follows:
- One service target for each logical service
- One information store target for each Oracle Collaboration Suite Database

**Identifying Oracle Mail Hosts and Databases**

Before you begin creating the Oracle Mail targets, you should have a complete list of the hosts and the databases where your Oracle Mail components reside. For example, you should know the system identifier (SID) and password for each database.

The following sections describe how you can obtain this information using the Oracle Internet Directory for your Oracle Collaboration Suite installations:

- **Identifying the Oracle Mail Component Hosts**
- **Identifying Locations of Oracle Collaboration Suite Databases**
- **Identifying the Connection String for an Oracle Collaboration Suite Database**

**Identifying the Oracle Mail Component Hosts**

You can identify the Oracle Mail hosts by using the following `ldapsearch` command for your Oracle Internet Directory:

```
$PROMPT> ldapsearch -h oid_host -poid_port -Dcn=orcladmin -wwelcome1 -b 'cn=Computers,cn=OracleContext' 'objectclass=orclMailProcessConf' orclmailinstanceid
```

For example:
```
$PROMPT> ldapsearch -hhas15.acme.com -p4032 -Dcn=orcladmin -wx9djiks189 -b 'cn=Computers,cn=OracleContext' 'objectclass=orclMailProcessConf' orclmailinstanceid
```

**Identifying Locations of Oracle Collaboration Suite Databases**

To identify the hosts and the names of the databases where your Oracle Collaboration Suite Databases are located, you can use the following `ldapsearch` command for your Oracle Internet Directory:

```
$PROMPT> ldapsearch -hoid_host -poid_port -Dcn=orcladmin -worcladmin_pwd -b 'cn=EMailServerContainer,cn=Products,cn=OracleContext' 'objectclass=orclMailStores'
```

For example:
```
$PROMPT> ldapsearch -hmghost42.acme.com -p3060 -Dcn=orcladmin -wx9djiks189 -b 'cn=EMailServerContainer,cn=Products,cn=OracleContext' 'objectclass=orclMailStores'
```
Identifying the Connection String for an Oracle Collaboration Suite Database

Find the connection string for an Oracle Collaboration Suite Database, so you can connect to the information store or provide the host, port, SID, user name, or password properties for the information store, as follows:

1. Obtain the value of the orclDBDistinguishedName attribute for the Oracle Collaboration Suite Database.
   
   You can obtain this value by searching for the Oracle Collaboration Suite Database host and database properties, using the command described in "Identifying Locations of Oracle Collaboration Suite Databases".

2. Use the ldapsearch command to find the orclnetdescrstring attribute of the Oracle Collaboration Suite Database:
   
   ```bash
   $PROMPT> ldapsearch -h oid_host -p oid_port -Dcn=orcladmin -w orcladmin_pwd -b 'value_of_orclDBDistinguishedName' -s base 'objectclass=*
   
   For example:
   
   $PROMPT> ldapsearch -hmgthost42.acme.com -p3060 -Dcn=orcladmin -wx9djiksl89 -b 'cn=v2store,cn=OracleContext' -s base 'objectclass=*
   ```

About Oracle Mail Service Targets

The service targets monitor the Oracle Mail services. Thus, it is most beneficial to locate these targets close to where the user community using the services resides. It is also possible to create multiple targets for each service in order to measure responsiveness from multiple geographical locations.

One service target must be created for each service type. For example, an SMTP IN Service is implemented over four hosts; however, only one target is needed to monitor the overall service.

The same guidelines apply to the Oracle WebMail service. However, for Oracle WebMail use the Oracle Enterprise Manager 10g application performance management capabilities for monitoring.

Oracle Enterprise Manager 10g includes the following Oracle Mail service types:

- E-Mail SMTP Inbound Service
- E-Mail SMTP Outbound Service
- E-Mail IMAP Service
- E-Mail POP Service
- E-Mail NNTP Inbound Service

To configure service monitoring, configure targets at points in the network close to the user communities accessing Oracle Mail. Thus, having an SMTP_IN service monitoring target type in a few key geographical locations is necessary to get an overall perspective on the SMTP_IN monitoring.

Oracle suggests using the following naming convention for service targets: SMTP_IN_SERVICE_information_store location_of_observation, such as SMTP_IN_SERVICE_EMEA_LONDON.

For monitoring Oracle WebMail, create a Web Application target and record an availability transaction for Oracle WebMail. This transaction must be run from beacons in key geographical locations that represent user communities.

This section discusses the following topics:
Creating Oracle Mail Service Targets

Create Oracle Mail service targets, as follows:

1. Using the Grid Control Console, navigate to the Agent home page for the Oracle Management Agent that was installed on the Oracle Collaboration Suite Database host, as follows:
   a. Click the **Targets** tab.
   b. Click the link in the **Name** column of the **Host** type.
   c. Click the **Targets** link.
   d. Click the link in the **Name** column of the **Agent** type.

2. In the **Monitored Targets** section of the page, select one of the following service types from the **Add** list and click **Go** to display the **Add E-Mail Service** page for that particular service:
   - E-Mail SMTP Inbound Service
   - E-Mail SMTP Outbound Service
   - E-Mail IMAP Service
   - E-Mail POP Service
   - E-Mail NNTP Inbound Service

**Note:** Ensure that you select a **Service** and not a **Server**.

Oracle recommends creating targets for the E-Mail IMAP and E-Mail SMTP Inbound services, at the minimum, as described in the subsequent steps.

   a. Select **E-Mail IMAP Service** from the **Add** list and click **Go** to display the **Add E-Mail IMAP Service** page.

   b. On the **Add E-Mail IMAP Service** page, enter a name for the target in the **Name** field.

   Provide the required information, as described in **Table 7–1**.

**Table 7–1  E-Mail IMAP Service Target Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Address</td>
<td>The host name or the IP address of the load balancer or system used by clients for accessing the IMAP service.</td>
</tr>
<tr>
<td>Service Port</td>
<td>The port where the IMAP service is running.</td>
</tr>
<tr>
<td>E-Mail Address</td>
<td>The e-mail address of a test user account to be used for the status and the service availability of the IMAP service. You can use the orclguest@your_domain account that is created by default in the e-mail system.</td>
</tr>
</tbody>
</table>
c. Click **OK** to create the target.

d. Select **E-Mail SMTP Inbound Service** from the **Add** list and click **Go** to display the Add E-Mail SMTP Inbound Service page.

e. On the Add E-Mail SMTP Inbound Service page, enter a name for the target in the **Name** field.

    Provide the required information, as described in Table 7–2.

Table 7–2 E-Mail SMTP Inbound Service Target Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP Host</td>
<td>The host name or the IP address of the load balancer or the system used for accessing the SMTP IN service.</td>
</tr>
<tr>
<td>Sender E-Mail</td>
<td>The e-mail address of a test account used for sending an e-mail and that will be used for the status and the service availability of the SMTP IN service. You can use the orclguest@your_domain account that is created by default in the e-mail system.</td>
</tr>
<tr>
<td>Recipient E-Mail</td>
<td>The e-mail address of a test account used for receiving an e-mail and that will be used for the status and the service availability of the SMTP IN service. You can use the orclguest@your_domain account that is created by default in the e-mail system. <strong>Note:</strong> Sender E-Mail and Recipient E-Mail can be the same address.</td>
</tr>
</tbody>
</table>

f. Click **OK** to create the target.

3. Follow these same procedures for creating POP, NNTP inbound, and SMTP outbound service targets.

Creating an Oracle WebMail Web Application Target

To monitor your Oracle WebMail instances, create a Web Application target for each Oracle WebMail instance. Web Application targets can be monitored for availability and performance with Application Performance Management transactions. You can also measure the response time of pages in your Web Applications using End-User Performance Monitoring.

Create a Web Application target for your Oracle WebMail instance, as follows:

1. Using the Grid Control Console, navigate to the Agent home page for the Oracle Management Agent that was installed on the Oracle WebMail host.

2. In the **Monitored Targets** section of the page, select **Web Application** from the **Add** list.

   Oracle Enterprise Manager 10g displays the Create Web Application Wizard, which guides you through the process of creating the Web Application.

   When prompted for the home page URL, enter the URL for the Oracle WebMail instance. For example:

   http://host1.acme.com:7778/um/traffic_cop
Click **Help** if you need help using the wizard.

3. Click **OK** to create the target.

4. Use the instructions in the online Help to create some representative transactions to measure the availability and performance of the Web Application you just created.

   For example, create a transaction that logs in and reads an e-mail message.

   **See Also:** *Oracle Enterprise Manager Advanced Configuration* to enable End-User Performance Monitoring for the Web Application using the procedures for earlier versions of the Oracle Application Server

---

**Note:** Before you enable End-User Performance Monitoring to monitor your Oracle Collaboration Suite Web Application target, you must apply patch number 3040716 to the Oracle Application Server middle tier instance. You can download this patch from OracleMetaLink:

http://metalink.oracle.com/

---

**Creating the Oracle Mail Oracle Collaboration Suite Database Target**

One information store target must be created for each Oracle Collaboration Suite Database created for Oracle Mail. It is also possible to locate these targets on any host on the network capable of accessing the Oracle Collaboration Suite Database. The benefit of this approach is that the target deployment becomes nonintrusive to the Oracle Mail information stores.

Oracle Enterprise Manager 10g includes one Oracle Mail information store target type. You must add and configure an information store target for each Oracle Collaboration Suite Database in the network that you want to monitor.

Create an Oracle Mail information store target, as follows:

1. Using the Grid Control Console, navigate to the Agent home page for the Oracle Management Agent that was installed on the Oracle Collaboration Suite Database host, as follows:
   a. Click the **Targets** tab.
   b. Click the link in the **Name** column of the **Host** type.
   c. Click the **Targets** link.
   d. Click the link in the **Name** column of the **Agent** type.

2. In the **Monitored Targets** section of the page, select **E-Mail Collaboration Suite Database** from the **Add** list and click **Go** to display the Add E-Mail Collaboration Suite Database page.

   Provide the required information, as described in Table 7–3.

---

**Table 7–3  E-Mail Collaboration Suite Database Target Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collaboration Suite Database Connector Descriptor</td>
<td>The connect descriptor for the Oracle Collaboration Suite Database</td>
</tr>
</tbody>
</table>
Creating the Oracle Internet Directory Client Target

Oracle Internet Directory client targets are useful to measure responsiveness of Oracle Internet Directory for Oracle Mail. Thus, one such target must be created on each host where an Oracle Mail server runs. The collection of such targets will give a view of Oracle Internet Directory responsiveness across all Oracle Mail hosts.

Create the Oracle Internet Directory client target, as follows:

1. Using the Grid Control Console, navigate to the Agent home page for the Oracle Management Agent that was installed on the Oracle Internet Directory Client host, as follows:
   a. Click the **Targets** tab.
   b. Click the link in the **Name** column of the **Host** type.
   c. Click the **Targets** link.
   d. Click the link in the **Name** column of the **Agent** type.

2. In the **Monitored Targets** section of the page, select **OID Client** from the **Add** list and click **Go** to display the Add OID Client page.

   Provide the required information, as described in Table 7–4.

### Table 7–4 Oracle Internet Directory Client Target Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP Client Oracle home path</td>
<td>The path of the Oracle home of the LDAP client system. This will be used to invoke the ldapsearch or ldapcompare utility for the computation of the various Oracle Internet Directory Client metrics. For example, the ldapsearch or ldapcompare utility exists in the following directory, based on the value you enter in this field: LDAP_Client_Oracle_home_path/bin/</td>
</tr>
<tr>
<td>LDAP Host</td>
<td>The host name of the system where the LDAP server is running.</td>
</tr>
<tr>
<td>LDAP Port</td>
<td>The port where the LDAP server is running.</td>
</tr>
</tbody>
</table>
Click OK to create the target.

Creating the E-mail Group Target

After all the Oracle Mail targets are configured, you can create the e-mail group target, which provides a custom user interface for managing your Oracle Collaboration Suite environment.

The Oracle Collaboration Suite Email group home page contains the alerts table, followed by a table of rows of component targets and columns of key metrics. The server targets listed here can also be remotely started and stopped from this page.

Create the e-mail group target, as follows:

1. Click the Targets tab in the Grid Control Console.
2. Click All Targets.
3. Select Collaboration Suite Component from the Add list and click Go to display the Create Collaboration Suite Component: Component Type page.
4. Select E-Mail from the list of Oracle Collaboration Suite components and click Continue to display the Create Collaboration Suite Component: Targets page.
5. Enter a name for the e-mail group in the Name field, such as My Email.
6. Select the following targets from the Target Type list. Select the target from the Available Targets list and use the Move or Move All arrow to shuttle the target to the Selected Targets list.
   - **Host**: The host targets where the Oracle Mail servers reside
   - The database and listener targets that support the Oracle Mail servers
   - An E-Mail IMAP Service and E-Mail IMAP Server
   - An E-Mail SMTP Inbound Service and E-Mail SMTP Inbound Server
   - An E-Mail SMTP Outbound Server
   - An E-Mail POP Server
   - An E-Mail NNTP Inbound Server
   - An E-Mail List Server
   - An E-Mail Virus Scrubber
   - An E-Mail Housekeeper
   - An E-Mail Collaboration Suite Database
   - An Oracle Internet Directory Client

3. Click OK to create the target.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP User</td>
<td>The user name of a test user account that is needed for the ldapsearch or ldapcompare command. It is possible to use the default user setup for Oracle Enterprise Manager 10g monitoring: &quot;cn=emd admin,cn=oracle internet directory&quot;</td>
</tr>
<tr>
<td>LDAP Password</td>
<td>The password of the test user account that is needed for the ldapsearch or ldapcompare command. For the Oracle Enterprise Manager 10g monitoring user, the default is welcome.</td>
</tr>
</tbody>
</table>
Using oesmon and oeschart

An E-Mail Web Application

7. Click OK to create the group target.

8. Add this group to any existing or future Oracle Collaboration Suite group.

Purging Monitoring Data from the Oracle Collaboration Suite Database

When you monitor your Oracle Mail targets with Oracle Enterprise Manager 10g, the Oracle Management Agent gathers monitoring data about the Oracle Mail targets and uploads them to Oracle Management Service, which loads them into Oracle Management Repository.

However, the Oracle Mail information store itself also gathers monitoring data about your Oracle Mail targets. After you start monitoring your Oracle Mail targets with Oracle Enterprise Manager 10g, the data saved in the Oracle Collaboration Suite Database is redundant with the information available in Oracle Management Repository.

---

**Note:** Purging monitoring data is done automatically by the Housekeeper process when it is configured to run in the Statistics Cleanup operation mode.

---

Using oesmon and oeschart

oesmon and oeschart are command-line utilities used to collect and view Oracle Mail system statistics for the purposes of monitoring the performance of Oracle Mail.

This section discusses the following topics:

- Using oesmon
- Using oeschart

Using oesmon

The oesmon utility obtains raw metric data directly from Oracle Mail server processes and provides a summary of the mail system’s statistics. Each statistic is represented by either an ASCII string or a number, rendered in keyword-value pairs.

Table 7–5 lists oesmon syntax options.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>oesmon</td>
<td>Returns the usage message</td>
</tr>
<tr>
<td>oesmon targets</td>
<td>Lists all possible targets for Oracle Mail servers</td>
</tr>
<tr>
<td>oesmon names target</td>
<td>Lists all of the metric names for a particular target</td>
</tr>
<tr>
<td>oesmon get target metric_name</td>
<td>Returns the statistics</td>
</tr>
</tbody>
</table>

Oracle Mail has nine service types, such as the IMAP service. These services can run on the same host or on separate hosts. One or more instances of a service can be running on a host. The oesmon utility collects statistical information about a service on a host (target). Targets are named as a concatenation of:

host:um_system:service_type
In this example, host is the name of the host where the service is running, and service_type is one of the following types listed in Table 7–6.

### Table 7–6 Different Service Types Used in Target Names

<table>
<thead>
<tr>
<th>service_type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>gc</td>
<td>Housekeeper</td>
</tr>
<tr>
<td>imap</td>
<td>IMAP server</td>
</tr>
<tr>
<td>list</td>
<td>List Server</td>
</tr>
<tr>
<td>pop</td>
<td>POP server</td>
</tr>
<tr>
<td>smtp_in</td>
<td>SMTP process for inbound mail routing</td>
</tr>
<tr>
<td>smtp_out</td>
<td>SMTP process for outbound mail routing</td>
</tr>
<tr>
<td>nntp_in</td>
<td>NNTP inbound news server</td>
</tr>
<tr>
<td>nntp_out</td>
<td>NNTP outbound news server</td>
</tr>
<tr>
<td>vs</td>
<td>Virus Scrubber</td>
</tr>
</tbody>
</table>

All statistics and managed objects have names. Names are case-sensitive and contain only alphanumeric characters and the underscore character (_). Statistic names are hierarchical and separated by a period (.). A request for a managed object returns all of the managed objects and statistics beneath it.

**See Also:** Appendix H, "Oracle Mail Server Metrics" for a complete list of the available statistics

Consider the following example:

oesmon get mycomputer:um_system:pop .um.admin

In this case, two values are returned for the two metric objects in the hierarchy:

- process identifier
- date and time the service was started

```plaintext
.um.admin.os_pid = 8239
.um.admin.uptime = Wed Jan 29 14:17:36 2003
.um.admin.log.discard = 0
.um.admin.log.total = 100
```

In the previous example:

- .um.admin.log.discard is the number of log messages discarded when high log levels cause log messages to be generated faster than they can be written to disk
- .um.admin.log.total is the total number of log messages logged by the processes, including the ones that are discarded and written to disk

```plaintext
oesmon get mycomputer:um_system:pop .um.admin.os_pid
```

Only the process identifier is returned.

```plaintext
.um.admin.os_pid = 8239
```
Using oeschart

Oracle Mail servers track a range of metrics that are periodically stored in a set of mail statistics tables. The `oeschart` utility generates charts and images that can be used to publish reports and Web pages, providing a company with a graphic picture of the status of the mail system implementation.

This section discusses the following topics:

- Setting the Statistics Collection Interval
- Cleaning Up Mail Statistics
- Mail Statistics Schema
- Creating Graphs
- Displaying Graphs in Oracle Enterprise Manager

Setting the Statistics Collection Interval

You can set the frequency by which metrics are sampled and recorded using the `oidadmin` administration tool provided by Oracle Internet Directory.

The `orclMailAdminCollectionInterval` parameter specifies the number of seconds that elapse between statistics collecting. A setting of zero (0) seconds stops the service from logging statistics altogether.

Set the `orclMailAdminCollectionInterval` parameter at the target level, rather than the instance level. If you set the value at the instance level, statistics collection occurs at different intervals for each instance of the same type of mail service.

Collecting statistics at the same interval for all server types is not recommended. The collection process utilizes different amounts of resources and collects statistics of varying degrees, depending on which mail service is engaged in collecting the statistics. For example, the Housekeeper process is more resource intensive and collects fewer dynamic statistics than the SMTP server collection process.

The recommended collection intervals for the different types of servers are:

- Housekeeper: 3600 (one hour)
- IMAP: 600 (ten minutes)
- POP: 600 (ten minutes)
- SMTP_IN: 600 (ten minutes)
- SMTP_OUT: 600 (ten minutes)
- List: 600 (ten minutes)

See Also: Appendix H, “Oracle Mail Server Metrics” for more information about server statistics

Note: The collection interval parameters are not configurable in Oracle Enterprise Manager 10g.

See Also: Chapter 4, "Directory Administration Tools" in Oracle Internet Directory Administrator’s Guide for information about how to access `oidadmin`
Using oesmon and oeschart

- NNTP_IN: 600 (ten minutes)
- NNTP_OUT: 600 (ten minutes)

Cleaning Up Mail Statistics
Perform the following steps to clean up mail statistics through the Housekeeper process:

1. Using Application Server Control Console for Collaboration Suite, navigate to the Oracle Mail Service Targets page.

   See Also: "Oracle Enterprise Manager 10g Application Server Control Console for Collaboration Suite" on page 1-3 for information about accessing Application Server Control Console for Collaboration Suite

2. Click Housekeeper.

3. Click an instance in the Process Instances section.

4. Select Statistics Cleanup from the Operation Mode list in the Housekeeping Operations section.

5. Click Apply.

6. Return to the Housekeeper page.

7. Click the name of the instance you selected in Step 3.

8. In the General Parameters section, enter the number of days you want to retain sample data in the Age Threshold parameter.

9. Click Apply.

10. Stop and start the Housekeeper process to apply the changes.

Mail Statistics Schema
Each mail process has a default store database. Processes supporting multiple stores, such as the IMAP server, have a default store that is set in the orclMailAdminStoreDN parameter during the installation of each Oracle Collaboration Suite Applications tier.

Statistical information is stored in tables in the esperftbl tablespace in the default mail store of the process. Because these tables can expand indefinitely, you should monitor the esperftbl tablespace and delete or export data as needed.

The schema consists of the following:

- es_perf_process Table
- es_perf_metric Table
- es_perf_timestamp Table
- es_perf_sample Table
- es_perf_data View

es_perf_process Table The es_perf_process table is a list of the process instance records. The column process_dn is the complete distinguished name (DN) of the process, found in Oracle Internet Directory. The processes that produce metric data insert records into this table as needed.
Table 7–7 lists values and descriptions for columns contained in the `es_perf_process` table.

**Table 7–7  es_perf_process Table**

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process_id</td>
<td>Number (nonzero)</td>
<td>An internal assigned unique number for each process</td>
</tr>
<tr>
<td>process_dn</td>
<td>Varchar2 (500)</td>
<td>The DN of the process in Oracle Internet Directory</td>
</tr>
</tbody>
</table>

**es_perf_metric Table** Table 7–8 lists values and descriptions for columns contained in the `es_perf_metric` table.

**Table 7–8  es_perf_metric Table**

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>metric_id</td>
<td>Number (nonzero)</td>
<td>Internally assigned unique number for each metric</td>
</tr>
<tr>
<td>metric_name</td>
<td>Varchar2 (100)</td>
<td>Name of the metric</td>
</tr>
<tr>
<td>metric_type</td>
<td>Number (nonzero)</td>
<td>If 1, the metric is numeric</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If 2, the metric is a string, and defines which column is important in the</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>es_perf_sample</code> table</td>
</tr>
</tbody>
</table>

**es_perf_timestamp Table** The `es_perf_timestamp` table records each time metric data is stored in the tables. This table, along with the `es_perf_data` view grows without bound over time. You must clean out historic data that is no longer needed for charting or analysis at the installation. This can be done by configuring the Housekeeper process.

Table 7–9 lists values and descriptions for columns contained in the `es_perf_timestamp` table.

**Table 7–9  es_perf_timestamp Table**

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>timestamp_id</td>
<td>Number</td>
<td>Internally assigned unique number for each time period that a process enters</td>
</tr>
<tr>
<td>date</td>
<td>Date</td>
<td>Time the data was inserted</td>
</tr>
</tbody>
</table>

**es_perf_sample Table** The `es_perf_sample` table records each metric at each time stamp. This table increases over time, so you must delete data that is no longer required in order to keep the table size manageable.

There are two possible columns that store the sample data, depending upon whether the data is numerical (`nvalue`) or a string (`svalue`).

Table 7–10 lists values and descriptions for columns contained in the `es_perf_sample` table.

**Table 7–10  es_perf_sample Table**

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process_id</td>
<td>Number (nonzero)</td>
<td>Corresponds to the process_id row in <code>es_perf_process</code></td>
</tr>
</tbody>
</table>
Using oesmon and oeschart

**Table 7–10  (Cont.) es_perf_sample Table**

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>metric_id</td>
<td>Number (nonzero)</td>
<td>Corresponds to the metric_id row in es_perf_metric</td>
</tr>
<tr>
<td>timestamp_id</td>
<td>Number (nonzero)</td>
<td>Corresponds to the timestamp_id row in es_perf_timestamp</td>
</tr>
<tr>
<td>nvalue</td>
<td>Number (nonzero)</td>
<td>Numeric value of the metric (if the metric is numeric)</td>
</tr>
<tr>
<td>svalue</td>
<td>Varchar2 (1000)</td>
<td>String value of the metric (if the metric is a string)</td>
</tr>
</tbody>
</table>

**es_perf_data View**  
\( \text{es\_perf\_data} \) is a view of the tables described in this section: es_perf_process, es_perf_metric, es_perf_timestamp, and es_perf_sample. Table 7–11 lists values and descriptions for columns contained in the es_perf_data view.

**Table 7–11  es_perf_data View**

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process_dn</td>
<td>Varchar2 (500)</td>
<td>The DN of the process in Oracle Internet Directory</td>
</tr>
<tr>
<td>metric_name</td>
<td>Varchar22 (100)</td>
<td>Name of the metric</td>
</tr>
</tbody>
</table>
| metric_type | Number (nonzero)       | If 1, the metric is numeric  
If 2, the metric is a string, and defines which column is important in the es_perf_sample table |
| timestamp   | Date                   | Time the value was sampled                                                  |
| nvalue      | Number (nonzero)       | Numeric value of the metric (if the metric is numeric)                      |
| svalue      | Varchar2 (1000)        | String value of the metric (if the metric is a string)                      |

**Creating Graphs**

The oeschart utility creates graphs. The utility requires a single command-line parameter that points to a property file. The property file is a text file with keyword value pairs defining the information the utility needs to generate the graph. A valid property file would have the following mandatory and optional parameters.

Table 7–12 and Table 7–13 describe mandatory entries and optional values, respectively.

**Table 7–12  oeschart Mandatory Properties**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Host name of the statistics database</td>
</tr>
<tr>
<td>port</td>
<td>Database listener port</td>
</tr>
<tr>
<td>sid</td>
<td>SID or service name for the server</td>
</tr>
<tr>
<td>username</td>
<td>Account user</td>
</tr>
<tr>
<td>password</td>
<td>Account password</td>
</tr>
<tr>
<td>process_dn</td>
<td>Query used to gather statistics, such as process_dn=%value_in_ini_file%, which retrieves all processes that follow this DN pattern. This lets you graph a specific process, a set of processes, or the entire system by specifying the level of detail.</td>
</tr>
</tbody>
</table>
Using oesmon and oeschart

Monitoring Oracle Mail

The following is an example of a property file that informs the oeschart utility to generate an xy graph of the number of concurrent IMAP sockets for all IMAP servers in aggregate over the last 24 hours:

```
server=testdb.acme.com
sid=test
port=1521
username=schema_owner_username
password=schema_owner_username_password
process_dn=test1:um_system:imap:
```

### Table 7–12 (Cont.) oeschart Mandatory Properties

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>metric_name</td>
<td>Metric to query</td>
</tr>
<tr>
<td>graph_type</td>
<td>Type of graph. Possible graphs are:</td>
</tr>
<tr>
<td></td>
<td>■ command_data</td>
</tr>
<tr>
<td></td>
<td>■ xy_rate</td>
</tr>
<tr>
<td></td>
<td>■ xy_cummulative</td>
</tr>
<tr>
<td></td>
<td>■ xy_current</td>
</tr>
<tr>
<td>image_file_name</td>
<td>Choose a name for the generated file.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: Either .gif or .png will be appended to this file name depending upon which encode_type you choose.</td>
</tr>
<tr>
<td>image_title</td>
<td>Title to display on the graph</td>
</tr>
<tr>
<td>number_of_hours</td>
<td>Number of hours, going backward in time, starting from the present</td>
</tr>
</tbody>
</table>

### Table 7–13 oeschart Optional Properties

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>encode_type</td>
<td>gif</td>
<td>Possible values are gif and png</td>
</tr>
<tr>
<td>image_dir</td>
<td>./</td>
<td>Directory where graphs are stored</td>
</tr>
<tr>
<td>aggregate_time_period</td>
<td>600</td>
<td>Time span in which multiple logging processes are grouped together and the metrics combined to show an aggregate value.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>As an example, consider two running IMAP servers, IMAP1 and IMAP2. IMAP1 logged its statistics at 3:00 p.m. and IMAP2 logged its statistics at 3:02 p.m. The servers log statistics at intervals specified in seconds using oidadmin relative to when they started; in this case, IMAP2 must have been started 2 minutes after IMAP1. To show the total number of sockets on the system, combine the values from IMAP1 and IMAP2. aggregate_time_period defines what is an acceptable window for different process statistics to be combined. This should be the same as the submit period specified in oidadmin for this process type.</td>
</tr>
<tr>
<td>max_lifetime</td>
<td>300</td>
<td>Number of seconds until the program terminates</td>
</tr>
<tr>
<td>show_statistics</td>
<td>FALSE</td>
<td>Number of data points, minimum, maximum, average, and median, at the bottom of the graph</td>
</tr>
<tr>
<td>debug</td>
<td>FALSE</td>
<td>Provides a detailed output of the utility</td>
</tr>
</tbody>
</table>

The following is an example of a property file that informs the oeschart utility to generate an xy graph of the number of concurrent IMAP sockets for all IMAP servers in aggregate over the last 24 hours:
Using oesmon and oeschart

```plaintext
graph_type=xy_current
image_dir=full_path_images_directory
number_of_hours=24
encode_type=png
show_statistics=true
aggregate_time_period=600
debug=false
max_lifetime=120

metric_name=.ES_SPS.socket.currload
image_file_name=socketcount
image_title=Socket count on test1
```

**See Also:** Appendix H, "Oracle Mail Server Metrics" for a complete list of metric names

oeschart obtains information from the es_perf schema and generates one of four possible types of charts. Three of these are variations of scatter graphs. The fourth is a bar chart.

By executing oeschart at regular intervals, you are provided with a current view that can be published on a company Web site or within Oracle Enterprise Manager 10g.

For example, you can schedule the creation of graphs that show information such as the number of connected sockets, the login response time, and the number of queued outbound messages, and publish the results in a custom HTML page or in Oracle Enterprise Manager.

### Displaying Graphs in Oracle Enterprise Manager

To display graphs in Oracle Enterprise Manager:

1. Modify the target metadata definition.

   The `$ORACLE_HOME/sysman/admin/metadata` directory contains a list of target metadata definition files.

   For a particular target definition, add the following elements to the **Instance Properties** section:

   ```xml
   <!--This property specifies the total number of statistic charts to be displayed -->
   <InstanceProperty NAME="totalNumberOfStats" CREDENTIAL="FALSE" OPTIONAL="TRUE">
     <Display>
       <Label NLSID="totalnumberofstats">Total Number of Statistics</Label>
     </Display>
   </InstanceProperty>

   <!--This property specifies the header title for the first charting picture-->
   <InstanceProperty NAME="Title0" CREDENTIAL="FALSE" OPTIONAL="TRUE">
     <Display>
       <Label NLSID="stat0">Statistic Number 0</Label>
     </Display>
   </InstanceProperty>

   <!--This property specifies the tool tips string for the first charting picture, coded to Section 508 standards-->
```
2. To increase the number of charts displayed, change the value of the `totalNumberOfStats` parameter in the `targets.xml` file accordingly, and the additional picture properties must be defined using the following naming standard:

   Title[N], ToolTips[N], PicPath[N], PicPhysicalPath[N]

   In this naming standard, `N` is a nonnegative natural number.

3. Edit the `targets.xml` file to specify the property instance values, by adding the following properties to the specific target section in `$ORACLE_HOME/sysman/emd/targets.xml` file:

   ```xml
   <Property NAME="totalNumberOfStats" VALUE="1"/>
   <Property NAME="ToolTips0" VALUE="My First Statistic Tool Tips"/>
   <Property NAME="PicPhysicalPath0" VALUE="/sysman/webapps/emd/ias/umsg/es/images/pic1.gif"/>
   <Property NAME="PicPath0" VALUE="/emd/ias/umsg/es/images/pic1.gif"/>
   <Property NAME="Title0" VALUE="My First Statistic Header"/>
   ```

   In the preceding example, the `...es/images...` portion of the directory does not exist. It must be created or the administrator can choose another directory.

If any of the following situations occur, the charting picture is skipped and not displayed in Oracle Enterprise Manager:

- `totalNumberOfStats` is missing, zero, or not a number
- `Title[N]` is missing for the particular chart
- `ToolTips[N]` is missing for the particular chart
- `PicPath[N]` is missing for the particular chart
- `PicPhysicalPath[N]` is missing for the particular chart
- The picture file specified under `PicPhysicalPath[N]` does not exist
This chapter discusses Oracle Mail policies configured using the Oracle Collaboration Suite 10g WebMail client.

This chapter includes the following topics:

- Overview of Oracle Mail Policies
- Managing Oracle Mail Filters
- Oracle Mail Routing Control
- Oracle Mail Archive Policies
- Message Recall

Overview of Oracle Mail Policies

Oracle Mail policies are tools that an administrator can use to filter out unwanted mail that may contain viruses, or prevent spam from being sent and received.

Virus filters can be applied to messages coming in from and going out to the Internet, messages being sent locally (between users of Oracle Collaboration Suite), and messages being stored in the Oracle Collaboration Suite Database to detect anything that could potentially harm the e-mail system.

Additional tools include routing control, which provides administrators with the ability to trust or reject e-mail from specific senders, domains, recipients, and hosts, thereby minimizing or eliminating spam e-mail; and archive policies, which enable administrators to store messages in a third-party storage facility in order to better manage message storage and retrieval.

Using the Oracle WebMail client, administrators can:

- Manage filters for antivirus, antispam, or custom filters, and create archive policies.
- Create, reorder, and remove filters, and apply them to various points in the message delivery cycle.
- Configure Oracle Mail to trust or reject messages from specific people, domains, or servers.
- Set archiving policies of messages for users.
Managing Oracle Mail Filters

Filters enable administrators to customize the processing of messages by checking whether a set of conditions are met by a message and, if those conditions have been met, to execute some action within Oracle Mail.

The Filters page of the Oracle WebMail client is the page on which you create filters. After filters are created, they are listed on this page, and can be edited, removed, or applied to specific servers from this location.

On this page, you can add new filters, edit and remove existing filters, and change the order in which the filters are applied.

This section includes the following topics:

- Creating a Filter
- Editing Filters
- Reordering Filters
- Applying Filters
- Editing Applied Filters

Creating a Filter

To create a filter:

1. Open the Oracle WebMail client.

   **See Also:** "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client

2. Click the **Administration** tab.

3. Click the **Policy** subtab.

4. Click **Add** to display the New Filter page.

5. Enter information in the following fields:

   - **Name**: The name of the filter. This information is required.
   - **File Name**: Enter a library file to be called to perform the specified filter function. This information is required.
   - **Active**: Select **Yes** from the list to enable the filter. This information is required.
   - **External Process**: This information is required.
   - **Capable of Message Modification**: Select whether or not you want the software to modify a message upon which a filter has acted. This information is required.
   - **Description**: Enter descriptive text of what the function of the filter is.
   - **External Administration URL**: If this filter requires additional administration, enter a URL to an administration page of the third-party software that you are trying to call with this filter.

   In some cases, you may want to override the filter and system flags associated with a particular filter. To do this, click the icon adjacent to **Filter Flags** or
System Flags to list the values that will be overridden during filter application. The filter is then applied to all messages.

For the SAVSE filters shipped with Oracle Mail, the values for Filter Flags or System Flags are inherited from the filter definition and the filter is only applied to messages that meet these criteria.

6. Click OK to add the filter.

Editing Filters

To edit filters:

1. Open the Oracle WebMail client.

   See Also: "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client

2. Click the Administration tab.

3. Click the Policy subtab.

4. Click the name of the filter in the Name column to display the Edit Filter page.

5. Edit the information, as necessary.

   See Also:
   - "Editing SAVSE Filters" on page 6-10 for information about editing SAVSE filters
   - "Applying Filters" on page 8-4 for definitions of the various attributes

6. Enter filter or system flags.

   Table 8–1 lists current valid system flags for filter processes.

   Note: These system flags to not apply to the SAVSE filters.

<table>
<thead>
<tr>
<th>System Flag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>version=ocsv1</td>
<td>Set this flag to ocsv1 if an Oracle Collaboration Suite Release 1 (9.0.3) external filter process is used in Oracle Collaboration Suite 10g.</td>
</tr>
<tr>
<td>forward=1</td>
<td>Set this flag to 1 for filters acting as mail forwarding MTAs that will be responsible for further handling of mail messages.</td>
</tr>
</tbody>
</table>

7. Click OK to apply any changes.

Reordering Filters

Reordering filters changes the order in which the filters are applied. An administrator can specify which filters are applied to messages first.

To reorder filters:
1. Open the Oracle WebMail client.

   See Also: "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client

2. Click the Administration tab.

3. Click the Policy subtab.

4. Click Reorder.

5. Select the filter you want to move and use the arrows to move the filter toward the top or bottom of the list.

6. Click OK to apply any changes or Cancel to return to the Filters page.

Applying Filters

You can apply particular filters to act on messages at various stages in the delivery cycle of the message. Filters can be applied to incoming messages, outgoing messages, messages delivered within the local Oracle Mail domain, and all messages stored in the Oracle Collaboration Suite Database.

To apply filters:

1. Open the Oracle WebMail client.

   See Also: "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client

2. Click the Administration tab.

3. Click the Policy subtab.

4. Click the Application link.

5. Click either Incoming, Outgoing, Local, or Collaboration Suite Database to display a list of Oracle Collaboration Suite Applications tier servers associated with that point in the delivery cycle of the message.

   - Incoming: Filter is applied to all incoming messages.
   - Outgoing: Filter is applied to all messages delivered outside the local Oracle Mail domain.
   - Local: Filter is applied to all messages delivered within the local Oracle Mail domain.
   - Collaboration Suite Database: Filter is applied to all messages stored in the Oracle Collaboration Suite Database.

6. Click the icon in the Configure Filters column. If you clicked Collaboration Suite Database in the preceding step, go to "Configuring Filters for an Oracle Collaboration Suite Database" on page 8-5 for a description of that page.

7. Click Apply Filter.

8. Select a filter from the Filter list.

9. In the Options section, select Yes from the Allow Message Modification list to enable the filter to modify messages.
10. In some cases, you may want to override the filter and system flags associated with a particular filter. To do this, click the icon adjacent to Filter Flags or System Flags to list the values that will be overridden during filter application. The filter is then applied to all messages.

Otherwise, the values for Filter Flags or System Flags are inherited from the filter definition, and the filter is only applied to messages that meet these criteria.

11. Click OK to apply the filter and return to the Configure Filters page. Applied filters are displayed.

12. To disable a filter, select a filter from the list to be unapplied and click Unapply Filter. A confirmation page displays. Click Yes to confirm or No to cancel.

13. In the Advanced section, click Remove Instance Level Settings.

---

**Note:** This section displays only if some filter attribute is set at the instance level. Typically, all filter attributes are set at the target level, only, but if a filter is applied at the instance level, this button displays. When the button is clicked, the instance level settings are removed.

---

14. If you apply any filters, you must restart the associated servers.

- For incoming mail, restart the SMTP inbound, SMTP outbound, and NNTP inbound servers.
- For outgoing mail, restart the SMTP outbound server and the List Server.

---

**Note:** Because the NNTP outbound server is not integrated with the filtering system, is not necessary to restart the NNTP outbound server when filters are applied to outgoing mail.

---

- For local mail, restart the SMTP inbound and SMTP outbound servers and the List Server.
- For mail stored on the Oracle Collaboration Suite Database, restart the Virus Scrubber.

**Configuring Filters for an Oracle Collaboration Suite Database**

When applying filters to the Oracle Collaboration Suite Database, set the following attributes:

- **Pre-Scan Mode:** Select one of the following choices from the list:
  - **Disabled:** Only those messages that have been isolated by a previous prescan operation are sent through the filters for scrubbing.
  - **Enabled:** First, all messages are prescanned and messages that match the prescan criteria are isolated. Then, only those isolated messages are sent through the filters for scrubbing.
  - **Pre-Scan Only:** All messages are prescanned only. Messages that match the prescan criteria are isolated.

- In the **Pre-Scan Criteria** section, select all or any of the following from the Matching list to specify that all, or any one, of the prescan filters listed in the table are applied.
Messages matching these criteria are removed from the mailbox of the respective users until the third-party scanner verdict is harmless/not-affected.

If no prescan filters are listed, add them, as follows:

1. Click Add.
2. Enter information for the following attributes:
   - **Message Attribute**: Select from this list upon which attribute of e-mail messages this filter will act. Attributes include: Subject, From, Sent Date, Attachment Name, Scanner Version, and Specify Header.
   - **Operator**: Select from this list to specify whether the message attribute should contain or not contain a certain value.
   - **Value**: Enter the condition upon which the message attribute will act.

   For example, to filter messages from john@foo.com, select From as the Message Attribute, and contains from the Operator list, and enter john@foo.com in the Value field.

3. Click Continue to return to the Configure Filters page. Prescan filters are displayed in the table.

   ■ In the Filters section, apply filters that have been configured for scrubbing Oracle Collaboration Suite Databases, as follows:
   
   1. Click Apply Filter.
   2. Select a filter from the Filter list.
   3. Information about the selected filter displays in the Definition section.
   4. In the Options section, select Yes from the Allow Message Modification list to enable the filter to modify messages.
   5. In some cases, you may want to override the filter and system flags associated with a particular filter. To do this, click the icon adjacent to Filter Flags or System Flags to list the values that will be overridden during filter application. The filter is then applied to all messages. Otherwise, the values for Filter Flags or System Flags are inherited from the filter definition and the filter is only applied to messages that meet these criteria.
   6. Click OK to apply the filter and return to the Configure Filters page. Applied filters are displayed.
   7. To disable a filter, select a filter from the list to be unapplied and click Unapply Filter. A confirmation page displays. Click Yes or No.

   ■ In the If Repair Fails section, choose whether a virus-infected message is to be immediately deleted or quarantined to folder.
   
   1. Select from the If Repair Fails list:
Managing Oracle Mail Filters

Oracle Mail Policies 8-7

- **Delete**: To delete the message
- **Quarantine**: To quarantine the message somewhere for possible future repair

---

**Note**: When **Quarantine** is selected, two new text boxes are rendered in Oracle WebMail:

**Quarantine Destination E-Mail Address**: Enter a valid e-mail address to which infected messages are to be sent for quarantine

**Quarantine Destination Folder**: Specify a valid folder name into which quarantined messages are stored

---

2. Enter a message to send to the sender of a failed message in the **Notification Message to Message Sender** field.

3. Enter a message to send to the recipient of a failed message in the **Notification Message to Message Recipient** field.

- If there are filters applied at the instance level, the **Advanced** section displays. Click **Remove Instance Level Settings** to remove all settings at the instance level.

---

**Note**: This section displays only if some filter attribute is set at the instance level. Typically, all filter attributes are set at the target level, only, but if a filter is applied at the instance level, this button displays. When the button is clicked, the instance level settings are removed.

---

- Click **Save** to save the prescan criteria to Oracle Internet Directory.

---

**Editing Applied Filters**

Once a filter has been applied, it can be edited at any time.

To edit applied filters:

1. Open the Oracle WebMail client.

   **See Also**: "**Oracle Collaboration Suite 10g WebMail Client**" on page 1-2 for information about how to access the Oracle WebMail client

2. Click the **Administration** tab.

3. Click the **Policy** subtab.

4. Click the **Application** link.

5. Click **Incoming**, **Outgoing**, **Local**, or **Collaboration Suite Database** to display a list of Oracle Collaboration Suite Applications tier servers associated with that point in the delivery cycle of the message.

6. To unapply a filter, select a filter from the list to be unapplied and click **Unapply Filter**.

   A confirmation page displays. Select **Yes** to unapply the selected filter.

7. Click the icon in the **Configure Filters** column.
8. Click the icon in the **Edit** column of the filter to be edited to display the configuration page for that filter.

9. Attributes in the **Options** section, only, can be edited.

10. Click **OK** to apply edits to the filter.

---

### Oracle Mail Routing Control

Spam and viruses are continuing problems for e-mail users. Routing control provides administrators with the ability to configure Oracle Mail with a basic set of message functions, such as rejecting or trusting e-mail from specific senders, domains, recipients, and hosts. Routing control rules can be applied to incoming mail, outgoing mail, and incoming news messages.

This section includes the following topics:

- Configuring Routing Control for Incoming Mail
- Configuring Routing Control for Outgoing Mail
- Configuring Routing Control for Incoming News

---

**Note:** Any changes made for routing control settings in the Oracle WebMail client are automatically reflected in Oracle Enterprise Manager 10g.

---

### Configuring Routing Control for Incoming Mail

Configure Oracle Mail to reject or trust incoming mail according to various criteria, and create rewriting rules for sender and recipient.

There are four categories of routing control settings for incoming mail, each accessible by a link on the Configuring Routing Control: Incoming Mail page:

- **General:** These settings enable DNS checks; establish limits on incoming messages to prevent flooding of the network; and specify whether relaying of messages through the system is allowed, and to which domains listed in the table messages can be relayed.

- **Reject:** These settings specify which messages containing any of certain IP addresses, domains, or e-mail addresses are to be denied access to the system. Reject settings are tested before Trust settings.

- **Trust:** These settings specify which messages containing any of certain IP addresses, domains, or e-mail addresses are to be granted access to the system.

- **Advanced:** These settings enable security checks on incoming messages; establish limits on the number of recipients allowed in an envelope, the number of headers allowed in a message, and the size of the shell; specify header values and message attachments to be disallowed; and establish rewriting rules.

To configure routing control for incoming mail:

1. Open the Oracle WebMail client.

   **See Also:** "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client

2. Click the **Administration** tab.
3. Click the Policy subtab.

4. Click Routing Control.

5. Click Incoming Mail to configure routing control settings for incoming mail.

6. Click the icon in the Configure Routing Control column to display the Configure Routing Control: Incoming Mail page.

7. Click the appropriate link to display a particular routing control settings page.

This section includes the following topics:

- Configuring General Routing Control Settings for Incoming Mail
- Configuring Reject Routing Control Settings for Incoming Mail
- Configuring Trust Routing Control Settings for Incoming Mail
- Configuring Advanced Routing Control Settings for Incoming Mail
- Saving and Copying Routing Control Settings for Incoming Mail

**Configuring General Routing Control Settings for Incoming Mail**

To configure general routing control settings:


2. Ensure that Enable Routing Control is checked.

3. Select Enable from the DNS check on HELO/EHLO domains list to check if the domain name in the HELO/EHLO command exists on the DNS server. If it does not exist, the connection is rejected.

4. Select Enable from the DNS check on sender domains list to determine if the sender’s address exists on the DNS server.

**Denial of Service Attacks Section**

5. Enter a number in the Maximum Flood Count field that is the sum of the number of e-mail messages and the number of connection requests from this host within a time interval considered to be flooding, a characteristic of spam in which a sender sends a large amount of mail to one server in a short period of time.

6. Enter a number in the Maximum Time Interval field that is the number of seconds, used in conjunction with Maximum Flood Count, to determine whether a host is flooding the server with unwanted e-mail.

**Allowed Relay Domains Section**

7. Select True, False, or Authenticate from the Allow message relay list.

   This setting will determine whether the SMTP Inbound server will act as a relay server to other MTAs.

   - **True**: Allows relay of e-mail whose recipient domains are listed in the table
   - **False**: Disallows relay of e-mail whose recipient domains are listed in the table
   - **Authenticate**: Authenticated e-mail messages will not be delivered to all outside domains but only to those domains listed in the table

8. Search the list of available domains by entering a text string in the Search field and clicking Go.
9. To add domains to the list, click **Add Domain** to display the Add Allowed Relay Domains page.

10. Enter the name of an allowed domain in the **Domain** field and click **OK** to add the domain.

**Configuring Reject Routing Control Settings for Incoming Mail**

To configure the server to block rejected IP and e-mail addresses, domains, and sender-recipient pairs:

1. Click **Reject** on the Configure Routing Control: Incoming Mail page.

2. Ensure that **Enable Routing Control** is checked.

**Client IP Addresses Section**

Add, or search for, rejected client IP addresses in this section.

To search the list of disallowed IP addresses, enter a string in the **Search** field and click **Go**.

3. Click **Add IP Address** to display the Add IP Addresses to Reject page.

4. Enter an IP address and reason for rejection in the appropriate fields.

   Click **Add Another Row** to enter additional IP addresses.

5. Click **OK** to add the IP address to the list of rejected IP addresses and to return to the Configure Routing Control: Incoming Mail page.

   Click **Cancel** to return to the Configure Routing Control: Incoming Mail page.

6. To remove an IP address from the rejected list on the Configure Routing Control: Incoming Mail page, select an IP address and click **Remove**. A confirmation page displays.

**Note:** The **Remove** button displays only when the Client IP Addresses list is populated.

7. To edit IP address information, click the icon in the **Edit** column on the Configure Routing Control: Incoming Mail page. Edit the settings as necessary.

**Client Domains Section**

Add or search for rejected client domains in this section.

To search the list of disallowed domains, enter a string in the **Search** field and click **Go**.

8. Click **Add Domain** to display the Add Client Domains to Reject page.

9. Enter a domain name and reason for rejection in the appropriate fields.

   Click **Add Another Row** to enter additional domains.

10. Click **OK** to add the domain to the list of rejected client domains and to return to the Configure Routing Control: Incoming Mail page.

    Click **Cancel** to return to the Configure Routing Control: Incoming Mail page.

11. To remove a client domain from the rejected list on the Configure Routing Control: Incoming Mail page, select a domain and click **Remove**. A confirmation page displays.
12. To edit client domain information, click the icon in the Edit column on the Configure Routing Control: Incoming Mail page. Edit the settings as necessary.

**Sender Domains Section**
Add or search for rejected sender domains in this section.
To search the list of disallowed domains, enter a string in the Search field and click Go.

13. Click **Add Domain** to display the Add Sender Domains to Reject page.
14. Enter a domain name and reason for rejection in the appropriate fields.
   Click **Add Another Row** to enter additional domains.
15. Click **OK** to add the domain to the list of rejected sender domains and to return to the Configure Routing Control: Incoming Mail page.
   Click **Cancel** to return to the Configure Routing Control: Incoming Mail page.
16. To remove a sender domain from the rejected list on the Configure Routing Control: Incoming Mail page, select a domain and click **Remove**. A confirmation page displays.

**Note:** The Remove button displays only when the Client Domains list is populated.

17. To edit sender domain information, click the icon in the Edit column on the Configure Routing Control: Incoming Mail page. Edit the settings as necessary.

**Sender E-mail Addresses Section**
Add or search for rejected sender e-mail addresses in this section.
To search the list of disallowed sender e-mail addresses, enter a string in the Search field and click Go.

18. Click **Add E-mail Address** to display the Add Sender E-mail Addresses to Reject page.
19. Enter an e-mail address and reason for rejection in the appropriate fields.
   Click **Add Another Row** to enter additional e-mail addresses.
20. Click **OK** to add the address or addresses to the list of rejected sender e-mail addresses and to return to the Configure Routing Control: Incoming Mail page.
   Click **Cancel** to return to the Configure Routing Control: Incoming Mail page.
21. To remove a sender e-mail address from the rejected list on the Configure Routing Control: Incoming Mail page, select an e-mail address and click **Remove**. A confirmation page displays.

**Note:** The Remove button displays only when the Sender E-mail Addresses list is populated.
22. To edit sender e-mail address information, click the icon in the **Edit** column on the Configure Routing Control: Incoming Mail page. Edit the settings as necessary.

**Recipient E-mail Addresses Section**
Add or search for rejected recipient e-mail addresses in this section.
To search the list of disallowed recipient e-mail addresses, enter a string in the **Search** field and click **Go**.

23. Click **Add E-mail Address** to display the Add Recipient E-mail Addresses to Reject page.

24. Enter an e-mail address and reason for rejection in the appropriate fields.
    Click **Add Another Row** to enter additional e-mail addresses.

25. Click **OK** to add the address or addresses to the list of rejected recipient e-mail addresses and to return to the Configure Routing Control: Incoming Mail page.
    Click **Cancel** to return to the Configure Routing Control: Incoming Mail page.

26. To remove a recipient e-mail address from the rejected list on the Configure Routing Control: Incoming Mail page, select an e-mail address and click **Remove**. A confirmation page displays.

**Note:** The **Remove** button displays only when the Recipient E-mail Addresses list is populated.

27. To edit recipient e-mail address information, click the icon in the **Edit** column on the Configure Routing Control: Incoming Mail page. Edit the settings as necessary.

**Sender-Recipient Pairs Section**
Add or search for rejected sender-recipient e-mail address pairs in this section.
To search the list of rejected sender-recipient pairs, enter a string in the **Search** field and click **Go**.

28. Click **Add Pair** to display the Add Sender-Recipient Pairs to Reject page.

29. In the **Sender** field, enter the information to the left of the at sign (@) in the e-mail address.

30. From the drop down list, select **LOCALDOMAIN** to specify domains within your Oracle Collaboration Suite installation; **NONLOCALDOMAIN** to specify domains outside of your Oracle Collaboration Suite installation; or **(other, please specify)** to specify any domain.
    If you select **(other, please specify)**, you must enter a domain name in the adjacent field.

31. Repeat the previous two steps for the **Recipient** field.

32. Enter a reason for rejection in the **Reject Reason** field.

33. Click **OK** to add the pair to the list of rejected sender-recipient pairs and to return to the Configure Routing Control: Incoming Mail page.
    Click **Cancel** to return to the Configure Routing Control: Incoming Mail page.
34. To remove a sender-recipient pair from the rejected list on the Configure Routing Control: Incoming Mail page, select an e-mail address and click **Remove**. A confirmation page displays.

**Note:** The **Remove** button displays only when the Sender-Recipient Pairs list is populated.

35. To edit sender-recipient pairs information, click the icon in the **Edit** column on the Configure Routing Control: Incoming Mail page. Edit the settings as necessary.

### Configuring Trust Routing Control Settings for Incoming Mail

For some routing control settings, an administrator can specify whether authentication of the MTA is required.

Authentication requires that the sender enter a user name and password the first time a message sent. Once established, authentication by the sender is no longer required.

To configure the server to accept trusted IP and e-mail addresses, domains, and sender-recipient pairs:

1. Click **Trust** on the Configure Routing Control: Incoming Mail page.
2. Ensure that **Enable Routing Control** is checked.

**Client IP Addresses Section**

Add, search for, remove, or edit trusted client IP addresses in this section.

To search the list of allowed IP addresses, enter a string in the **Search** field and click **Go**.

3. Click **Add IP Address** to display the Add Trusted IP Addresses page.
4. Enter an IP address in the **IP Address** field.
   - Click **Add Another Row** to enter additional IP addresses.
5. Click **OK** to add the IP address to the list of trusted IP addresses and to return to the Configure Routing Control: Incoming Mail page.
   - Click **Cancel** to return to the Configure Routing Control: Incoming Mail page.
6. To remove an IP address from the trusted list on the Configure Routing Control: Incoming Mail page, select an IP address and click **Remove**. A confirmation page displays.

**Note:** The **Remove** button displays only when the Client IP Addresses list is populated.

7. To edit IP address information, click the icon in the **Edit** column on the Configure Routing Control: Incoming Mail page. Edit the settings as necessary.
Client Domains Section
Add, search for, remove, or edit trusted client domains in this section.

Note: Antispam checks will not be applied to messages sent from computers in the domains listed in this section.

To search the list of allowed domains, enter a string in the Search field and click Go.

8. Click Add Domain to display the Add Trusted Client Domains page.

9. Enter a domain name in the Domain field.
   Click Add Another Row to enter additional domains.

10. Click OK to add the domain to the list of trusted client domains and to return to the Configure Routing Control: Incoming Mail page.
    Click Cancel to return to the Configure Routing Control: Incoming Mail page.

11. To remove a client domain from the trusted list on the Configure Routing Control: Incoming Mail page, select a domain and click Remove. A confirmation page displays.

Note: The Remove button displays only when the Client Domains list is populated.

12. To edit client domain information, click the icon in the Edit column on the Configure Routing Control: Incoming Mail page. Edit the settings as necessary.

Sender Domains Section
Add, search for, remove, or edit trusted sender domains in this section.

To search the list of allowed domains, enter a string in the Search field and click Go.

13. Click Add Domain to display the Add Trusted Sender Domains page.

14. Enter a domain name in the Domain field. Select Require MTA Client to be Authenticated to require that the MTA client be authenticated.
    Click Add Another Row to enter additional domains.

15. Click OK to add the domain to the list of trusted sender domains and to return to the Configure Routing Control: Incoming Mail page.
    Click Cancel to return to the Configure Routing Control: Incoming Mail page.

16. To remove a sender domain from the trusted list on the Configure Routing Control: Incoming Mail page, select a domain and click Remove. A confirmation page displays.

Note: The Remove button displays only when the Sender Domains list is populated.

17. To edit sender domain information, click the icon in the Edit column on the Configure Routing Control: Incoming Mail page. Edit the settings as necessary.
**Sender E-mail Addresses Section**
Add, search for, remove, or edit trusted sender e-mail addresses in this section.

To search the list of allowed sender e-mail addresses, enter a string in the **Search** field and click **Go**.

18. Click **Add E-mail Address** to display the Add Trusted Sender E-mail Addresses page.

19. Enter an e-mail address. Select **Require MTA Client to be authenticated** to enable another level of security to the sender e-mail address listed.

   Click **Add Another Row** to enter additional e-mail addresses.

20. Click **OK** to add the address or addresses to the list of trusted sender e-mail addresses and to return to the Configure Routing Control: Incoming Mail page.

   Click **Cancel** to return to the Configure Routing Control: Incoming Mail page.

21. To remove a sender e-mail address from the trusted list on the Configure Routing Control: Incoming Mail page, select an e-mail address and click **Remove**. A confirmation page displays.

   **Note:** The **Remove** button displays only when the Sender E-mail Addresses list is populated.

22. To edit sender e-mail address information, click the icon in the **Edit** column on the Configure Routing Control: Incoming Mail page. Edit the settings as necessary.

**Sender-Recipient Pairs Section**
Add, search for, remove, or edit trusted sender-recipient e-mail address pairs in this section.

To search the list of trusted sender-recipient pairs, enter a string in the **Search** field and click **Go**.

23. Click **Add Pair** to display the Add Trusted Sender-Recipient Pairs page.

24. In the **Sender** field, enter the information to the left of the at sign (@) in the e-mail address.

25. From the drop down list, select **LOCALDOMAIN** to specify domains within your Oracle Collaboration Suite installation; **NONLOCALDOMAIN** to specify domains outside of your Oracle Collaboration Suite installation; or **(other, please specify)** to specify any domain.

   If you select **(other, please specify)**, you must enter a domain name in the adjacent field.

26. Repeat the previous two steps for the **Recipient** field.

27. Select **Require MTA Client to be authenticated** to enable another level of security to the sender-recipient pair listed.

28. Click **OK** to add the pair to the list of trusted sender-recipient pairs and to return to the Configure Routing Control: Incoming Mail page.

   Click **Cancel** to return to the Configure Routing Control: Incoming Mail page.
29. To remove a sender-recipient pair from the trusted list on the Configure Routing Control: Incoming Mail page, select an e-mail address and click **Remove**. A confirmation page displays.

**Note:** The **Remove** button displays only when the Sender-Recipient Pairs list is populated.

30. To edit sender-recipient pairs information, click the icon in the **Edit** column on the Configure Routing Control: Incoming Mail page. Edit the settings as necessary.

**Configuring Advanced Routing Control Settings for Incoming Mail**

To configure the server to reject disallowed headers and attachments, and set rewriting rules:

1. Click **Advanced** on the Configure Routing Control: Incoming Mail page.

2. Ensure that **Enable Routing Control** is checked.

3. In the **Maximum number of recipients allowed in the envelope** field, enter a number to limit the number of allowable recipients.

4. From the **Match envelope and message header** list, select either **Do not check** or **Envelope sender and message From header must match**. This setting ensures that the sender identified in the **From** field of a message matches the actual sender of the message.

5. From the **Match SASL authenticated ID and message header** list, select either **Do not check**, **SASL authenticated ID and envelope sender must match**, or **SASL authenticated ID and message From header must match**.

   This is applicable when the SMTP inbound server is enabled for SASL authentication. When **SASL authenticated ID and envelope sender must match** is selected, the ID used for SASL authentication is compared to the actual sender of the message. When **SASL authenticated ID and message From header must match** is selected, the SASL-authenticated ID is compared to the value in the **From** field of the message.

6. In the **Maximum Number of Headers Allowed in a Message** field, enter the maximum number of RFC822 headers allowed in a single message. IMAP uses this parameter to perform a spam check on messages during an **APPEND** operation. The default value is 1000.

7. In the **Maximum Size of Shell** field, enter the maximum size of the database shell, in bytes, for a message. IMAP uses this parameter to perform a spam check on messages during an **APPEND** operation. The shell comprises all the headers of the message plus the placeholders for MIME body parts. The default value is 1000000.

**Disallowed Headers Section**

To search the list of disallowed headers, enter a string in the **Search** field and click **Go**.
8. Click **Add Header** to display the Create Disallowed Headers page.

9. Select a field from the **Header** list.

10. Enter a string in the **Value** field.

11. Enter a reason for rejection in the **Reject Reason** field.

12. Click **OK** to add the header information to the list of disallowed headers and return to the Configure Routing Control: Incoming Mail page.

   Click **Cancel** to return to the Configure Routing Control: Incoming Mail page.

13. To remove a header from the disallowed list on the Configure Routing Control: Incoming Mail page, select a header and click **Remove**. A confirmation page displays.

   **Note:** The **Remove** button displays only when the Disallowed Headers list is populated.

14. To edit header information, click the icon in the **Edit** column.

**Disallowed Attachments Section**

To search the list of disallowed attachments, enter a string in the **Search** field and click **Go**.

15. Click **Add Attachments** to display the Add Attachments to Reject page.

16. Enter an attachment name (wildcards can be used) and a reason for rejection.

17. Click the icon in the **Remove** column to remove the attachment from the list.

18. Click **Add Another Row** to add another attachment to reject.

19. Click **OK** to add the attachments to the list of rejected attachments and return to the Configure Routing Control: Incoming Mail page.

   Click **Cancel** to return to the Configure Routing Control: Incoming Mail page.

20. To remove an attachment from the disallowed list on the Configure Routing Control: Incoming Mail page, select an attachment name and click **Remove**. A confirmation page displays.

   **Note:** The **Remove** button displays only when the Disallowed Attachments list is populated.

21. To edit attachment information, click the icon in the **Edit** column.

**Rewriting Rules Section**

This section has one subsection: Recipient Rewriting Rules.

**Recipient Rewriting Rules**

22. Click **Create Rule** to display the Create Recipient Rewriting Rule page.

23. In the **Pattern to match** field, enter a string using $+ to match a nonempty substring and $* to match an empty or nonempty substring. For example, $+.+$@company.com matches first.last@company.com.
24. Enter delimiting characters in the **Characters delimiting a substring in the pattern** field.

25. From the **Action** list, select **Apply Rewrite** to rewrite the address according to the rewrite string rule; **Reject Address** to reject the address, send a DSN to sender, and continue with next recipient; **Discard Address** to discard the address and continue with next recipient; or **Stop** to ignore subsequent rules.

26. In the **Rewrite to Apply** field, enter a string using $1, $2, and so on to substitute matching parts. For example, rewriting $+_@company.com to $1.$2@company.com rewrites first_last@company.com to first.last@company.com.

27. Enter a description for the recipient rewriting rule in the **Description** field.

28. Click **OK** to add the new rule to the list of recipient rewriting rules and return to the Configure Routing Control: Incoming Mail page. Click **Cancel** to return to the Configure Routing Control: Incoming Mail page.

29. Click **Reorder** to display the Reorder Recipient Rewriting Rules page and change the order in which recipient rewriting rules are applied.

30. Select the rule you want to move and use the arrows to move the rule toward the top or bottom of the list.

31. Click **OK** to apply any changes or **Cancel** to return to the Configure Routing Control: Incoming Mail page.

32. To remove a recipient rewriting rule from the list on the Configure Routing Control: Incoming Mail page, select a rule and click **Remove**. A confirmation page displays.

---

**Note:** The **Remove** button displays only when the Recipient Rewriting Rules list is populated.

---

33. To edit recipient rewriting rule information, click the icon in the **Edit** column.

**Saving and Copying Routing Control Settings for Incoming Mail**

When finished with routing control, you must save the settings to apply them. You can also copy routing control settings to other servers.

To save routing control settings, click **Save Settings** on the Configure Routing Control Settings: Incoming Mail page.

**Note:** You can save or copy routing control settings at any time from any of the four category pages: General, Reject, Trust, and Advanced.

To copy the settings applied to this server to other available servers, click **Copy Settings**.

1. Select a server from the **Available Servers** list and move it to the **Selected Servers** using the buttons between the lists.

2. Click **OK** to return to the Configure Routing Control: Incoming Mail page. Click **Cancel** to return to the Configure Routing Control page without applying any routing control settings.
Configuring Routing Control for Outgoing Mail

To configure Oracle Mail to apply sender or recipient rewriting rules to outgoing mail:

1. Open the Oracle WebMail client.

See Also: "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client

2. Click the Administration tab.
3. Click the Policy subtab.
4. Click Routing Control.
5. Click Outgoing Mail to configure routing control settings for outgoing mail.
6. Click the icon in the Configure Routing Control column to display the Configure Routing Control: Outgoing Mail page.
7. Click the appropriate link to display a particular routing control settings page.

Sender Rewriting Rules
8. Click Create Rule to display the Create Sender Rewriting Rule page.
9. In the Pattern to match field, enter a string using $+ to match a nonempty substring and $* to match an empty or nonempty substring. For example, $+.$+@company.com matches first.last@company.com.
10. Enter delimiting characters in the Characters delimiting a substring in the pattern field.
11. From the Action list, select Apply Rewrite to rewrite the address according to the rewrite string rule; Reject Address to reject the address, send a DSN to sender, and continue with next recipient; Discard Address to discard the address and continue with next recipient; or Stop to ignore subsequent rules.
12. In the Rewrite to Apply field, enter a string using $1, $2, and so on to substitute matching parts. For example, rewriting $+_+$+@company.com to $1.$2@company.com rewrites first_last@company.com to first.last@company.com.
13. Enter a description for the sender rewriting rule in the Description field.
14. Click OK to add the new rule to the list of sender rewriting rules and return to the Configure Routing Control: Outgoing Mail page.

Click Cancel to return to the Configure Routing Control: Outgoing Mail page.
15. Click Reorder to display the Reorder Sender Rewriting Rules page and change the order in which sender rewriting rules are applied.
16. Select the rule you want to move and use the arrows to move the rule toward the top or bottom of the list.
17. Click OK to apply any changes or Cancel to return to the Configure Routing Control: Outgoing Mail page.
18. To remove a sender rewriting rule from the list on the Configure Routing Control: Outgoing Mail page, select a rule and click Remove. A confirmation page displays.
To edit sender rewriting rule information, click the icon in the **Edit** column.

**Recipient Rewriting Rules**

20. Click **Create Rule** to display the Create Recipient Rewriting Rule page.

21. In the **Pattern to match** field, enter a string using $+ to match a non-empty substring and $* to match an empty or non-empty substring. For example, $+.+$@company.com matches first.last@company.com.

22. Enter delimiting characters in the **Characters delimiting a substring in the pattern** field.

23. From the **Action** list, select **Apply Rewrite** to rewrite the address according to the rewrite string rule; **Reject Address** to reject the address, send a DSN to sender, and continue with next recipient; **Discard Address** to discard address and continue with next recipient; or **Stop** to ignore subsequent rules.

24. In the **Rewrite to Apply** field, enter a string using $1, $2, and so on to substitute matching parts. For example, rewriting $+_.+$@company.com to $1.$2@company.com rewrites first_last@company.com to first.last@company.com.

25. Enter a description for the recipient rewriting rule in the **Description** field.

26. Click **OK** to add the new rule to the list of recipient rewriting rules and return to the Configure Routing Control: Outgoing Mail page.

Click **Cancel** to return to the Configure Routing Control: Outgoing Mail page.

27. Click **Reorder** to display the Reorder Recipient Rewriting Rules page and change the order in which recipient rewriting rules are applied.

28. Select the rule you want to move and use the arrows to move the rule toward the top or bottom of the list.

29. Click **OK** to apply any changes or **Cancel** to return to the Configure Routing Control: Outgoing Mail page.

30. To remove a recipient rewriting rule from the list on the Configure Routing Control: Outgoing Mail page, select a rule and click **Remove**. A confirmation page displays.

**Note:** The **Remove** button displays only when the Recipient Rewriting Rules list is populated.

31. To edit recipient rewriting rule information, click the icon in the **Edit** column.

**Saving and Copying Routing Control Settings for Outgoing Mail**

When finished with routing control, you must save the settings to apply them. You can also copy routing control settings to other servers.

To save routing control settings, click **Save Settings** on the Configure Routing Control Settings: Outgoing Mail page.
To copy the settings applied to this server to other available servers, click **Copy Settings**.

1. Select a server from the **Available Servers** list and move them to the **Selected Servers** using the buttons between the lists.
2. Click **OK** to return to the Configure Routing Control: Outgoing Mail page.

Click **Cancel** to return to the Configure Routing Control page.

**Configuring Routing Control for Incoming News**

Spam can be delivered through incoming news articles from newsgroups. Routing control settings can be configured to reject or trust incoming news according to various criteria, to secure incoming news from spammers.

There are three categories of routing control settings for incoming news, each accessible by a link on the Configuring Routing Control: Incoming News page:

- **General**: These settings enable DNS checks and establish limits on incoming articles to prevent flooding of the network.
- **Reject**: These settings specify which articles containing any of certain IP addresses, domains, or e-mail addresses are to be denied access to the system.
- **Trust**: These settings specify which articles containing any of certain IP addresses, domains, or e-mail addresses are to be granted access to the system.

To configure routing control for incoming news:

1. Open the Oracle WebMail client.

   **See Also:** "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client

2. Click the **Administration** tab.
3. Click the **Policy** subtab.
4. Click **Routing Control**.
5. Click **Incoming News** to configure routing control settings for incoming news.
6. Click the icon in the **Configure Routing Control** column to display the Configure Routing Control: Incoming News page.
7. Click the appropriate link to display a particular routing control settings page.

This section includes the following topics:

- **Configuring General Routing Control Settings for Incoming News**
- **Configuring Reject Routing Control Settings for Incoming News**
- **Configuring Trust Routing Control Settings for Incoming News**

**Configuring General Routing Control Settings for Incoming News**

To configure general routing control settings:

1. Click **General** on the Configure Routing Control: Incoming News page.
2. Ensure that **Enable Routing Control** is checked.
3. Select Enable from the **DNS check on client domain** list to check if the domain name exists on the DNS server. If it does not exist, the connection is rejected.

4. Select Enable from the **Match Authenticated Sender and From Message Header** list to compare the ID used to log in to the NNTP server to the **From** field in the message.

5. Enter the maximum number of newsgroup IDs that can be specified in an article in the **Maximum Number of Cross Posts Allowed** field.

**Denial of Service Attacks Section**

6. Enter a number in the **Maximum Flood Count** field that is the sum of the number of e-mail articles and the number of connection requests from this host within a time interval considered to be flooding, a characteristic of spam in which a sender sends a large amount of mail to one server in a short period of time.

7. Enter a number in the **Maximum Time Interval** field that is the number of seconds, used in conjunction with **Maximum Flood Count**, to determine whether a host is flooding the server with unwanted e-mail.

**Configuring Reject Routing Control Settings for Incoming News**

To configure the server to block rejected IP and e-mail addresses, and domains:


2. Ensure that **Enable Routing Control** is checked.

**Client IP Addresses Section**

Add, search for, remove, or edit rejected client IP addresses in this section.

To search the list of disallowed IP addresses, enter a string in the **Search** field and click **Go**.

3. Click **Add IP Address** to display the Add IP Addresses to Reject page.

4. Enter an IP address in the **IP Address** field.

   Click **Add Another Row** to enter additional IP addresses.

5. Click **OK** to add the IP addresses to the list of rejected IP addresses and to return to the Configure Routing Control: Incoming News page.

   Click **Cancel** to return to the Configure Routing Control: Incoming News page.

6. To remove an IP address from the rejected list on the Configure Routing Control: Incoming News page, select an IP address and click **Remove**. A confirmation page displays.

   **Note:** The **Remove** button displays only when the Client IP Addresses list is populated.

7. To edit IP address information, click the icon in the **Edit** column on the Configure Routing Control: Incoming News page. Edit the settings as necessary.

**Client Domains Section**

Add, search for, remove, or edit rejected client domains in this section.

To search the list of disallowed domains, enter a string in the **Search** field and click **Go**.
8. Click **Add Domain** to display the Add Client Domains to Reject page.

9. Enter a domain name in the **Domain** field.
   
   Click **Add Another Row** to enter additional domains.

10. Click **OK** to add the domains to the list of rejected client domains and to return to the Configure Routing Control: Incoming News page.
   
   Click **Cancel** to return to the Configure Routing Control: Incoming News page.

11. To remove a client domain from the rejected list on the Configure Routing Control: Incoming News page, select a domain and click **Remove**. A confirmation page displays.

    **Note:** The **Remove** button displays only when the Client Domains list is populated.

12. To edit client domain information, click the icon in the **Edit** column on the Configure Routing Control: Incoming News page. Edit the settings as necessary.

**Sender Domains Section**

Add, search for, remove, or edit rejected sender domains in this section.

To search the list of disallowed domains, enter a string in the **Search** field and click **Go**.

13. Click **Add Domain** to display the Add Sender Domains to Reject page.

14. Enter a domain name in the **Domain** field.
   
   Click **Add Another Row** to enter additional domains.

15. Click **OK** to add the domain to the list of rejected sender domains and to return to the Configure Routing Control: Incoming News page.
   
   Click **Cancel** to return to the Configure Routing Control: Incoming News page.

16. To remove a sender domain from the rejected list on the Configure Routing Control: Incoming News page, select a domain and click **Remove**. A confirmation page displays.

    **Note:** The **Remove** button displays only when the Sender Domains list is populated.

17. To edit sender domain information, click the icon in the **Edit** column on the Configure Routing Control: Incoming News page. Edit the settings as necessary.

**Sender E-mail Addresses Section**

Add, search for, remove, or edit rejected sender e-mail addresses in this section.

To search the list of disallowed sender e-mail addresses, enter a string in the **Search** field and click **Go**.

18. Click **Add E-mail Address** to display the Add Sender E-mail Addresses to Reject page.

19. Enter an e-mail address in the **E-mail Address** field.
   
   Click **Add Another Row** to enter additional e-mail addresses.
20. Click **OK** to add the addresses to the list of rejected sender e-mail addresses and to return to the Configure Routing Control: Incoming News page. Click **Cancel** to return to the Configure Routing Control: Incoming News page.

21. To remove a sender e-mail address from the rejected list on the Configure Routing Control: Incoming News page, select an e-mail address and click **Remove**. A confirmation page displays.

```
Note: The Remove button displays only when the Sender E-mail Addresses list is populated.
```

22. To edit sender e-mail address information, click the icon in the **Edit** column on the Configure Routing Control: Incoming News page. Edit the settings as necessary.

### Configuring Trust Routing Control Settings for Incoming News

To configure the server to accept trusted IP and e-mail addresses, and domains:

1. Click **Trust** on the Configure Routing Control: Incoming News page.
2. Ensure that **Enable Routing Control** is checked.

#### Client IP Addresses Section

Add, search for, remove, or edit trusted client IP addresses in this section.

To search the list of allowed IP addresses, enter a string in the **Search** field and click **Go**.

3. Click **Add IP Address** to display the Add Trusted IP Addresses page.
4. Enter an IP address in the **IP Address** field.
   - Click **Add Another Row** to enter additional IP addresses.
5. Click **OK** to add the IP addresses to the list of trusted IP addresses and to return to the Configure Routing Control: Incoming News page.
   - Click **Cancel** to return to the Configure Routing Control: Incoming News page.
6. To remove an IP address from the trusted list on the Configure Routing Control: Incoming News page, select an IP address and click **Remove**. A confirmation page displays.

```
Note: The Remove button displays only when the Client IP Addresses list is populated.
```

7. To edit IP address information, click the icon in the **Edit** column on the Configure Routing Control: Incoming News page. Edit the settings as necessary.

#### Client Domains Section

Add, search for, remove, or edit trusted client domains in this section.

To search the list of allowed domains, enter a string in the **Search** field and click **Go**.

8. Click **Add Domain** to display the Add Trusted Client Domains page.
9. Enter a domain name in the **Domain** field.
   - Click **Add Another Row** to enter additional domains.
10. Click OK to add the domains to the list of trusted client domains and to return to the Configure Routing Control: Incoming News page.

Click Cancel to return to the Configure Routing Control: Incoming News page.

11. To remove a client domain from the trusted list on the Configure Routing Control: Incoming News page, select a domain and click Remove. A confirmation page displays.

**Note:** The Remove button displays only when the Client Domains list is populated.

12. To edit client domain information, click the icon in the Edit column on the Configure Routing Control: Incoming News page. Edit the settings as necessary.

**Sender Domains Section**
Add, search for, remove, or edit trusted sender domains in this section.

To search the list of allowed domains, enter a string in the Search field and click Go.

13. Click Add Domain to display the Add Trusted Sender Domains page.

14. Enter a domain name in the Domain field.

   Click Add Another Row to enter additional domains.

15. Click OK to add the domains to the list of trusted sender domains and to return to the Configure Routing Control: Incoming News page.

   Click Cancel to return to the Configure Routing Control: Incoming News page.

16. To remove a sender domain from the trusted list on the Configure Routing Control: Incoming News page, select a domain and click Remove. A confirmation page displays.

   **Note:** The Remove button displays only when the Sender Domains list is populated.

17. To edit sender domain information, click the icon in the Edit column on the Configure Routing Control: Incoming News page. Edit the settings as necessary.

**Sender E-mail Addresses Section**
Add, search for, remove, or edit trusted sender e-mail addresses in this section.

To search the list of allowed sender e-mail addresses, enter a string in the Search field and click Go.

18. Click Add E-mail Address to display the Add Trusted Sender E-mail Addresses page.

19. Enter an e-mail address in the E-mail Address field.

   Click Add Another Row to enter additional e-mail addresses.

20. Click OK to add the addresses to the list of trusted sender e-mail addresses and to return to the Configure Routing Control: Incoming News page.

   Click Cancel to return to the Configure Routing Control: Incoming News page.
21. To remove a sender e-mail address from the trusted list on the Configure Routing Control: Incoming News page, select an e-mail address and click **Remove**. A confirmation page displays.

**Note:** The **Remove** button displays only when the Sender E-mail Addresses list is populated.

22. To edit sender e-mail address information, click the icon in the **Edit** column on the Configure Routing Control: Incoming News page. Edit the settings as necessary.

**Saving and Copying Routing Control Settings for Incoming News**

When finished with routing control, you must save the settings to apply them. You can also copy routing control settings to other servers.

To save routing control settings, click **Save Settings** on the Configure Routing Control Settings: Outgoing Mail page.

To copy the settings applied to this server to other available servers, click **Copy Settings**.

1. Select a server from the **Available Servers** list and move them to the **Selected Servers** using the buttons between the lists.
2. Click **OK** to return to the Configure Routing Control: Incoming News page. Click **Cancel** to return to the Configure Routing Control page.

**Oracle Mail Archive Policies**

Using the e-mail archive feature, you can establish a message archiving policy for every user. As the administrator, you can assign a policy individually to each user, that will copy all mail messages, both to and from that user, including envelope information for those messages, and mail the resultant information to a specified e-mail address.

To enable this feature, an administrator must perform the following tasks:

- Create one or more e-mail archiving policies. These policies define the destination address to which all archived messages are sent, and the format in which the information is sent.

  **See Also:** "Creating an Archive Policy" on page 8-27

- Associate these policies with Oracle Collaboration Suite users. For each user, there can be only one or no assigned policy. If a policy is assigned to a user, all mail to and from the user is archived based upon the parameters of that policy.

  **See Also:** "Associating Users with an Archive Policy" on page 8-28

- Use Oracle Enterprise Manager 10g Application Server Control Console for Collaboration Suite to enable the following:

  - The **Archive Processing** parameter in either the SMTP inbound, SMTP outbound, or List Server server instance (when enabled or disabled in any one of the preceding three servers, it forces archiving to be enabled on all instances of the other two server types as well).
This parameter determines whether the servers will check all messages for archive eligibility.

---

**Note:** This parameter must contain the same value for all the Applications tier to ensure that archive message processing is consistent.

---

- The **Archive Queue Process** parameter in the SMTP outbound target. This parameter enables the SMTP outbound server to generate and deliver archive messages.
- The **External Filter** parameter in the SMTP outbound target. This parameter must be enabled for the archiving feature to function.

This section includes the following topics:

- Creating an Archive Policy
- Editing an Archive Policy
- Associating Users with an Archive Policy
- Enabling Message Archiving

**Creating an Archive Policy**

To create an archive policy:

1. Open the Oracle WebMail client.

   **See Also:** "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client

2. Click the **Administration** tab.
3. Click the **Policy** subtab.
4. Click **Archive**.
5. Click **Add** to display the Add Archive Policy page.
6. Enter information into the following fields:

   - **Name**: Short unique name to define this policy. The text from this field is displayed in a list on the Add User and Modify User pages in Oracle WebMail to easily identify the policy for administrators.
     This information is required.
   - **Description**: Enter a description for the archive policy.
   - **Active**: Select to enable the archive policy.
   - **Additional Header**: Additional extended headers added to each archive message header. For example, `x-oracle-archive:Envelope version 1.0`.
   - **Archive SMTP Host**: The fully qualified name of the SMTP host to which you want to send all archive messages. This field is optional. If left blank, the archive journaling process will use the domain component of the e-mail
address entered in the To field to find the MX record for that domain and will mail the archive message to that e-mail address using standard Internet SMTP logic.

If you enter a host name in this field, it will act as an SMTP relay.

- Archive SMTP Port: The port number of the Archive SMTP Host.
- Archive E-mail Address: Enter a fully qualified e-mail address of the archiving facility in which all messages are to be archived.

This information is required.

- Archive Format: Select a supported archive format for the policy. The archive format determines how an e-mail message is packaged to include all its recipient information before being sent to the archive server. Different archive servers may support different formats. In Oracle Mail, currently only one format is supported: Basic Archiving Format.

7. Click OK to create the archive policy.

Click Cancel to return to the Archive page.

8. To remove an archive policy from the list on the Archive page, select an archive policy and click Remove. A confirmation page displays.

---

**Note:** The Remove button displays only when the archive policy list is populated.

---

**Editing an Archive Policy**

To edit an archive policy:

1. Open the Oracle WebMail client.

   **See Also:** "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client

2. Click the Administration tab.

3. Click the Policy subtab.

4. Click Archive.

5. In the Name column, click the archive policy that you want to edit.

6. Modify the policy attributes as necessary.

7. Click OK to apply the changes.

   Click Cancel to return to the Archive page.

---

**Associating Users with an Archive Policy**

Once archive policies are created, users are associated with a specific policy so that their messages will be archived.

Associating a user with a specific archive policy occurs when the new user is added to a particular domain. The domain has default new user settings that apply to the new user.
See Also: "Setting Default New User Attributes" on page 2-6 for more information about setting new user attributes.

An administrator can also associate a user with a particular archive policy using the ocsucr command-line utility.

---

Note: Associating users with an archive policy is optional. Unless an administrator sets default new users to be associated with a particular archive policy, default new users will not be associated with an archive policy, although individual users can later be associated with an archive policy.

---

### Enabling Message Archiving

For message archiving to occur, an instance of the SMTP outbound server must be configured to perform archive queue processing.

To enable message archiving:

1. Open the Application Server Control Console for Collaboration Suite.

   See Also: "Oracle Enterprise Manager 10g Application Server Control Console for Collaboration Suite" on page 1-3 for information about accessing the Application Server Control Console for Collaboration Suite.

2. Click the application server instance where Oracle Mail is installed.

3. Click Mail Application in the System Components section to display the Mail Application page.

4. Select the SMTP outbound server and click Stop to bring down the server.

5. Click SMTP Outbound Server to display the SMTP Outbound Server page.

6. Click Create to create a new instance.

7. Select Enable from the Archive Processing parameter list, located in the General Parameters section.

   Note: Enabling Archiving Processing from either the SMTP outbound, SMTP inbound, or List Server targets forces enabling of the parameter on the other two targets.

8. Select Enable from the Archive Queue Processing parameter list, located in the General Parameters section.

9. Click Apply.

10. Return to the Mail Application Service Targets page.

11. Select the SMTP outbound server and click Start to bring up the server.
Message Recall

**Message Recall**

**Note:** Recalling messages is an expensive operation because it involves searching the entire Oracle Collaboration Suite Database for the messages matching the search criteria. Therefore, the message recall operation will take a long time to complete.

Message recall enables administrators to locate messages in an Oracle Collaboration Suite 10g Database and move those messages to a specified folder for further analysis. Messages moved to the folder will no longer be accessible to users.

To enable the message recall feature:

1. Select the Oracle Collaboration Suite 10g Database in which you want to search for messages from the Oracle Collaboration Suite 10g Database list.

2. In the Message Recall Criteria section, select all or any of the following from the Matching list to specify that all, or any one of the filters listed in the table be applied.

   Messages matching these criteria are removed from the mailbox.

   If no filters are listed, add them, as follows:

   a. Click Add.

   b. Enter information for the following attributes:

      Select from the Message Attribute list upon which attribute of e-mail messages this filter will act. Attributes include: Subject, From, Sent Date, Attachment Name, and [Specify Header].

      Enter a string of text in the Value field to specify criteria upon which the filter will act.

**Note:**

- If you select the [Specify Header] message attribute, you must specify the header upon which the filter will act in the Header field.

- If you select the Sent Date message attribute, select from the Operator list either on, before, or since. Enter a date in the Value field in the form mm/dd/yyyy or click the calendar icon adjacent to the field to select a date.

For example, to filter messages from john@foo.com, select From from the Message Attribute list and enter john@foo.com in the Value field.

3. In the Specify e-mail address to store recalled messages field, enter the e-mail address of the account to where the recalled messages will be moved.

4. In the Specify folder to store recalled messages field, enter the name of the folder or subfolder to which the recalled messages will be moved.

   Use the form my_folder or my_folder/my_subfolder.
5. Click **Submit** to begin locating messages that satisfy the filter criteria and moving those messages to the special folder.
E-mail servers process and manage extremely large volumes of data because e-mail is typically used for simple collaboration and communication. Increasingly, it is also used for dynamic workflows. The power and simplicity of e-mail adds to its own problems. Employees typically manage many megabytes for stored e-mail, and process hundreds of messages in a typical day or week. With this growth in e-mail, levels of productivity suffer.

The rules engine within Oracle Mail can make the processing of e-mail information more efficient, improving employee productivity. Unlike some e-mail client-based rule technologies, server-side rules operate in the server—and, therefore, do not require a user to be connected to the network—and can be integrated more easily with back-end server processes or business logic. Client-side rules, common with many mail programs, are typically no more than filters for simple filing or deleting of messages based on recipient or subject string attributes. Because they are client-side, they limit users to a single interface—they might not apply, for example, when checking e-mail from an Internet terminal or wireless device. And of course, nothing happens if the user is not connected and logged in.

Whether the rule is a personal rule or a systemwide rule not visible to an end user, the properties of the rule (how it is stored and how it works) are the same. This chapter shows differences between rule types for their conditional processing and possible actions.

This chapter includes the following topics:

- What Is a Server-Side Rule?
- Managing Server-Side Rules
- Server-Side Rule Examples

### What Is a Server-Side Rule?

Rules allow the creation of conditional actions based on the properties of a message and its processing by the MTA. They can be as simple as a rule created by an end-user to move messages from a manager to a special folder, to more complex rules created by system administrators to perform secondary PL/SQL routines for every message passing through the MTA.

Before defining the components of a server-side rule, consider the typical life cycle of an e-mail message, as shown in Figure 9-1. First, consider an incoming message sent to the system. It will typically transition through four distinct states, or processes:

- **Arrival**: A message is transported to the system through a Transport Agent and placed in the System Inbox queue for processing (paths 4 and 5 in Figure 9-1).
What Is a Server-Side Rule?

- **Delivery**: The Delivery Agent processes queue is processed and the system places the message into a recipient’s Inbox (paths 6 and 7 in Figure 9–1).
- **Processed**: The message is in a user’s workspace and may be filed, copied, or tagged with status flags using the user’s e-mail client (path 8 in Figure 9–1).
- **Deleted**: The user deletes the message and the system removes all associated data (path 9 in Figure 9–1).

Outgoing messages are a simpler because sent messages pass through only two states:

- **Composed**: A user creates a message from the e-mail client, from which the message passes to some Transport Agent through the system Outbox or is placed in a queue for processing, when the message is sent.
- **Dispatched**: The system processes the recipient list for the message and delivers it to its destination.

Paths 1, 2, and 3 in Figure 9–1 are events in the life cycle of an outgoing message.

Each time a message changes from state to state, it can be identified as a specific event, and trigger the rules engine. Conditions and attributes of the messages can then be evaluated, and relevant actions taken. Since the rule is executed in the server, integration with other business logic, for example, is not dependent on a client connection. Rules processing is continuous, 24 hours a day.

**Figure 9–1  Life Cycle of an E-mail Message**

A server-side rule is a combination of three properties:

- An **event** that triggers the rule
- A **condition** (made up of an expression that resolves to true or false)
- An **action** that is performed if the condition is met

The events that trigger rule processing are defined internally within the Oracle Mail Server, and they define points in the life cycle of a message as it is processed through the MTA and managed in the Oracle Collaboration Suite Database.

**Events**

Events are instants in the life cycle of a message, defined points in the processing of a message, that enable the rules engine to perform condition testing when they occur. There are eight basic events where rules can be condition tested.
What Is a Server-Side Rule?

- **Relay**: When a message is transferred through the MTA to an external location.
- **Reception**: When a message is received by the SMTP inbound queue before the recipient names are resolved. This is triggered once for each message. This event can only be caught by a system wide rule. You cannot create a domain wide or user-level rule with this event because it is triggered before the name resolution.
- **Deliver**: When a message is delivered to a recipient’s Inbox, after name resolution. This event is triggered for every recipient of the message.
- **Flag change**: When the status of a message changes, such as from unread to read or to marked for deletion.
- **Copy**: When a message is copied to an IMAP folder. Copying to a local folder does not trigger any rule.
- **Move**: When a message moves to another IMAP folder. Moving a message to a local folder sets the deleted flag, meaning that the message is deleted from the IMAP server when the message moves to a local folder.
- **Expunge**: When messages are purged or folders are compacted from the client.
- **Expire**: A message is marked with an expiry date, and during the execution cycle of the Housekeeper server it is determined that this date has passed.

Notice that these events cover most of the significant stages in the normal life cycle of an e-mail message as it passes in or out of the system and Oracle Collaboration Suite Database. Some events are more applicable to the internal operation of the MTA (such as message relay), while others are more relevant to end-user e-mail management (such as message copy).

The remainder of this section describes how the context within which the rule is defined (whether it is system wide, or for an individual user) affects when the rule can be executed, and the actions it can perform. While there is no difference in the creation or operation of a rule as a result of which context it belongs to, there are some restrictions on the detailed rule definition. User-level rules, for example, cannot be used to check messages as they are relayed by the MTA.

There are three different contexts within which a rule may execute:

- **System wide**: For all messages in the system regardless of sender or recipient
- **Domain wide**: For all messages sent to or from one e-mail domain
- **User**: For all messages sent to a specific user. User-level rules typically are used to take actions based on end-user actions, such as message delivery and automatically filing messages.

It is important to note that not all events occur in every context. For example, **Relay** is a system event, not a user event. End users cannot create rules that check conditions when messages are relayed, just as they cannot normally view the internal queue status of the mail server in their everyday interaction with the mail system. Conversely, system and domain rules do not have permissions to perform actions that would normally be part of the end user’s interaction with the system, such as copying messages to subfolders of the mail account.

**Conditions**

A condition determines whether the action for the server-side rule is executed. Conditions can be compounded to support greater flexibility in the invocation of rule actions.

Typically, conditions fall into one of the following categories:
What Is a Server-Side Rule?

- Conditions built using the rule engine expression syntax of operators and attributes
- Custom PL/SQL functions loaded into the es_mail schema, that return a status of 0 (if the condition is true) or 1 (if the condition is not true)
- Conditions that perform message body searches

If no condition is present in a rule definition, the action is taken every time the event is triggered.

Expressions

An expression is the logic that determines whether the condition is true or false. It is defined by a special syntax of operators and attributes. If the result of the condition is true, the action is performed; otherwise, it is ignored.

The syntax of expressions includes operators such as `equal`, `contains`, and `istru`. Conditions can also be compounded with logical `and`, `or`, and negation, allowing great flexibility. When you create expressions, the rule engine exposes a number of message attributes that can be used to test the veracity of the condition. Most of these are taken from the message header (such as the sender or subject), or relate to particular attributes of the message (such as the `message_id`, character set, or a flag that is set).

Table 9–1 lists various server-side rule expressions.

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>equal</td>
<td>Numerical operator that tests whether an attribute is numerically equal to the operand</td>
</tr>
<tr>
<td>greaterthan</td>
<td>Numerical operator that tests whether an attribute is numerically greater than the operand</td>
</tr>
<tr>
<td>greaterequal</td>
<td>Numerical operator that tests whether an attribute is numerically greater than or equal to the operand</td>
</tr>
<tr>
<td>lessthan</td>
<td>Numerical operator that tests whether an attribute is numerically less than the operand</td>
</tr>
<tr>
<td>lessequal</td>
<td>Numerical operator that tests whether an attribute is numerically less than or equal to the operand</td>
</tr>
<tr>
<td>stringequal</td>
<td>String operator that tests whether a string attribute is the same as the operand</td>
</tr>
<tr>
<td>startswith</td>
<td>String operator that tests whether the operand is a prefix of the attribute</td>
</tr>
<tr>
<td>endswith</td>
<td>String operator that tests whether the operand is a suffix of the attribute</td>
</tr>
<tr>
<td>contains</td>
<td>String operator that tests whether the operand is a substring of the attribute</td>
</tr>
<tr>
<td>isnull</td>
<td>String operator that tests whether the attribute value is an empty string (NULL)</td>
</tr>
<tr>
<td>between</td>
<td>Range operator that requires two operands for lower limit and upper limit</td>
</tr>
<tr>
<td>in</td>
<td>Range operator that requires one or more operands to form a discrete list and test whether the attribute value is present in the list</td>
</tr>
<tr>
<td>istrue</td>
<td>Boolean operator that tests whether the attribute value is true or false</td>
</tr>
</tbody>
</table>
Attributes
Attributes are the set of variables available within the rules engine extracted from the message. They can be used in conditions and, in some cases, for dynamic substitution with rule actions. They loosely fall into two categories: information taken from the message header and status attributes of the message or the rule context, as defined in Table 9–2 and Table 9–3, respectively.

Table 9–2 Message Header Attributes
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rfc822From</td>
<td>Message from field</td>
</tr>
<tr>
<td>Rfc822to</td>
<td>Message to field</td>
</tr>
<tr>
<td>Rfc822CC</td>
<td>Message cc field</td>
</tr>
<tr>
<td>Rfc822Date</td>
<td>Message date field</td>
</tr>
<tr>
<td>Rfc822Subject</td>
<td>Message subject field</td>
</tr>
<tr>
<td>Rfc822ReplyTo</td>
<td>Message replyto field</td>
</tr>
<tr>
<td>Xheader</td>
<td>Custom extended header</td>
</tr>
<tr>
<td>Sender</td>
<td>Message sender field</td>
</tr>
<tr>
<td>Recipients</td>
<td>Expanded recipients</td>
</tr>
<tr>
<td>ReceivedDate</td>
<td>Internal received date</td>
</tr>
<tr>
<td>ContentType</td>
<td>MIME content-type from the first MIME body part header</td>
</tr>
<tr>
<td>CharSet</td>
<td>MIME charset header from the first MIME body part header</td>
</tr>
<tr>
<td>Xpriority</td>
<td>Message Xpriority field from the message header</td>
</tr>
<tr>
<td>Message_id</td>
<td>Unique identifier for a message</td>
</tr>
<tr>
<td>MessageType</td>
<td>Identifies messages as e-mail, voice mail, or fax</td>
</tr>
</tbody>
</table>

Table 9–3 Message Status Attributes
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MessageSize</td>
<td>Message size in bytes</td>
</tr>
<tr>
<td>Folder</td>
<td>Current folder in the processing context</td>
</tr>
<tr>
<td>Flag</td>
<td>Flag that changed during flagchange event</td>
</tr>
<tr>
<td>OverQuota</td>
<td>Whether the user account is over quota</td>
</tr>
<tr>
<td>RuleStatus</td>
<td>Return status of the previous rule</td>
</tr>
<tr>
<td>Sendhost</td>
<td>Internal</td>
</tr>
</tbody>
</table>

Actions
An action is the final stage of rule processing after an event and a condition are successfully matched. The product provides a standard set of mail operations, such as forward, copyto, and reject, and is also expandable to allow custom PL/SQL to be integrated as a site-specific rule action.

The possible actions are:
- forward: Forward the message to new recipients
- discard: Drop the message without delivery, without notifying the sender
What Is a Server-Side Rule?

- **bcc**: Send a blind copy to a defined recipient
- **pass**: Take no action
- **reject**: Reject the message, notifying the sender of a reason
- **moveto**: Move the message to a defined folder
- **copyto**: Copy the message to a defined folder
- **setprop**: Set a property value for the message
- **notify**: Send an additional message to some other destination notifying the recipient of this event
- **reply**: Send a reply message to the message sender
- **replyall**: Send a reply message to all original recipients
- **break**: Stop further rule processing
- **call**: Execute some external user-defined PL/SQL procedure

Because these actions differ in their functionality, each requires a different set of parameter values. For example, the `forward` action requires three parameters: a recipient list, a subject field, and a message body.

Table 9–4 lists each action and the associated parameters required by that action.

<table>
<thead>
<tr>
<th>Action</th>
<th>Parameter 1</th>
<th>Parameter 2</th>
<th>Parameter 3</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bcc</td>
<td>Bcc recipient</td>
<td>NA</td>
<td>NA</td>
<td>Bcc message to new recipient</td>
</tr>
<tr>
<td>break</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>Stops subsequent rule processing</td>
</tr>
<tr>
<td>call</td>
<td>Procedure name</td>
<td>User-defined</td>
<td>User-defined</td>
<td>Calls an external PL/SQL procedure (defined by user)</td>
</tr>
<tr>
<td>copyto</td>
<td>Folder name</td>
<td>NA</td>
<td>NA</td>
<td>Copies message to specified folder</td>
</tr>
<tr>
<td>discard</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>Silently discards message from system</td>
</tr>
<tr>
<td>forward</td>
<td>recipient</td>
<td>subject</td>
<td>message template</td>
<td>Forwards message to new recipient list using Parameter 2 for subject and Parameter 3 for the message body</td>
</tr>
<tr>
<td>moveto</td>
<td>Folder name</td>
<td>NA</td>
<td>NA</td>
<td>Moves message to specified folder</td>
</tr>
<tr>
<td>notify</td>
<td>Recipient</td>
<td>Subject</td>
<td>Message template</td>
<td>Notifies recipient in Parameter 1 of event that triggered the rule</td>
</tr>
<tr>
<td>pass</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>Messages proceed as though no rules have been invoked</td>
</tr>
<tr>
<td>reject</td>
<td>Reason string</td>
<td>NA</td>
<td>NA</td>
<td>Message is rejected, with DSN return to sender. This action can only be invoked under relay and reception events as system wide rules.</td>
</tr>
</tbody>
</table>
What Is a Server-Side Rule?

Not all actions are available in every context. For example, `reject` is an action of the SMTP process that is only available in the System context—an end user cannot tell the system to reject a message; `copyto` is an action within the user environment, not available to System and Domain rules.

For some actions, the parameters can include variable values generated at run time by the rules engine. For example, the `notify` action automatically sends an e-mail to the address specified in the rule. The third parameter to the `notify` action is a message template string that defines the message body of the notification. To extract values from the triggering e-mail, when this message is generated, enclose the attribute name with `%...%` delimiters. For example:

```xml
...<action>
  <command tag="notify" />
  <parameter>mailadmin@domain.com</parameter>
  <parameter>Notifying you of this event</parameter>
  <parameter>Message sent by %rfc822from%</parameter>
</action>
...
```

This action will notify `mailadmin@domain.com` when the rule condition is matched and generate a message body including the message’s sender.

The `call` is a special case action allowing a user-defined PL/SQL procedure to be executed. When defining this action, two user-defined parameters are passed to the PL/SQL package. The system also passes the event ID, mail session ID, and a mail message object to your procedure. Following is an example of the procedure:

```plsql
procedure myProc(p_eventid in integer, 
                p_sessionid in integer, 
                p_msgobj in mail_message_obj, 
```
The value of `p_status` should be set to 0 on successful completion, because this may influence subsequent rule events.

Managing Server-Side Rules

This section discusses managing server-side rules, including creation, editing, how rules are stored, and the order in which they are executed.

This section includes the following topics:

- Creating Server-Side Rules
- How Server-Side Rules Are Stored
- Order in Which Server-Side Rules Are Executed

Creating Server-Side Rules

There are two ways to create server-side rules: using the `oesrl` administrative command-line utility, or using an end-user e-mail interface. Only user-level rules can be created with an e-mail interface, but any kind of rule can be created with `oesrl`

The `oesrl` utility provides two input formats for rule creation: XML or a Java-style properties file.

This section includes the following topics:

- Displaying Existing Server-Side Rules with `oesrl`
- Creating Server-Side Rules with `oesrl`
- Editing Server-Side Rules
- Deleting Server-Side Rules
- Creating Server-Side Rules Using an E-mail Client

Displaying Existing Server-Side Rules with `oesrl`

Use the `-p` option with `oesrl` to display a set of server-side rules in the native XML format. This output format can be edited to modify or create new rules.

Examples

To list all the rules belonging to `user1@domain.com`:

```bash
$ oesrl -p user1@domain.com
```

To list all the rules applying to the `domain.com` domain:

```bash
$ oesrl -p domain.com
```

To list all the rules applying systemwide to all messages:

```bash
$ oesrl -p um_system
```
Creating Server-Side Rules with oesrl

Entering the command `oesrl -x filename` loads the server-side rules contained in the `filename` file. Rule syntax must be correctly provided, or `oesrl` will report an error. The format of the XML file used by `oesrl` includes two high-level sections:

- **account**: This section defines the qualified name of the rule owner, and the type of rule (system, domain, or user). For example, `<account qualifiedName="domain.com" ownerType="domain">`.
- **rulelist**: This section defines all the rules that apply for a given event. Within this XML tag, all attributes, conditions, and actions (Table 9–4) will be defined. For example, `<rulelist event="deliver">`.

In the `rulelist` section, server-side rules are defined with the `rule` tag. Each rule contains a condition to check, and an action to perform if the condition evaluates to true. Note that the condition is optional, so it is possible to perform the action for every message by simply omitting the condition clause. Following is a full example XML file that sends a BCC of the message to an administrator when mail is relayed to the `yahoo.com` domain:

```xml
<account qualifiedName="UM_SYSTEM" ownerType="system">
  <rulelist event="relay">
    <rule description="Rule" group="all" active="yes" visible="yes">
      <condition negation="no" junction="and">
        <attribute tag="rfc822to"/>
        <operator caseSensitive="no" op="contains"/>
        <operand>yahoo.com</operand>
      </condition>
      <action>
        <command tag="bcc" />
        <parameter>mailadmin@domain.com</parameter>
      </action>
    </rule>
  </rulelist>
</account>
```

Rules can be set as inactive without physically deleting them by setting `active="no"`. Also, if an administrator must force an end user to use a particular rule, it is possible to hide a rule from the Oracle WebMail client by setting `hidden="no"`.

**See Also:** "oesrl" on page D-24 for more examples of server-side rules

Editing Server-Side Rules

To edit existing rules, or add new rules from the command line, first print existing rules to a file, then edit that file with new rules or modifications. Then reload that file to overwrite the existing rule set.

**Note:** Supported e-mail clients can be used to edit user-created rules.

Deleting Server-Side Rules

Remove the `<rule></rule>` block from the XML file for each rule you want to delete.
Creating Server-Side Rules Using an E-mail Client

Only Oracle WebMail, Oracle Connector for Outlook, and Oracle Web Access Client can be used to create rules because server-side rule syntax is specific to Oracle Mail. These clients can be used to create and manage rules, though, as noted previously, only rules created by end users can be created this way.

How Server-Side Rules Are Stored

The server-side rule definition is stored internally within Oracle Internet Directory, and normally is not something that must be managed. All interaction with rules should be through the published interfaces. Within the LDAP directory information tree (DIT), rules are stored in their XML format alongside the corresponding directory element to which they apply. For example, user-created rules are stored in the Oracle Mail server container part of the DIT with the person to which that the rule belongs. Domain-level rules are a subentry of the e-mail domain, and system rules sit at the top level of the Oracle Mail DIT.

The following three examples show how each type of rule is stored in the DIT.

- System rule:

```plaintext
orclmailrulescope=System_Rule,cn=UM_SYSTEM,cn=EMailServerContainer,cn=Products,cn=OracleContext
```

- Domain rule:

```plaintext
orclmailrulescope=Domain_Rule,dc=oracle,dc=com,cn=UM_SYSTEM,cn=EMailServerContainer,cn=Products,cn=OracleContext
```

- User-created rule:

```plaintext
orclmailrulescope=User_Rule,mail=janed@domain.com,cn=Users,dc=domain,dc=com,cn=UM_SYSTEM,cn=EMailServerContainer,cn=Products,cn=OracleContext
```

**Note:** This DIT location is not formally a public interface and is subject to change in future releases of Oracle Mail. Additionally, dynamic PL/SQL is also created internally to the Oracle Collaboration Suite Database for each rule. It is important to always use published interfaces when modifying rules to ensure future compatibility and prevent corruption of the directory and database schema.

Order in Which Server-Side Rules Are Executed

Server-side rule execution is a simple sequence. The break action, if present, terminates further rule processing for this event. Apart from this limited control, it is not currently possible to execute certain rules based on previous rules, or execute in a different sequence based on a particular result. In summary, rules are executed:

- By context, in the following order:
  1. System
  2. Domain
  3. User
- Sequentially, as they are read from Oracle Internet Directory, in the current context

User-created rules execute in the order determined by the creator in the client.
Server-Side Rule Examples

See Also: "oesrl" on page D-24 for a list of examples of various server-side rules
This chapter describes how to back up and recover Oracle Mail. This chapter includes the following topics:

- Overview of Oracle Mail Backup and Recovery
- Backing Up and Recovering the Oracle Collaboration Suite Database
- Backing Up and Restoring User Data with oesbkp
- Recovering Messages with LogMiner
- Recovering Messages with Oracle Flashback Query

Overview of Oracle Mail Backup and Recovery

Disaster planning is a critically important aspect of administering an e-mail system. System files and the Oracle Collaboration Suite Database itself must be backed up regularly using the standard Oracle Database tools in order to be able to recover all or part of the e-mail system and data if a disaster occurs.

In addition to the standard database backup and recovery tools, the following processes and tools allow you to back up and recover data on a more granular level:

- The oesbkp utility backs up and recovers folders, messages, address book entries, and server-side rules for individual users
- LogMiner-based mail recovery recovers deleted messages using database redo logs
- Flashback query-based mail recovery recovers messages using Oracle Flashback Query

Backing Up and Recovering the Oracle Collaboration Suite Database

Oracle Mail uses Oracle Database 10g as its information storage database, so standard database backup and recovery methods can be used to maintain copies of the most current contents of the e-mail system. It is important to perform a full system backup at regularly scheduled times so that the entire Oracle Mail system can be restored to that snapshot if needed. Partial backups of the system can be performed between full backups so that the system can be recovered to a more recent point in time.

Oracle Collaboration Suite Database backup methods include:

- Export backup, which is appropriate for small Oracle Mail systems
Hot backup, which provides online backup and restore operations without shutting down the system

Cold backup, which requires shutting down the system

**Note:** Individual user accounts cannot be restored from database backups. To back up and restore individual user accounts, use the `oesbkp` utility, described in "Backing Up and Restoring User Data with oesbkp" on page 10-2.

### See Also:
- *Oracle Database Backup and Recovery Basics*
- *Oracle Database Backup and Recovery Advanced User's Guide*

## Backing Up and Restoring User Data with oesbkp

Individual e-mail users are categorized into two states:

- **Active:** Can access their mailboxes
- **Inactive:** Cannot access their mailboxes

Individual e-mail user accounts can be backed up and restored using the `oesbkp` command-line utility. `oesbkp` restores backed-up items at different levels of granularity. For example, you can restore either an entire user account or a single folder, which is particularly useful for backing up and restoring critical information.

**Note:** The backup and restore functionality cannot be applied to inactive users.

To back up inactive users, make them temporarily active, perform the backup, and return the users to their inactive status.

`oesbkp` backs up the following user data into flat files:

- Folders
- Messages
- Private address book entries
- Server-side rules

When restoring user accounts:

- All messages in the account are restored in a new folder to avoid overwriting existing messages
- Private address entries are restored in the user’s private address book, but entries that already exist are not restored
- A user’s restored server-side rules overwrite existing server-side rules

### Using oesbkp

The `oesbkp` syntax is as follows:

```bash
oesbkp task={backup | restore} user=userid@domain password=admin_password [type={all | mail | rules | addrbook}] [admindn=database_account_with_admin_...]
```
Table 10–1 lists oesbkp parameters and definitions.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Valid Values</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>task</td>
<td>(backup</td>
<td>restore)</td>
<td>None</td>
</tr>
<tr>
<td>user</td>
<td>Fully qualified user name</td>
<td>None</td>
<td>Fully qualified name, including the domain, of the user being backed up or restored. For example a valid value is <a href="mailto:user@domain.com">user@domain.com</a>, whereas user@domain and user are not valid values.</td>
</tr>
<tr>
<td>password</td>
<td>Any string</td>
<td>None</td>
<td>Password for the distinguished name (DN).</td>
</tr>
<tr>
<td>type</td>
<td>(all</td>
<td>mail</td>
<td>rules</td>
</tr>
<tr>
<td>admindn</td>
<td>Any valid DN for the LDAP server</td>
<td>cn=orcladmin</td>
<td>DN that the tool uses to bind to the LDAP server. The DN should have admin privileges, such as orcladmin and umadmin.</td>
</tr>
<tr>
<td>ldaphost</td>
<td>Any host name</td>
<td>localhost</td>
<td>Name of the host where Oracle Internet Directory is installed.</td>
</tr>
<tr>
<td>ldapport</td>
<td>Any integer</td>
<td>389</td>
<td>Port on which Oracle Internet Directory is listening.</td>
</tr>
<tr>
<td>backupdir</td>
<td>Any valid directory</td>
<td>user.dir</td>
<td>Location where the backup is being created or restored from.</td>
</tr>
<tr>
<td>folder</td>
<td>Any folder name</td>
<td>None</td>
<td>Name of the folder to be backed up or restored. If no value is specified, then all available folders are backed up or restored.</td>
</tr>
</tbody>
</table>

Note: When maintaining multiple backups for a particular user, ensure that each backup is named uniquely to avoid overwriting files.

Note the following information regarding oesbkp parameters:

- Parameter and value pairs must be specified with a blank space separating them on the oesbkp command line. Parameters can appear in any order.

- The following parameters are mandatory:
  - task
  - user
  - password

Logging information for oesbkp is stored in:

$ORACLE_HOME/oes/log/um_system/backup/number/text.log
The *number* variable is generated by the system and does not represent a process ID or other such number.

`oesbkp` creates the following backup files:

- The `user_rules.xml` file contains the specified user’s server-side rules.
- The `user_addrbook.ldif` file contains the specified user’s address book entries.
- The `user_foldermap` file contains mapping between the specified user’s files and folders, which enables the backup of folders that have names containing characters that are not supported by the operating system.
- The `user_n` (user_1, user_2, and so forth) file represents each of the user’s folders.

Folders are restored in subfolders in the following user account folder:

```
restore_dd-Mon-yyyy hh24:mi/subfolder_name
```

The `subfolder_name` variable has the same name as the original folder being restored, and `dd-Mon-yyyy hh24:mi` shows when the restore operation occurred (not when the backup operation occurred).

If a user is over quota when the backup is performed, the over-quota messages are also backed up. If a user’s folder is being restored and the messages in the folder cause the user to go over quota, the restore operation does not occur. Check the `oesbkp` log files to view the user’s current quota and usage, and if necessary, increase the user’s quota before restoring messages.

The following example shows how to create a full backup of all folders, messages, and private address book entries for `john@acme.com` in the `/bkp/allbkps` directory:

```
oesbkp task=backup type=all user=john@acme.com admindn=cn=orcladmin password=abcd ldaphost=ldap.acme.com ldapport=4032 backupdir=/bkp/allbkps
```

The folders created in the `/bkp/allbkps` directory are:

```
john@acme.com_rules.xml  john@acme.com_addrbook.ldif  john@acme.com_foldermap
john@acme.com_1  john@acme.com_2
```

The following example shows how to restore the messages to the inbox of `john@acme.com` from the backup stored in the `/bkp/allbkps` directory:

```
oesbkp task=restore type=mail user=john@acme.com password=abcd backupdir=/bkp/allbkps folder=inbox
```

In this example, if the restore operation is performed at 2:00 a.m. on January 17, 2006, the messages are restored to John’s account in a new folder named *inbox*, which is a subfolder of `restore_17-Jan-2006 02:00`.

---

**Recovering Messages with LogMiner**

Database *redo logs* record all changes made to data. If a failure prevents modified data from being permanently written to the data files, the changes can be obtained from the redo logs using the Oracle Database 10g LogMiner feature. With LogMiner, you can use SQL to read, analyze, and interpret log files.

Whenever an Oracle Mail message is deleted, the change in data is recorded in a database redo log. With LogMiner, you can retrieve deleted messages from the redo logs.
To fully translate the contents of redo logs, LogMiner requires access to a database dictionary. Without the database dictionary, LogMiner returns internal object identifiers and presents data in hexadecimal form. A LogMiner dictionary file contains information that identifies the database from which it was created and the time it was created. The data dictionary must be extracted prior to using LogMiner to recover Oracle Mail messages.

If you want to use LogMiner recovery, any and every Housekeeper process instance must have the **Support Log Miner Recovery** parameter enabled.

**See Also:** "Process Control Message Cleanup” on page 3-25 for information about setting up LogMiner to recover messages

**See Also:** The following documents for information about LogMiner:
- *Oracle Database Concepts*
- *Oracle Database Administrator's Guide*

### Recovering Messages with Oracle Flashback Query

This section contains the following topics:

- Using Oracle Flashback Query to Recover Messages
- MAIL_RECOVERY_FQ Package

### Using Oracle Flashback Query to Recover Messages

Oracle Mail users and administrators can recover messages deleted as of a certain time using the Oracle Flashback Query feature. The flashback query-based e-mail recovery applies to e-mail messages transferred to another folder. Oracle Flashback Query creates a snapshot of the database at a certain point in time, from which an Oracle Mail user can recover all messages that are in a particular folder at a specific point in time.

Oracle Flashback Query uses the retention control functionality provided by the Automatic Undo Management feature of the Oracle Collaboration Suite Database. The database maintains information that is used to roll back, or undo, changes to the database. Undo information consists of records of the actions of transactions, primarily before they are committed. Retention control enables you to specify the minimum period of time for which database undo information is saved before the space is overwritten by newer transactions.

When an Oracle Mail message is deleted, a record is created in the database undo logs. When Oracle Flashback Query retrieves the deleted message, the message is restored from the undo logs. The longer the undo information is retained, the older the deleted messages Oracle Mail users can retrieve using Oracle Flashback Query. A message can be recovered only if retention control is enabled and the message was deleted within the specified retention period.

The length of time for which database undo information is retained depends upon the amount of available disk space, the amount of e-mail traffic going through the Oracle Mail system, and the user activity on the system. The longer the undo information is retained or the heavier the activity on the e-mail system, the more disk space is required. An Oracle Mail system that receives a large number of messages each day requires more disk space to retain undo information than a system that receives just a few messages each day.
Deleted messages can be retrieved with Oracle Flashback Query using the Microsoft Outlook client connecting to Oracle Mail through Oracle Connector for Outlook. Recovered messages are recovered to the folder of the user’s choice. Flashback recovery by Oracle Mail through the Oracle Connector for Outlook can be enabled or disabled using the Oracle WebMail client administration pages.

See Also: Oracle Connector for Outlook Online Help for more information about recovering messages using Microsoft Outlook through the Outlook Connector.

Administrators can also use the PL/SQL package MAIL_RECOVERY_FQ to recover messages for a user using Oracle Flashback Query.

See Also: "MAIL_RECOVERY_FQ Package" on page 10-7

Recovered messages are included in quota calculations. If a user’s quota is exceeded during flashback recovery, no additional messages are recovered.

See Also: "A Word About Quota" on page 2-3 for more information about quota.

A message can be recovered even if it exists in a different folder. For example, if a message was moved from a user’s Inbox to FolderA and the user decided to recover the moved message into RecoverInbox, a pointer to the message would be created in RecoverInbox.

If a user tries to recover a message that already exists in the destination folder, the message retrieval fails. For example, if the message already exists in RecoverInbox and the user tries to recover that message into RecoverInbox, the recovery is not performed.

To set up Oracle Flashback Query:

1. Ensure that the Oracle Collaboration Suite Database is using an undo tablespace. By default, an undo tablespace is created during the installation of Oracle Collaboration Suite 10g.

2. Set the retention time:

   ALTER SYSTEM SET UNDO_RETENTION=time_in_seconds

   For example, to retain undo information for at least 3 hours, set the UNDO_RETENTION parameter as follows:

   ALTER SYSTEM SET UNDO_RETENTION=10800

   Note: The UNDO_RETENTION parameter can be set in the initialization parameter file.

3. Optional: To enable e-mail users to use the Oracle Flashback Query feature to recover deleted messages through the Microsoft Outlook client (this requires e-mail users to use Oracle Connector for Outlook):
Recovering Messages with Oracle Flashback Query

1. Open the Oracle WebMail client.

   **See Also:** "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client

2. Click the **Administration** tab. The **Domain** subtab displays by default.

3. Click **Domain Settings**.

4. Select an installation from the **Installation** list.

5. Select a domain from the **Domain** list.

6. Click **Submit**.

7. Select **enable** from the **Flashback Mail Recovery** list.

8. Click **Submit** to apply the changes.


   **See Also:** "Oracle Enterprise Manager 10g Application Server Control Console for Collaboration Suite" on page 1-3 for information about accessing the Application Server Control Console for Collaboration Suite

10. Click the application server instance where Oracle Mail is installed.

11. Click **Mail Application** in the **System Components** section to display the Mail Application page.

12. Select the IMAP Server process and click **Restart**.

**MAIL_RECOVERY_FQ Package**

The MAIL_RECOVERY_FQ package retrieves deleted messages from one or all of a user’s folders as of a specified point in time. The syntax is as follows:

```sql
mail_recovery_fq.get_recover_messages(
    p_usernameVARCHAR2,
    p_domainnameVARCHAR2,
    p_int_in_minsNUMBER,
    p_quotaNUMBER,
    p_fromfolderVARCHAR2,
    p_checksubfldrsNUMBER,
    p_tofolderVARCHAR2)
```

**Table 10–2** lists parameters and descriptions for the `get_recover_messages` procedure.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>p_username</td>
<td>User ID of the account from which to recover e-mail</td>
</tr>
<tr>
<td>p_domainname</td>
<td>Domain name of the user</td>
</tr>
<tr>
<td>p_int_in_min</td>
<td>Time, in minutes, to go back in the past to search for deleted e-mail</td>
</tr>
<tr>
<td>p_quota</td>
<td>If the value is 0, no quota check is performed</td>
</tr>
<tr>
<td></td>
<td>If the value is 1, a quota check is performed</td>
</tr>
</tbody>
</table>
To use the `mail_recovery_fq` package to recover messages:

1. Run SQL*Plus.
2. Connect to the database as `es_mail`.
3. Execute the `mail_recovery_fq.get_recover_messages` procedure.

    For example, run the following procedure to recover all deleted messages in the last 30 minutes for a specified user into a newly created folder, named `recovbox`, without performing any quota check.

    ```sql
    mail_recovery_fq.get_recover_messages('e-mailID_of_user_without_domain',
    'e-mail_domain_of_user', 30, 0, NULL, 0, recovbox);
    ```

### Table 10–2 (Cont.) `get_recover_messages` Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>p_fromfolder</code></td>
<td>If a value is specified, then only <code>p_fromfolder</code> is checked for deleted e-mail messages. If the value is null, then all of the user’s folders are checked for deleted e-mail messages.</td>
</tr>
<tr>
<td><code>p_checksubfldrs</code></td>
<td>If the value is 0, only <code>p_fromfolder</code> is checked for deleted e-mail messages. If the value is 1, all subfolders for <code>p_fromfolder</code> are checked for deleted e-mail messages.</td>
</tr>
<tr>
<td><code>p_tofolder</code></td>
<td>Destination of the retrieved messages. If the specified folder does not exist, the folder is created by the specified name for the deleted e-mail messages. If a folder is not specified, the system creates a folder named <code>RECMMSG_dd-Mon-yyyy hh24:mi</code> in which to store the deleted e-mail messages. The time stamp shows when the recovery occurred, not when the deletion occurred.</td>
</tr>
</tbody>
</table>
Troubleshooting Oracle Mail

This appendix outlines identification and resolution paths for issues affecting Oracle Mail. An assumption is made that, prior to any problems or issues and under similar load, the system behaved correctly, something changed, and now a problem has presented itself.

**See Also:** "Tuning Oracle Mail" in *Oracle Collaboration Suite Administrator’s Guide* for tuning due to an increased load

This appendix includes the following topics:

- Becoming Aware of a Problem
- End-User Issues
- Oracle Mail Application Problems
- Problems with Oracle Collaboration Suite Database
- Debugging Oracle Mail

**Becoming Aware of a Problem**

An administrator can be alerted to a problem through the following methods:

- Oracle Enterprise Manager 10g, including the Oracle Enterprise Manager 10g Grid Control Console and Oracle Enterprise Manager 10g Application Server Control Console for Collaboration Suite

  An administrator can be alerted to a problem by a metric or *beacon transaction* exceeding a threshold. This alert can come from any of the Oracle Mail metrics, delivery time, slow protocol transaction times, or if the availability drops below a defined level. An alert can be generated for any event that could degrade, or has substantially degraded, the quality of service.

  **See Also:** *Oracle Enterprise Manager Configuration for Oracle Collaboration Suite* for information about setting thresholds

- Help desk
  A user reports a complaint.

- Log files
  As an administrator, you can scripts and notification tools to periodically examine log files for errors. Viewing log files is the principal tool for identifying process-related issues. You can view the Oracle Mail-related logs within Oracle
Enterprise Manager 10g. Run the `esd_logscan.pl` script, located in the
$ORACLE_HOME/oes/admin directory, to search information in log files.

Process logs can be found in the $ORACLE_HOME/oes/log/server-type
directory. For example, List Server logs are found in the $ORACLE_
HOME/oes/log/list directory.

**See Also:** Appendix B, "Oracle Mail Error Messages" for a list of
error messages, possible causes, and actions to resolve the errors

- **Scripts and command-line tools**
  
  The `oesmon` command-line utility provides command-line access to near real-time
metric data in raw format. This metric data is sampled periodically by Oracle
Enterprise Manager 10g Grid Control and can be viewed in charted form using the
Oracle Enterprise Manager 10g Grid Control Console. The `oesmon` utility directly
contacts running servers and returns current values, whereas the Grid Control
Console charts typically sample at a rate of once every 10 minutes.

  **See Also:** Chapter 7, "Monitoring Oracle Mail" for more information
about `oesmon`

Oracle Mail also ships with various utility scripts located in the $ORACLE_
HOME/oes/admin directory to analyze a running system. These server diagnostic
scripts all have names starting with `esd_`. For example, the `esd_mail_
queue.sql` script can be used to monitor the activity of the mail queues and
check for messages stuck in the queues. Also, the `esd_logscan.pl` Perl script
can be used to search for errors in the log files and format the information so that
it is easier to read than the raw log file.

- **Others**

  Administrators doing spontaneous monitoring of the system, or other sources.

  - **CPU Usage**
    
    If a process is consuming an unusually large amount of resources, monitoring
the CPU usage will bring this process to the highest level. Use a system
monitoring tool such as `top` to view process CPU usage.

  - **Memory Usage**
    
    Excessive memory usage by a process will degrade the performance of all
system processes, in addition to the overall performance of the system. Use a
system monitoring tool such as `top` to view process memory usage.

  - **Disk Usage**
    
    Every transaction in the database is written to an archive log file that is sized
in advance by the database administrator. If the transactions can no longer be
written to file because of space constraints, the database will stop and all
end-user connections will end. Therefore, it is imperative that the
administrator monitor disk space capacity to insure that disk space is available
for continuous operation.

    Log file entries are continuously written to various file locations within the
Oracle Mail directory structure. These files can become quite large and can
cause some disruption if the directory gets full. Although the log files turn
over based on the size to which they are set, it is good practice to monitor the
disk to which log files are being written.
Use the command `df -k` to view the current and available disk usage.

**End-User Issues**

**Note:** This appendix only addresses issues that are specific to administrators. Troubleshooting and FAQs for end-users can be found at


End-user issues are commonly identified by a user contacting a Help desk. These issues range from login issues to simple functionality issues. They can be local to a single account or to a wider audience of users experiencing the same problem.

To evaluate a problem, first determine whether the problem is local to the account or systemwide.

This section includes the following topics:

- Problems with Mail Clients
- Problems with Mail Delivery
- Problems with a Single Message

**Problems with Mail Clients**

To best determine the nature of a mail client issue, it is important to understand which client the user is using. Some issues relate to one client but not the others. These issues may also not be a product of the client itself but rather of the back-end application. Determine the difference by the types of incidents that are reported.

This section addresses problems with the mail clients, including:

- User Unable to Log In to Account
- High Login Time Experienced
- It Takes a Long Time to Download a Mail Message
- Unable to Read a Particular Message
- During Peak Periods, Valid Users Receive Invalid Username and Password Error
- Cannot Send Mail
- Server Says Password is Incorrect but Password Has Not Changed
- It Takes a Long Time to Open the Inbox
- Oracle WebMail Client Issues

**User Unable to Log In to Account**

When a user connects to the Applications tier using any type of mail client, the first thing that occurs is connection establishment. For this to succeed, the Applications tier must be listening for and accepting connections. When the connection is established, the next step is authentication of the user. This requires access to the Oracle Internet Directory server. After the user is authenticated, the user's Inbox folder is retrieved, which requires access to the Oracle Collaboration Suite Database holding the user's
folders and messages. A problem encountered during any of these steps will prevent users from accessing their accounts.

Some of the common problems that prevent users from successfully logging in are:

- User password has expired
- IMAP or POP servers are not configured to connect to all Oracle Collaboration Suite Databases
- Servers have reached the maximum connections to the Oracle Collaboration Suite Database or Oracle Internet Directory

**Diagnosing Connection Establishment**

Issues with IMAP or POP client connection establishment can be diagnosed by using telnet to connect to the Applications tier, as follows:

```
telnet apptier.foo.com 143
```

In this example, `apptier.foo.com` is the Applications tier host computer and 143 is the IMAP protocol port. This should succeed and return a banner line which indicates that the server is ready. Enter `1 logout<ENTER>` to disconnect from the IMAP server and enter `quit<ENTER>` to disconnect from the POP server, where `<ENTER>` indicates pressing the Enter key.

If the attempt does not succeed, check the status of both the listener and the server. On the Applications tier host, use the commands `lsnrctl status listener_es` to display the status of the listener and `lsnrctl services listener_es` to display the services provided by the listener. Use the command `opmnctl status` to display the status of the Applications tier processes and verify that either the IMAP server or POP server is started.

**Diagnosing Oracle Internet Directory and Oracle Collaboration Suite Database Issues**

To see if there are issues with the Oracle Internet Directory server or the Oracle Collaboration Suite Database, check the IMAP or POP log files for errors. Specifically, ESCAPI-500 errors will be logged when a server runs out of either free Oracle Internet Directory or Oracle Collaboration Suite Database connections, or both, in the pools. Use `esd_logscan.pl` to search in the log files for ESCAPI-500 and also for ORA-XXXXX, which will be logged if there are database errors.

See Also: "esd_logscan.pl" on page D-46 for script usage information

The following section contains additional information about Oracle Internet Directory server diagnostics.

**High Login Time Experienced**

High login times can be experienced for the following reasons:

- This problem is most likely to occur due to slower response time from the Oracle Internet Directory server. The following Oracle Internet Directory administration tools can be used for the Oracle Internet Directory server.
  - `ldapbind` (found in the `$ORACLE_HOME/bin` directory): By entering the appropriate information, the `ldapbind` command determines whether you can authenticate a client to a server. If the connection is slow or fails to connect and all supplied parameters are correct, there may be an issue with either the
Oracle Internet Directory listener (oidmon) or its associated daemon (oidldapd).

Enter the following command with one or more of the options listed in Table A–1 to try to authenticate the client to the Oracle Internet Directory server:

$ ldapbind options

Table A–1  Options Used to Authenticate a Client to an Oracle Internet Directory Server

<table>
<thead>
<tr>
<th>Option</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>-D &quot;binddn&quot;</td>
<td>When authenticating to the directory, specifies doing so as the entry specified in binddn—that is, the DN of the user seeking authentication. Use this with the -w password option.</td>
</tr>
<tr>
<td>-w password</td>
<td>Provides the password required to connect (simple authentication)</td>
</tr>
<tr>
<td>-h ldaphost</td>
<td>Connects to ldaphost, rather than to the default host, that is, your local computer. ldaphost can be a computer name or an IP address.</td>
</tr>
<tr>
<td>-p ldappor</td>
<td>Connects to the directory on TCP port ldappor. If you do not specify this option, the tool connects to the default port (389).</td>
</tr>
<tr>
<td>-W wallet_location</td>
<td>Specifies wallet location required for one-way or two-way SSL connections. For example, on UNIX, you could set this parameter as follows: -W file:/home/my_dir/my_wallet. On Microsoft Windows, you could set this parameter as follows: -W file:C:\my_dir\my_wallet</td>
</tr>
<tr>
<td>-P wallet_password</td>
<td>Specifies the wallet password required for one-way or two-way SSL connections.</td>
</tr>
<tr>
<td>-U SSLAuth</td>
<td>Specifies SSL authentication mode:</td>
</tr>
<tr>
<td></td>
<td>1: No authentication required</td>
</tr>
<tr>
<td></td>
<td>2: One-way authentication required</td>
</tr>
<tr>
<td></td>
<td>3: Two-way authentication required</td>
</tr>
<tr>
<td>-E &quot;.character set&quot;</td>
<td>Specifies native character set encoding.</td>
</tr>
</tbody>
</table>

- ldapcheck (found in the $ORACLE_HOME/ldap/bin directory): This command performs a quick check of the necessary LDAP processes showing their existence (see following usage example). It displays the process name and its associated operating system process id (PID).

$ ldapcheck

Checking Oracle Internet Directory processes...

Process oidmon is Alive as PID 8158
Process oidldapd is Alive as PID 8196
Process oidldapd is Alive as PID 8186
Not Running ---- Process oidrepld

See Also: Appendix A, “Syntax for LDIF and Command-Line Tools” in Oracle Internet Directory Administrator’s Guide for more information about these utilities

Check that connections between IMAP and the Oracle Internet Directory server are not timing out or being dropped because of any network issues.
Check the CPU usage on Oracle Collaboration Suite Applications tier system. High usage can result in higher connection time. If the IMAP server is suddenly consuming more of the CPU resources, check the log level for the server. If there is a lot of information going to the log files, it can degrade server performance. Lower the log level to resolve this.

It Takes a Long Time to Download a Mail Message
The downloading of messages can be delayed for the following reasons:

- Message retrieval fetches a binary large object (BLOB) from `ES_BODY`.
  - If any of the fetches are slow, there will be latency in message retrieval
  - Consider running the Statspak and check on waits for these objects
- A particular user may report long download times if he is reading messages from a slower tertiary store.
- A message having too many MIME parts will also increase download time. Many clients typically issue a separate request for each MIME part, resulting in round-trips to the server.

Ensure that the maximum number of Oracle Collaboration Suite Database connections to the server has not been reached and confirm the network connectivity between the client and the IMAP server, and the server and the database.

Unable to Read a Particular Message
Try to read the problematic message using different e-mail clients. Not all clients can display all types of rich messages. If the message can be viewed with one of the clients, use that client to move the message to a separate folder. If the log files report errors in the fetching of the message, contact Oracle Support with details from the log file.

During Peak Periods, Valid Users Receive Invalid Username and Password Error
This problem typically occurs when the LDAP connection pool has been exceeded. If CPU resources are available, increase the LDAP connection pool size for the IMAP server.

Cannot Send Mail
Mail can be prevented from being sent for the following reasons:

- This can occur due to the server not being able to obtain a database session to insert messages into mail store, which can occur if the number of clients sending messages simultaneously exceeds the maximum sessions configured for the inbound server. This problem is usually temporary. Check the inbound logs for one of the following error messages to verify this:
  - Could not get OCI service ctx
  - Queueing the request returns=-110
  - Getting service context from pool failed

If this problem occurs frequently, evaluate your system to determine if it requires a change in the configuration.

- The problem could be attributed to a particular message. Check the log file to analyze the nature of the message and detect potential problems, such as mail
causing a routing loop, mail too big, mail loop due to too many mime levels, routing address loop, and invalid recipient.

- If the problem is persistent, and all required processes (listener, database, SMTP inbound, and Oracle Internet Directory) are up and running, contact Oracle Support with details of the logs.

Server Says Password is Incorrect but Password Has Not Changed

See Also: "User Unable to Log In to Account" on page A-3 for troubleshooting information

It Takes a Long Time to Open the Inbox

One Inbox query goes through the ES_INSTANCE table to gather all rows of a folder. As the size increases, the number of blocks retrieved increases.

Check the database statistics and if the preceding query is an expensive query, consider analyzing the ES_INSTANCE table.

Oracle WebMail Client Issues

Unlike other servers, Oracle Java Mail API (OJMA) is an application programming interface (API), a building block used when creating an application such as Oracle WebMail. The application using OJMA can be dependent upon many other components, such as Oracle HTTP Server, Oracle Application Server Single Sign-On, Oracle Internet Directory, OC4J, or Oracle Application Server Web Cache. This topic only addresses how to diagnose OJMA-related issues. Refer to the documentation for other components if they are suspected when troubleshooting an issue.

- **User reports long response times**: To determine if the response time is related to the application or OJMA, turn on OJMA tracing and monitor the time it takes to request a message from the database. If this time is unacceptable, examine the database for performance issues.

  For timing information, set the following property:

  ```
  oracle.mail.sdk.esmail.timing=true
  oracle.mail.sdk.esmail.db_timing=true
  ```

  The timing information is generated in the $ORACLE_HOME/opmn/logs directory in an Oracle WebMail/OC4J environment. Otherwise, the timing information is set to standard output.

- **User reports long authentication or open public and shared folder times**: Both of these operations are dependent on the performance of the Oracle Internet Directory server. Check the Oracle Internet Directory server for any problems.

Problems with Mail Delivery

End-user mail delivery issues can occur from both sending of e-mail and receipt of e-mail.

This section addresses problems with the mail delivery, including:

- **User Says Mail Delivery to Internet Addresses Does Not Occur**
- **User Did Not Receive a Mail Message That Was Certainly Sent**
- **User Does Not Receive Mail for 4 to 5 Minutes, but There Is Little Database Load**
- **User Receives Most Messages Quickly, but Some Are Delayed for Hours or Days**
■ Users say They Received Mail from a Distribution List, While Others Say They Have Not
■ Message Is Caught in a Mail Loop
■ Messages Are Being Rejected
■ Message delivery is slow

User Says Mail Delivery to Internet Addresses Does Not Occur
Check the SMTP inbound parameter settings. If the Inbound Rules and Routing Control Relay Allowed parameter is set to False (open relay disabled), ensure that the local domains are given in the Trusted Domains SMTP Inbound Rules and Routing Control parameter.

If the system allows local users to connect to SMTP through an Internet service provider (ISP) so that the connection comes from a foreign domain, set Relay Allowed to Authenticated and the SMTP Inbound General Authentication parameter to either Optional or Mandatory.

See Also: "Oracle Mail SMTP Inbound Server" on page F-34 for definitions of these parameters

User Did Not Receive a Mail Message That Was Certainly Sent
Usually, a delivery status notification (DSN) will be sent back to the sender, indicating either a delay or a failure in the delivery. The only exception is when the user specifically requests not to send DSNs.

A DSN will also be sent to the postmaster with the delivery failure reason. To receive the DSN, enter a valid e-mail address in the Postmaster E-mail Address SMTP Inbound server parameter. Also ensure that the Postmaster DSNs SMTP Inbound server parameter is set to Failures or All.

See Also: "Oracle Mail SMTP Inbound Server" on page F-34 for definitions of these parameters

If delivery is delayed for any reason, the message will be present in the queue for up to 5 days (default queue timeout) and the reason for delivery failure will be stored in the Oracle Collaboration Suite Database. Use the esd_mail_queue.sql script to examine the Relay queue. This script will show the deferral reason stored in the Oracle Collaboration Suite Database.

See Also: "esd_mail_queue.sql" on page D-53 for script usage information

When the delivery fails with an irrecoverable error, both queue and recipient records will be cleaned by the Housekeeper server within a couple of hours, and there may not be any trace of it in the database. Log files will contain information showing why the message delivery failed, such as the following:

■ OCI_ERROR: ORA-20220: Folder locked
■ OCI_ERROR: ORA-20221: User locked
■ Local delivery failed for user
■ Failed to deliver to user inbox for local users
■ Delivery to user@foo.com failed with smtp_err=421 or
Connect failed: Connection refused for relay users

Use the `esd_find_message.sql` script to locate lost messages. This script searches the database for messages given various search criteria. Once the message is found and the message ID is known, use the `esd_show_message.sql` script to see if the message is stuck in any of the queues. This procedure should only be used as a last resort because the `esd_find_message.sql` is very expensive to run. It is better to directly examine the queues using the `esd_mail_queue.sql` script and visually inspect the generated report to see if there are any stuck messages addressed to the user.

See Also: “esd_find_message.sql” on page D-49, “esd_show_message.sql” on page D-50, and “esd_mail_queue.sql” on page D-53 for script usage information

When there is no trace of the message in the database, look for the message in the next possible hop to the destination. If the message is relayed to the Internet, there will be a log entry (at log level 16) in the log file.

It is possible that the user did not receive the message because the user was over quota for mail storage. Either have the user delete old e-mail or increase the user’s quota, if necessary. An administrator can check the amount of storage used by a single Oracle Mail account with the `esd_list_user_folders.sql` script. This script generates a report that lists all the user's folders and the size of each. The total space used is listed at the end of the report. Compare this value with the user’s quota. If the SMTP inbound server or SMTP outbound server or both servers are configured to log at the Notification level, they will log ESSM-203 messages when an e-mail message is processed for a user that is over quota.

See Also:
- "A Word About Quota" on page 2-3 for more information about quota
- "Modifying E-mail User Attributes" on page 2-4 for information about how to view a user’s quota attribute
- "esd_list_user_folders.sql" on page D-54 for script usage information

Check the local queue using the `esd_mail_queue.sql` script to see if e-mails are queued due to temporary problems. A message that has been in the local queue for only a short time is not generally a problem. The initial delivery attempt may have failed due to the user's Inbox folder being locked, which can occur when another process is delivering a message to the user's folder or when another server, such as IMAP, is accessing the Inbox.

See Also: “esd_mail_queue.sql” on page D-53 for script usage information

Delivery failure due to folder lock is a temporary problem that typically requires no action by the administrator. E-mail will be delivered shortly after the Inbox is unlocked by the process that currently has it locked. A message that has been in the local queue for a long time may be a more serious problem.

If the user's Inbox has somehow become permanently locked, contact Oracle Support for assistance in resolving the issue. A permanently locked Inbox may be the cause if many messages for the user are stuck in the local queue for an extended period of
time. The utllockt.sql database diagnostic script may be useful in diagnosing
database lock issues.

See Also: "utllockt.sql" on page D-57 for script usage information

User Does Not Receive Mail for 4 to 5 Minutes, but There Is Little Database Load

The most common reason for this is the MTA queue processor going to sleep when
there are no messages in the queue. The installation default is to have queue
processors sleep for 2 minutes, configured by the
orclMailSMTPQueuePollInterval setting.

Use the Oracle Internet Directory administration tool oidadmin to adjust this setting
to edit the information in the Oracle Internet Directory server. Using oidadmin,
navigate to the settings for the SMTP Outbound server and update the value. You can
decrease this interval to as little as 1 second, but keep in mind that very small values
will cause the SMTP servers to poll more frequently and will increase the load on the
Applications tier CPU and also on the Oracle Collaboration Suite Database.

See Also: Chapter 4, "Directory Administration Tools" in Oracle
Internet Directory Administrator’s Guide for information about how to
access oidadmin

User Receives Most Messages Quickly, but Some Are Delayed for Hours or Days

This can occur when the MTA gets terminated abruptly due to an internal error. When
this happens, a large number of messages can remain waiting to be requeued,
resulting in half an hour of recovery delay. A bad message in the queue could
potentially cause the MTA to go down every half an hour (or whenever it retries) and
that could cause long delays for other messages.

When the MTA goes down repeatedly, look for the oldest messages in the queue. This
can be determined based upon how frequently new log directory entries get created.
Under normal circumstances, messages must not be in the queue for more than an
hour.

If some messages get stuck for days, contact Oracle Support.

Users say They Received Mail from a Distribution List, While Others Say They Have
Not

Mail from distribution lists may be delivered to some members of the list but may not
be delivered to other members for the following reasons:

- If the log level is sufficiently high, check whether the name resolution is returning
  all the expected recipient addresses.

- Examine all the child messages created using the esd_find_message.sql script
  located in the $ORACLE_HOME/oes/admin directory for the delivery (1 child
  message is created for every 1000 recipients) and ensure that all the recipients are
  present, and then look for delivery errors, if any.

- The List Server may not be asking for DSNs in some cases. In that case, no failure
  notifications are sent back. Otherwise, a DSN is sent to the envelope's return path
  (es_envelope.mailfrom) and to the postmaster address.

- If the MTA goes down during the name resolution and delivery, this could also
  result in partial deliveries.

- Check the Oracle Internet Directory Query Entry Return Limit. This number
  should be at least equal to the size of the distribution list.
If the distribution list is very large, meaning the number of subscribers is large, it is possible that the List Server is still processing the list.

Check if any users have exceeded their quota and so have not yet received the mail from a distribution list.

Check if the users have suspended their subscription from the distribution list, in which case, resume their subscription.

Message Is Caught in a Mail Loop

A mail loop can be defined as a message that is being sent from one account to another and back again. One way this can happen is by having two separate accounts. For example, a user has a Yahoo e-mail account and a corporate e-mail account. The user goes on vacation. Before leaving, the user configures the Yahoo account to forward all messages to the corporate account. The user also sets a vacation automatic reply on the corporate account. When the corporate account receives the forwarded e-mail and sends back the automatic reply vacation message to the Yahoo account, which is set to automatically forward messages, the message cannot be delivered to either account and gets caught in a mail loop.

Mail loops result in a sudden increase in the number of messages coming into the system. The queues may start backing up as a result. Use the esd_mail_queue.sql script to get details of the messages in the queue.

After identifying a user with a mail loop, delete the rule using the oesrl utility and notify the user of the problem.

See Also: "oesrl" on page D-24 for information on how to delete a rule

See Also: Chapter 8, "Deploying Oracle Mail" in Oracle Collaboration Suite Deployment Guide if this level of load has not been encountered before either adding new processes, changing their parameters, or both

Note: When a server fails (crashes) it will be restarted by opmn. A line similar to the following is written to $ORACLE_HOME/opmn/logs/ipm.log:


Check the time stamps on these messages. If the time stamps are close together and if there are a lot of messages like this, the processes are frequently failing.

Messages Are Being Rejected

Causes for this problem include:

Antispam: Message is identified as spam
Antivirus: Attachment contains a known virus
Message Size: Message size meets or exceeds the maximum message size accepted
System rule or user rule criteria for rejection: MTA has evaluated rules stating that the message should be rejected if it meets certain criteria

Solutions include:

- Check the log files for entries showing that a message was rejected
- Check the message routing policy parameters in the Policy subtab of the Administration tab of the Oracle WebMail client and confirm the entries listed for rejection. If an entry matches a sender that should be allowed to send e-mail to this application, that entry should be removed or updated to allow the sender only.

  **See Also:** "Configuring Routing Control for Incoming Mail" on page 8-8 for more information about setting routing control policies

- Check the Maximum Message Size parameter on the SMTP inbound process
- Check system rules

**Message delivery is slow**

Causes for this problem include:

- Server is being spammed and there is a spike in the mail traffic
- Check the log files for frequent temporary failures and check if many log directories are getting created due to the server going down. Log files can show which message is getting processed when the server goes down. Moving problematic messages to a temporary queue will clear the requeued messages that were picked up before and could not be processed.
- Check for network contention or problems with the DNS server
- Check LDAP communication and Oracle Internet Directory for any performance problems
- Check for problems with insertion and any other performance issues with the Oracle Collaboration Suite Database

**Problems with a Single Message**

Often a single message can cause problems. This can be a message that is malformed or has a characteristic that is not acceptable, such as being in the form of spam or having a virus attachment to the message.

This section addresses problems with a single message, including:

- **Read E-mail Time Is Slow**
- **Misconfigured Rules Cause Mishandling of Messages**

**Read E-mail Time Is Slow**

  **See Also:** "It Takes a Long Time to Download a Mail Message" on page A-6 for more information
Misconfigured Rules Cause Mishandling of Messages

Check for specific rules. Rules are basically kept in two places: Oracle Internet Directory and in the user_source view on the Oracle Collaboration Suite Database associated with the user.

The Oracle Internet Directory information is stored in XML format and is what the user sees in Oracle Collaboration Suite. The user_source view contains the procedural information and is actually what is checked against when messages come through.

Example A–1 shows what a rule can look like in the directory and in the database.

Example A–1 Structure of a Rule

```
RGMUM1:UM903v2 % oesrl -p jane.doe@acme.com
<account qualifiedName="JANE.DOE@ACME.COM" ownerType="user" id="0">
<rulelist event="deliver">
<rule description="OEM Alerts US" groups="all" active="yes" visible="yes">
<condition negation="no" junction="or">
<condition negation="no" junction="and">
<attribute tag="rfc822to"/>
<operator caseSensitive="no" op="contains"/>
<operand>oemalerts_us@ACME.COM</operand></condition>
<action>
<command tag="moveto"/>
<parameter>/jane.doe/INBOX/oemalerts_us</parameter></action></rule>
```

The first rule states that if a message comes into the user’s inbox with the to string oemalerts_us@ACME.COM, move it to the oemalerts_us folder, which is a subfolder of the inbox.

Example A–2 shows how a rule appears in user_source.

Example A–2 Structure of a Rule in user_source View

```
SQL> select text from user_source where name like 'DELIVER_19225%';

TEXT
---------------------------------------------------------------------------------------------------------------------------------
PROCEDURE deliver_19225 AS
BEGIN
  IF ((UPPER(es_rule.rfc822to) LIKE '%$'|UPPER('oemalerts_us@ACME.COM')|'|'))
  THEN
    es_rule.moveto('/jane.doe/INBOX/oemalerts_us');
  END IF;
```
All rules in `user_source` have a name of `DELIVER_number`, where `number` is the user’s user ID (the same as the `folder_id` of the INBOX). When rules are created, they also trigger the creation of a procedure.

You can query against `user_source` to find other rules, such as ones that someone might have set up to delete messages or to send a blind copy (BCC) to an account.

**Oracle Mail Application Problems**

Any one of the Oracle Mail applications can experience problems due to physical or virtual areas of the installation that may require certain resources to be available. When these resources are depleted, an area of the application will be affected.

Mail protocols, mail queues, and housekeeping directly affect the operation of the Oracle Mail application.

This section includes the following topics:

- Problems with Mail Protocols
- Problems with the Mail Queues
- Problems with the Housekeeper Process

**Problems with Mail Protocols**

This section addresses problems with the IMAP, POP, SMTP, and NNTP protocols, including:

- Complete Failure of Protocol Servers
- Too Many IMAP/POP Database Connections
- Too Many SMTP Inbound Client Connect Rejections
- Connect Time to SMTP Server Is Long

**Complete Failure of Protocol Servers**

If the Oracle Mail protocol servers fail, try the following:

- If you can bind to a protocol server but cannot issue a successful command, check the log files for database-related problems.
- If you cannot bind to a protocol server, check to see if the listener is up.

  **See Also:**  "Checking the Health of the E-mail Protocol Server Listener" on page A-23 for instructions on checking the status of the listener

- If processes will not start using the Application Server Control Console for Collaboration Suite, and there is still no access, check the log files for possible issues.
- Ensure that the server parameters are configured correctly. Incorrect configuration can prevent the server from starting.

**Too Many IMAP/POP Database Connections**

If there are too many IMAP or POP database connections:

- Check for Oracle Collaboration Suite Database performance issues.
Check if one or more user folders are locked: Some transaction is holding a lock on `ES_FOLDER` or `ES_USER` records for one or more users. This causes the IMAP server to consume more and more database connections as the requesting clients time out a request and issue a similar request, which again causes the IMAP server to take more connections from the pool.

Use regular lock detection SQL scripts, such as `utllockt.sql` or Oracle Enterprise Manager 10g to detect this situation. `oesmon` output for the database connection dump (taken few minutes apart) will also show the same users still executing the same statements.

As a solution, end the session-holding lock and contact Oracle Support with all the information about the ended session.

**Too Many SMTP Inbound Client Connect Rejections**

Client connections can be rejected under a high load, typically due to the following:

- All available sessions have been consumed, so no database sessions are available to service client requests to send mail. This can be observed from the log message `Getting service context from pool failed`. Increasing the number of available sessions for the SMTP inbound server instance can reduce the number of rejections. However, this increase should not result in too many overall database sessions needed by different server instances running against the database.

- All threads up to the configured maximum have been consumed and new client requests result in failures. This can be observed from the log message `No worker available`. Increasing the maximum allowed threads will reduce client connect rejections. Consider increasing this limit in increments of 100.

**Connect Time to SMTP Server Is Long**

If it is taking a long time to connect to the SMTP server, the problem is most likely either that the network is slow or that the Oracle Collaboration Suite Applications tier protocol server is overloaded. Neither a database nor an Oracle Internet Directory connection is necessary for the initial greeting. If the Applications tier is not overloaded, begin to trace the network request to find the location of network congestion.

**Problems with the Mail Queues**

Messages that are accepted for delivery are placed in different queues based on the recipient list. The queues are defined as `local`, `relay`, `submit`, and `list`. Messages can become deferred or delayed, based on a problem that the message may be experiencing. These problems can be caused by network problems, system resource problems, or message content. However, an overabundance of messages can also delay e-mail delivery.

This section addresses problems with the mail queues, including:

- **Queues Are Building Up and Not Emptying**
- **Problems With the Local Queue**
- **Problems With the Relay Queue**
- **Problems With the Submit Queue**

**Queues Are Building Up and Not Emptying**

If mail queues are building up but not emptying, consider the following:
This is not unusual but should be evaluated.

- Consider increasing the number of SMTP inbound and outbound instances
- Consider increasing the number of pool connections to the LDAP and database servers

**See Also:** "Modifying Parameter Settings for a Specific Server Instance" on page 3-8 for information about editing SMTP server parameter settings

It is possible that a problematic bad message in the queue is causing the server to go down. Although very rare, this has been known to happen.

On UNIX systems, a symptom of this is core files in the log directories. A message that causes the mail servers to go down will do so repeatedly, because it is never removed from the queue. On UNIX systems, look for core files with the following command:

```
% find $ORACLE_HOME/oes/log/um_system/smtp* -name core
```

If core files are found, contact Oracle Support.

**Problems With the Local Queue**

The incoming message rate can be higher than that of the processing rate, which can result in Local queue growth. Monitor the Length of Local Queue metric of the Oracle Collaboration Suite Database target using the Grid Control Console. The `esd_mail_queue.sql` script can also be used to examine the current contents of the Local queue.

**See Also:** "esd_mail_queue.sql" on page D-53 for script usage information

If the count of messages in the Local queue continues to increase, you can infer that the system is not able to handle the incoming load.

Possible reasons for this are:

- Lack of system resources, slow Oracle Collaboration Suite Applications tier, slow database, or slow Oracle Internet Directory. SMTP and IMAP servers are known to spin in the past and consume all the CPU resources on the Applications tier.
- Large amount of incoming spam mail. This can be detected by looking at the sender's address in the `ES_ENVELOPE` table. If the envelope's `MAILFROM` is not like one of the local domains and not null (<>), it must be of external origin. Spam filters can be turned on to block those senders.

Run the `esd_queue_examine.sql` script located in the `$ORACLE_HOME/oes/admin` directory to determine if there is a large amount of spam in the incoming queue.

- Insufficient SMTP inbound and outbound instances. If the MTAs are processing at the expected rate and the queue is still growing, increase the number of MTAs.

If the count of messages with NULL `modified_date` is very low, delivery must be failing for some reason. SMTP inbound and outbound server log messages located in the `$ORACLE_HOME/oes/log/um_system/smtp_in` and `$ORACLE_HOME/oes/log/um_system/smtp_out` directories, respectively, should indicate what is happening.

Possible reasons for local mail delivery failure are:
Target database is down; log files will show ORA- XXXXX errors.

Oracle Internet Directory is down or name resolution is failing. The log files will indicate Oracle Internet Directory errors.

Folder locks are a rare occurrence, unless a large amount of mail is being delivered to a small number of users. Another possibility is that one of the user folders could have been locked by a nonexistent process or a session. This should only block mail for a single user, but could result in a lot of requeues.

**Problems With the Relay Queue**

Check for the following:

- **DNS problems**
  
  One of the most common problems is incorrect DNS setup or slow DNS servers. A failure in DNS lookup will result in relay failure. These errors can be seen in the SMTP outbound log located in the `$ORACLE_HOME/oes/log/um_system/smtp_out` directory.

- **Failure to connect to a foreign MTA**

  Causes for failure include:

  - The remote host is refusing the connection due to reverse DNS lookup failure or a spam check failure. If the relaying MTA is not one of the MX hosts of the domain and does not have a PTR record in the DNS, the foreign host might not allow the connection. Sometimes the relaying hosts can get blacklisted, denied connection, or both, if they are acting as open relays.

  - The relaying host is unable to make connections outside the Oracle Collaboration Suite installation due to firewall problems.

- **Mail locally relayed to one or more local Oracle Collaboration Suite Databases gets stuck**

  Common causes for this problem include:

  - One of the databases is down

  - One of the databases is not accepting mail fast enough

- **Mail loops caused by incorrect setup**

- **Messages bouncing between the Oracle Collaboration Suite and external agents, such as spam filters and virus scanners, due to incorrect address rewriting or setup.**

**Problems With the Submit Queue**

Check the following:

- Analyze the queue to check whether the backlog is submit, and the density of messages with similar subjects, senders, recipients, or domains within the queue using the `esd_queue_examine.sql` script.

  **See Also:** "esd_queue_examine.sql" on page D-49 for script usage information

- A large density of messages with similar subjects, senders, recipients, or domains usually occurs for one of two possible reasons: the system has been spammed with unwanted mail or there is a mail loop. Looking at the subject and headers is usually sufficient to distinguish between the two possibilities, if you need to look
further at the body of the message, you can use the `esd_show_message.sql` script.

First, look at the queue using the `esd_mail_queue.sql` script which lists all messages in the queue along with their message IDs. Find the ID of the message of interest. Then, use the `esd_show_message.sql` script to look at detailed information about that message.

**See Also:**  "esd_mail_queue.sql" on page D-53 and "esd_show_message.sql" on page D-50 for script usage information

### Problems with the Housekeeper Process

The Housekeeper is the daemon that cleans up unreferenced e-mail data, such as messages deleted by a user, queued messages already processed, and expired messages or folders with an expiration date.

The Housekeeper will perform the following tasks during its processing of the e-mail application:

---

**Note:** Not all of these events may apply and most are configurable.

---

**See Also:**  "Modifying Parameter Settings for a Specific Server Instance" on page 3-8 for information about editing Housekeeper server parameter settings

- Clean up expired regular messages
- Prune processed messages in queues
- Prune expunged messages
- Collect pruned messages
- Move messages to tertiary storage
- Text index synchronization
- Text index optimization

This section addresses problems with the Housekeeper, including:

- **Housekeeper Cannot Keep Up with Cleaning Up Old Mail**
- **Problems With the Collection Queue**
- **Problems With the Pruning Queue**

**Housekeeper Cannot Keep Up with Cleaning Up Old Mail**

If the Housekeeper cannot keep up with cleaning old mail:

- Determine which housekeeping tasks the system is running behind with. The possible areas include the pruning queue and the collection queue.
  - If the pruning queue is very large, consider increasing the **Concurrency Level** parameter on the Housekeeper server instance that performs the pruning task. In most cases, concurrency level of 4 to 6 would be more than adequate to handle a significant amount of backlog.
– If the collection queue is very large, consider increasing the **Concurrency Level** parameter on the Housekeeper server instance that performs the collection task.

If an instance is configured to perform both pruning and collection, the increased concurrency level will apply to both instances upon process refresh.

- Check if the **Frequency of Execution of Housekeeper Process** parameter is set unreasonably low. A frequency of every 60 or 120 minutes is recommended.

**See Also:** "Managing Oracle Mail Servers and Instances" on page 3-3 for instructions on modifying Housekeeper instances

### Problems With the Collection Queue

First, check whether the **Collection** parameter is configured on any Housekeeper instance.

If such an instance exists and the processes associated with the instance are running, the system may experience data inconsistencies or data corruptions. The next step is to check the Housekeeper log file on the Oracle Collaboration Suite Applications tier. If log file directories are getting created rapidly, it indicates that the server has failed. Locate the core dump (if present) and the log file content, and contact Oracle Support.

If this is not the case but there are ORA-XXXXX errors present in the log file, check the errors and see if the problem can be corrected. If not, contact Oracle Support.

If there are no errors reported in the log file but the log file grows at a very slow rate, consider increasing the **Concurrency Level** parameter on the instances with the **Collection** parameter enabled. Also check that **Log Miner Recovery** is disabled in the Housekeeper server configuration debug parameters. Enabling this parameter causes collection to slow down 300%. Therefore, if **Log Miner Recovery** is not going to be used in the system, it is recommended that this parameter be disabled.

Check whether Oracle Text is installed and configured correctly. If an installation does not use Oracle Text and it was not activated during installation, Oracle Mail might be adversely affected. Usually installation log files show whether Oracle Text index-related data is configured and created correctly. If not, the system is left with invalid Oracle Text indexes, which cause errors when the Housekeeper tries to delete entries from related tables. In that case, drop whichever index reported in the log file, if the system is not configured to enable text search in e-mail messages.

### Problems With the Pruning Queue

First, check whether the Housekeeper instances have the **Pruning** parameter enabled. If the Housekeeper instances are verified to be running correctly, monitor the length of the ES_QUEUE entries and see if they drop at a reasonable rate. Pruning causes the collection queue to grow. Do not be alarmed if you observe this behavior.

Next, check server log files on the back-end database $ORACLE_HOME to see if there are any errors reported. If core dumps are present, contact Oracle Support. Analyze and fix, if possible, any ORA-XXXXX errors found in the log file. Otherwise contact Oracle Support. ORA-XXXX errors occur very rarely in pruning logs.

### Problems with Oracle Collaboration Suite Database

The Oracle Collaboration Suite Database stores all of the e-mail messages, text indexing, and folders of every account that is authorized for access. After successful Oracle Internet Directory authentication, a user is passed to a single database connection to the database for message access. There is a possibility that access will fail
or be denied. This problem can be local to a single account or global to all accounts. By checking complaints from the user community, it should be easy to recognize a global problem.

This section includes the following topics:

- Oracle Collaboration Suite Database Connectivity Problems
- Oracle Collaboration Suite Database Performance Problems

Oracle Collaboration Suite Database Connectivity Problems

This section addresses connectivity problems with the Oracle Collaboration Suite Database.

Network Unavailable Causing Massive Problems

If the network suddenly goes offline, this can cause massive disruption to end-user connectivity, as well as e-mail process communication (in a distributed environment) and end-user communication, depending upon the severity of the outage.

It may be necessary to shut down the protocol processes until the network is stable. Once the network stabilizes, bring all processes back online.

Oracle Collaboration Suite Database Performance Problems

This section addresses performance problems with the Oracle Collaboration Suite Database, including:

- SQL*Net Service Is Unavailable
- Oracle Collaboration Suite Database Is Slow
- Archive Log File Directory Partition Is Full
- Oracle Mail Storage Tablespaces Are Full Due to Lack of Extents

SQL*Net Service Is Unavailable

SQL*Net is the protocol that enables access to the database. There is an instance of the SQL*Net listener on both the Infrastructure and Oracle Collaboration Suite Database tiers.

The following problems can occur if the SQL*Net listener is down:

- Users cannot connect to Oracle Internet Directory for authentication.
- When authenticated with Oracle Internet Directory, the user is passed to the storage database. If the SQL*Net listener is down, users cannot access the Oracle Collaboration Suite Database.

Check the listeners on both the Infrastructure and the Oracle Collaboration Suite Database locations by running the following commands:

- On each system where the database resides:
  
  ```sh
  $ lsnrctl status
  ```

- On the Applications tier system, if `ORACLE_HOME/network/admin/tnsnames.ora` is configured on the Applications tier to access the databases or, if not, on the Infrastructure and Oracle Collaboration Suite Database tiers:
  
  ```sh
  $ tnsping connect_string
  ```
Oracle Collaboration Suite Database Is Slow

The following symptoms could indicate a slow database:

- Slow response times for users opening folders, reading mail, and sending mail (not authenticating, only Oracle Internet Directory is contacted).

- Large number of database connections. If the database is slow to handle a request, the protocol servers can request a new database connection for the next unit of work that arrives. If the database is slow because of disk constraints, or some other hardware resource issue, increasing the database pool can make matters worse. The increased connections can tax a loaded database even further when a flood of new database requests comes in, each taking their own database and operating system memory. Whether the database is under stress can best be analyzed by a database administrator and through tools such as Statspack or Oracle Enterprise Manager 10g.

- The Housekeeper queues continue to grow and never catch up until a decrease in activity, such as over the weekend.

- Mail delivery slows down.

- Users see an unable to retrieve database connection error occasionally upon login. This causes the Applications tier to slow down if the maximum connection pool exceeds the available memory on the system.

Archive Log File Directory Partition Is Full

If archive logging is enabled, all of the transactions are saved to a file for recovery purposes.

**See Also:** "Oracle Mail Archive Policies" on page 8-26 for more information

To check the current space usage:

1. Change directory to the designated archive log directory or partition.
2. From the system command prompt, execute the following command to check the available space on the current disk drive:

   ```
   $ df -k
   ```

   A normal backup routine should be performed and confirmed. Afterwards, the files in the directory can be purged with the exception of the current log file.

   If this directory is not backed up and the directory partition reaches full capacity, then the database will literally stop until one of two things occurs to relieve the disk space:

   - Old archive files are moved off this partition to another partition
   - A backup is performed of the archive files to a storage medium for future recovery purposes

Oracle Mail Storage Tablespaces Are Full Due to Lack of Extents

If the Oracle Mail storage tablespaces run out of extents, e-mail delivery and end-user e-mail message commits fail. Check the database alert logs for any tablespace full errors.

**Table A–2** lists tablespaces upon which to focus an investigation should Oracle Mail tablespaces run out of extents.
To display a summary of available space of all tablespaces, execute the following SQL statement as `sys` or `system`:

```
SQL> select tablespace_name, sum(bytes) from dba_free_space group by tablespace_name order by sum(bytes);
```

The command returns the following:

<table>
<thead>
<tr>
<th>TABLESPACE_NAME</th>
<th>SUM(bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>XDB</td>
<td>262144</td>
</tr>
<tr>
<td>EXAMPLE</td>
<td>458752</td>
</tr>
<tr>
<td>USERS</td>
<td>983040</td>
</tr>
<tr>
<td>ESINFRQIDX</td>
<td>2490368</td>
</tr>
<tr>
<td>SYSTEM</td>
<td>3211264</td>
</tr>
<tr>
<td>ESSMLTBL</td>
<td>3407872</td>
</tr>
<tr>
<td>ESPERFTBL</td>
<td>5046272</td>
</tr>
<tr>
<td>ESFREQTBL</td>
<td>9568256</td>
</tr>
<tr>
<td>ESFREQIDX</td>
<td>9633792</td>
</tr>
<tr>
<td>ESNEWS</td>
<td>10223616</td>
</tr>
<tr>
<td>ESTERSTORE</td>
<td>10223616</td>
</tr>
<tr>
<td>ESBIGTBL</td>
<td>17039360</td>
</tr>
<tr>
<td>ESMRLMNR</td>
<td>52297728</td>
</tr>
<tr>
<td>……...</td>
<td></td>
</tr>
</tbody>
</table>

For each table within the tablespaces listed there is a `NEXT_EXTENT` column that has a particular size allocated, by default. As space decreases, the tablespace seeks more space to accommodate its `NEXT_EXTENT` setting. If there is not enough space, it fails to extend and the application begins to receive errors.

Solution: If space remaining is depleted, add another data file to the tablespace experiencing problems.

See Also: Oracle Database Administrator’s Guide for details about adding data files to the tablespace.
Debugging Oracle Mail

This section discusses various debugging strategies to aid in troubleshooting.

This section includes the following topics:

- Checking the Health of the E-mail Protocol Server Listener
- Checking Memory, PGA Memory, and Number of Processes Connecting from MTAs to an Oracle Collaboration Suite Database

Checking the Health of the E-mail Protocol Server Listener

The listener for Oracle Mail is called `listener_es`, by default. Execute the following command to check the listener status:

```
$ lsnrctl stat listener_es
```

**Example A–3** illustrates a typical return on the command.

**Example A–3  Status of Listener**

LSNRCTL for Linux: Version 9.0.1.4.0 - Production on 06-FEB-2004 11:23:32

Copyright (c) 1991, 2001, Oracle Corporation. All rights reserved.

Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=IPC)(KEY=UMREG)))

STATUS of the LISTENER
------------------------

<table>
<thead>
<tr>
<th>Alias</th>
<th>listener_es</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>TNSLSNR for Linux: Version 9.0.1.4.0 - Production</td>
</tr>
<tr>
<td>Start Date</td>
<td>17-DEC-2003 22:41:00</td>
</tr>
<tr>
<td>Uptime</td>
<td>50 days 12 hr. 42 min. 32 sec</td>
</tr>
<tr>
<td>Trace Level</td>
<td>off</td>
</tr>
<tr>
<td>Security</td>
<td>OFF</td>
</tr>
<tr>
<td>SNMP</td>
<td>OFF</td>
</tr>
<tr>
<td>Listener Parameter File</td>
<td>/u01/app/oracle/product/v2/network/admin/listener.ora</td>
</tr>
<tr>
<td>Listener Log File</td>
<td>/u01/app/oracle/product/v2/network/log/listener_es.log</td>
</tr>
</tbody>
</table>

Listening Endpoints Summary...

| (DESCRIPTION=(ADDRESS=(PROTOCOL=ipc)(KEY=UMREG))) |
| (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=rgmum9.us.oracle.com)(PORT=25))(PRESENTATION=ESSMI)) |
| (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=rgmum9.us.oracle.com))(PORT=143))(PRESENTATION=IMAP)) |
| (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=rgmum9.us.oracle.com))(PORT=110))(PRESENTATION=POP)) |
| (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=rgmum9.us.oracle.com)) |

Services Summary...

Service 'ESSMI' has 2 instance(s).
  Instance 'um_system', status READY, has 1 handler(s) for this service...
  Instance 'um_system', status READY, has 1 handler(s) for this service...
Service 'ESSMIAMOCS' has 2 instance(s).
  Instance 'um_system', status READY, has 1 handler(s) for this service...
  Instance 'um_system', status READY, has 1 handler(s) for this service...
Service 'IMAP' has 2 instance(s).
  Instance 'um_system', status READY, has 1 handler(s) for this service...
  Instance 'um_system', status READY, has 1 handler(s) for this service...

The command completed successfully.
Occasionally, memory usage must be checked in the Oracle Collaboration Suite Databases due to various issues with program global area (PGA) memory usage within the databases. First, check to see how many connections (and what type) are coming into the database.

Connect to the database as `es_diag` and run the `esd_show_sessions.sql` script.

To check PGA memory usage, use the following script:

```sql
set pages 9999
select s.sid, s.program, st.value from v$session s, v$sesstat st
where s.sid=st.sid and statistic#=20
  and s.program like 'es%' order by 3;
```

Output will return similar to the following:

```
303 esimapds@rgmum6 (TNS V1-V3)                          3339424
164 esimapds@rgmum13 (TNS V1-V3)                         3500144
285 esimapds@rgmum13 (TNS V1-V3)                         3735304
 82 esimapds@rgmum13 (TNS V1-V3)                         4394984
125 esls@rgmum2.us.oracle.com (TNS V1-V3)               7911248
```

The first column contains the SID and the program name; the second column contains the amount of memory consumed in bytes. In this example, there is a List Server instance from `rgmum2` using about 7.4 megabytes (MB) of PGA memory on this database instance. If you see processes consuming more than 5 or 6 MB, they should be investigated and bounced, if necessary.
This chapter explains how to interpret error messages and correct errors. It lists the error codes in numerical order, divided into the following groups:

- Overview of Oracle Mail Error Messages
- IMAP and POP Error Messages
- SMTP Error Messages
- Housekeeper Error Messages
- List Server Error Messages
- NNTP Error Messages
- Virus Scrubber Error Messages
- Oracle WebMail Error Messages

### Overview of Oracle Mail Error Messages

Oracle Mail error messages can appear in the user interface and in the administrative tools and process logs.

When a list of error messages, called an error stack, is displayed, the bottommost error in the stack is typically the cause of the error.

**Note:** The error stack can contain error messages from other Oracle products that Oracle Mail uses. When these additional errors appear, refer to the documentation for the given product.

### IMAP and POP Error Messages

Table B–1 describes the IMAP and POP error messages.
### Table B–1 IMAP and POP Error Messages

<table>
<thead>
<tr>
<th>Error Number and Message</th>
<th>Cause of the Error</th>
<th>Action to Resolve the Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>101, 0, Login failed</td>
<td>Invalid user name or password used for LOGIN command</td>
<td>- Check the user name and password and try again.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Ensure that server is configured for proper Oracle Collaboration Suite Database.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Can be a temporary error due to resource constraints.</td>
</tr>
<tr>
<td>102, 0, No of auth/login tries exceeded. Exiting</td>
<td>Used all your allowed login attempts</td>
<td>Check the user name and password; then retry in a new session.</td>
</tr>
<tr>
<td>103, 0, User logged out</td>
<td>IMAP/POP session ended either by LOGOUT/QUIT command or because of some other irrecoverable (fatal) server error, such as unable to read or write to client connection anymore</td>
<td>Session end by LOGOUT/QUIT command is normal. If you suspect an abnormal connection termination, check the server log file for other errors in this error chain.</td>
</tr>
<tr>
<td>105, 0, Authorization failed</td>
<td>Unsuccessful login attempt using authenticate command</td>
<td>Check the user credentials and try again.</td>
</tr>
<tr>
<td>106, 0, Could not retrieve folder id for folder=(sarg0). Error#(narg0)</td>
<td>Possibly a nonexistent folder name was used</td>
<td>Correct the folder name and try again. If the folder name is correct, check and resolve any other database errors in this error chain.</td>
</tr>
<tr>
<td>107, 0, Failed to get header info for folder=(sarg0) with fid=(narg1). Error#(narg0)</td>
<td>Could be due to an OCI error</td>
<td>Ensure all required packages are loaded in the database correctly. In particular, check if ES_FOLDER_API is loaded. Check and resolve any other database errors in this error chain.</td>
</tr>
<tr>
<td>108, 0, Failed to update folder=(sarg0) with fid=(narg1). Error#(narg0)</td>
<td>Could be due to an OCI error</td>
<td>Ensure all required packages are loaded in the database correctly. In particular, check if ES_FOLDER_API is loaded. Check and resolve any other database errors in this error chain.</td>
</tr>
<tr>
<td>109, 0, Failed to connect to database (sarg1). Error#(narg0)</td>
<td>Server unable to create OCI connection pool</td>
<td>Ensure the database is up and configured correctly in Oracle Internet Directory.</td>
</tr>
<tr>
<td>111, 0, Failed to get statement handle (narg1) with Error#(narg0)</td>
<td>Database-related error</td>
<td>Check for an OCI error in this error chain.</td>
</tr>
<tr>
<td>112, 0, Autologout: idle (narg0) minutes</td>
<td>Your session was idle for too long</td>
<td>Send noop or any other command before timeout.</td>
</tr>
<tr>
<td>113, 0, Out of free Memory. Requested (narg0) bytes.</td>
<td>No more free memory is available to the server</td>
<td>Reduce the load on the server by reducing any of following: maximum threads, maximum clients, OCI sessions, or Oracle Internet Directory connections. Ensure enough free memory is available for the server on your system.</td>
</tr>
<tr>
<td>114, 0, Module (sarg0): nesting level too deep, no stats</td>
<td>Internal error</td>
<td>Contact customer support.</td>
</tr>
<tr>
<td>117, 0, Failed to get body parts for messageID=(narg0)</td>
<td>Could be due to an OCI error</td>
<td>Check and resolve any other database errors in this error chain.</td>
</tr>
</tbody>
</table>
118, 0, Failed to get database session for db={sarg0}. Error#{narg0}
   No more free sessions are available in the OCI connection pool
   This error may be temporary, due to a spike in load. You may need to reevaluate your system to reduce the number of clients connecting to this database, increase the number of sessions in pool, or tune the system in general to get faster response.

119, 0, Failed to insert subscribed folder={sarg0}. Error#{narg0}
   Database error
   Check the OCI errors in this error chain.

120, 0, Failed to rename folder={sarg0})to {sarg1}. Error#{narg0}
   This error can occur for the following reasons:
   ■ Trying to rename a nonexistent folder.
   ■ The new name is already in use.
   ■ Rename is not allowed.
   Ensure that a folder with the old name exists and that the new name is not already in use or contains restricted characters. Check for any other database errors in this error chain.

121, 0, Failed to set SEEN flag for msgid={narg0} in fid={narg1}. Error#{narg2}
   Could be due to an OCI error
   Check and resolve any other database errors in this error chain.

122, 0, Failed to get shell for msgid={narg0}. Error#{narg1}
   Could be due to an OCI error
   Check and resolve any other database errors in this error chain.

123, 0, Failed to create hierarchical folders {sarg0}. Error#{narg0}
   This error can occur for the following reasons:
   ■ You cannot create INBOX in any case-insensitive form.
   ■ You may be trying to create a folder that already exists.
   Check the folder name you are trying to create. Also check for any OCI errors in this error chain.

124, 0, Failed to expunge {narg0} msgs from folder with fid={narg1}. Error#{narg2}
   Could be due to an OCI error
   Check and resolve any other database errors in this error chain.

125, 0, Bad flags list
   Syntax error in the flag list for the Store command
   Correct the syntax for the flag list.

126, 0, Failed to get folder Id for folder={sarg0}. Error#{narg0}
   This error can occur for the following reasons:
   ■ You may be looking for a nonexistent folder.
   ■ You may not have read permissions for a shared folder.
   Ensure you are looking for the right folder and its name is spelled correctly. If it is a shared folder, check its configuration and permissions in Oracle Internet Directory. Check and resolve any other database errors in this error chain.

127, 0, Failed to create shared folder={sarg0}. Error#{narg0},{sarg1}
   Database error
   Check and resolve database errors in this chain.
### Table B–2 SMTP Error Messages

<table>
<thead>
<tr>
<th>Error Number and Message</th>
<th>Cause of the Error</th>
<th>Action to Resolve the Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>100, 0, Memory allocation failed</td>
<td>The process is consuming too much memory.</td>
<td>Reduce the number of threads running and restart the process.</td>
</tr>
<tr>
<td>101, 0, Memory realloc failed</td>
<td>The process is consuming too much memory.</td>
<td>Reduce the number of threads running and restart the process.</td>
</tr>
<tr>
<td>103, 0, failed to create thread</td>
<td>There are too many threads in the process.</td>
<td>Reduce the number of threads and restart the server. If the problem persists, contact technical support.</td>
</tr>
<tr>
<td>175, 0, ESDSGetEntry failed (sarg0)</td>
<td>The Oracle Internet Directory server may be down.</td>
<td>Restart the Oracle Internet Directory server. If the problem still exists, contact technical support.</td>
</tr>
<tr>
<td>Error Number and Message</td>
<td>Cause of the Error</td>
<td>Action to Resolve the Error</td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>176, 0, ESDSGetEntry for entrytype failed (sarg0)</td>
<td>The Oracle Internet Directory server may be down.</td>
<td>Restart the Oracle Internet Directory server. If the problem still exists, contact technical support.</td>
</tr>
<tr>
<td>177, 0, ESDSGetAttribute failed for (sarg0)</td>
<td>The Oracle Internet Directory server may be down.</td>
<td>Restart the Oracle Internet Directory server. If the problem still exists, contact technical support.</td>
</tr>
<tr>
<td>200, 0, loop detected for the recipient: (sarg0)</td>
<td>The address resolution for the recipient resulted in a loop.</td>
<td>Ensure the data present in the Oracle Internet Directory server does not introduce any loops for the recipient. Check whether the auto forward attribute for the recipient introduces a chain ending with the original recipient.</td>
</tr>
<tr>
<td>201, 0, orclObjectId not populated in Oracle Internet Directory for user: (sarg0)</td>
<td>Mandatory attribute orclObjectId is missing in Oracle Internet Directory.</td>
<td>Populate correct value for the user in Oracle Internet Directory.</td>
</tr>
<tr>
<td>205, 0, failed to deliver to user inbox: (sarg0)</td>
<td>NA</td>
<td>Verify that ES_MESSAGE_API has been loaded.</td>
</tr>
<tr>
<td>208, 0, failed to index msg for user: (sarg0) index type: (sarg1)</td>
<td>NA</td>
<td>Verify that ES_OT_API has been loaded.</td>
</tr>
<tr>
<td>209, 0, message rejected by rules for user: (sarg0)</td>
<td>The user rule resulted in rejection of the message.</td>
<td>None</td>
</tr>
<tr>
<td>210, 0, message rejected by the recipient (sarg0) using replymode: reject</td>
<td>Automatic reject is set in the Oracle Internet Directory entry for the recipient.</td>
<td></td>
</tr>
<tr>
<td>212, 0, failed to delete local recipients</td>
<td>There may be OCI errors</td>
<td>Verify that ES_MESSAGE_API has been loaded.</td>
</tr>
<tr>
<td>213, 0, local delivery failed for user: (sarg0)</td>
<td></td>
<td>Check the log for exact reason for failure prior to this message, and see any correction for the user's setup is needed.</td>
</tr>
<tr>
<td>225, 0, failed to pickup unprocessed messages</td>
<td>Error in recovery processing</td>
<td>Verify that ES_QUEUE_API has been loaded.</td>
</tr>
<tr>
<td>226, 0, failed to requeue messages</td>
<td>Error in recovery processing</td>
<td>Verify that ES_QUEUE_API has been loaded.</td>
</tr>
<tr>
<td>243, 0, path for external filter process is NULL in Oracle Internet Directory</td>
<td></td>
<td>Populate external filter process with the path for the virus scanner executable if virus scanning is enabled.</td>
</tr>
<tr>
<td>302, 0, User (sarg0) logon failed. Oracle Internet Directory returns (narg0)</td>
<td>Unable to authenticate user in Oracle Internet Directory</td>
<td>Check user name and password to see if they are correct.</td>
</tr>
<tr>
<td>401, 0, Error (narg0): Unable to get msgid</td>
<td>Unable to get next message ID from database</td>
<td>Verify that the schema has been installed and that the package is valid.</td>
</tr>
</tbody>
</table>
Table B–2 (Cont.) SMTP Error Messages

<table>
<thead>
<tr>
<th>Error Number and Message</th>
<th>Cause of the Error</th>
<th>Action to Resolve the Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>402, 0, Error {narg0}</td>
<td>Unable to insert envelope information into database</td>
<td>Verify that the schema has been installed and that the package is valid.</td>
</tr>
<tr>
<td>403, 0, Error {narg0}</td>
<td>Unable to insert recipient information into database</td>
<td>Verify that the schema has been installed and that the package is valid.</td>
</tr>
<tr>
<td>404, 0, Error {narg0}</td>
<td>Unable to insert the message into a queue</td>
<td>Verify that the schema has been installed and that the package is valid.</td>
</tr>
<tr>
<td>405, 0, Error {narg0}</td>
<td>Unable to insert message into database</td>
<td>Check the OCI error and the ORACLE error.</td>
</tr>
<tr>
<td>406, 0, Error: Routing loop detected</td>
<td>Message may be in a loop by checking the Received: headers. Possible causes:</td>
<td>Check the rewriting rules and automatic forwarding setup, and notify the sender.</td>
</tr>
<tr>
<td></td>
<td>▪ Loop in address rewriting rules</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ Automatic forwarding between addresses</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ Forward set up by UNIX mail senders</td>
<td></td>
</tr>
<tr>
<td>407, 0, Error: Unable to read from client</td>
<td>Unable to read from client</td>
<td>Check the network connections.</td>
</tr>
<tr>
<td>500, 0, spam check failed for IP address: {sarg0}</td>
<td>DNS server failed to verify that the IP address of the SMTP client is correct.</td>
<td></td>
</tr>
<tr>
<td>501, 0, spam check failed for host: {sarg0}</td>
<td>DNS server failed to verify that the host is a valid Internet host.</td>
<td></td>
</tr>
<tr>
<td>502, 0, spam check failed for sender: {sarg0}</td>
<td>The sender is either in the list of rejected senders or in the list of rejected domains.</td>
<td></td>
</tr>
<tr>
<td>503, 0, spam check failed for recipient: {sarg0}</td>
<td>This error can occur for the following reasons:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ Relay is not allowed for the non local recipient's domain.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ The local recipient is in the list of rejected recipients.</td>
<td></td>
</tr>
<tr>
<td>650, 0, failed to get submit recipients</td>
<td>Could be due to OCI errors</td>
<td></td>
</tr>
<tr>
<td>651, 0, failed to delete submit recipients</td>
<td>Could be due to OCI errors</td>
<td>Verify that ES_MESSAGE_API has been loaded.</td>
</tr>
<tr>
<td>652, 0, failed to insert resolved recipients</td>
<td>Could be due to OCI errors</td>
<td>Verify that ES_MESSAGE_API has been loaded.</td>
</tr>
</tbody>
</table>

Table B–3 describes the Housekeeper error messages.
### Table B–3  Housekeeper Error Messages

<table>
<thead>
<tr>
<th>Error Number and Message</th>
<th>Cause of the Error</th>
<th>Action to Resolve the Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle error (sarg0) occurred during expiration</td>
<td>An RDBMS error prevented Housekeeper from successfully performing expiration.</td>
<td>Correct the generic RDBMS error and try running the Housekeeper again.</td>
</tr>
<tr>
<td>Oracle error (sarg0) occurred during queue pruning</td>
<td>An RDBMS error prevented Housekeeper from successfully performing pruning.</td>
<td>Correct the generic RDBMS error and try running the Housekeeper again.</td>
</tr>
<tr>
<td>Oracle error (sarg0) occurred during pruning</td>
<td>An RDBMS error prevented Housekeeper from successfully performing pruning.</td>
<td>Correct the generic RDBMS error and try running the Housekeeper again.</td>
</tr>
<tr>
<td>Oracle error (sarg0) occurred during collection</td>
<td>An RDBMS error prevented Housekeeper from successfully performing collection.</td>
<td>Correct the generic RDBMS error and try running the Housekeeper again.</td>
</tr>
<tr>
<td>Oracle error (sarg0) occurred during tertiary storing</td>
<td>An RDBMS error prevented Housekeeper from successfully performing tertiary storage.</td>
<td>Correct the generic RDBMS error and try running the Housekeeper again.</td>
</tr>
</tbody>
</table>

### List Server Error Messages

Table B–4 describes the List Server error messages.

### Table B–4  List Server Error Messages

<table>
<thead>
<tr>
<th>Error Number and Message</th>
<th>Cause of the Error</th>
<th>Action to Resolve the Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>Msg-id: 5002 (An error occurred while performing a database operation. Error= (sarg0))</td>
<td>The cause for this error is available in the error message.</td>
<td>Look at the oerr error for the error specified in the error message.</td>
</tr>
<tr>
<td>Msg-id: 5003 (Error occurred while connecting to the Oracle Internet Directory server on (sarg0)port (narg0)bind dn (sarg0))</td>
<td>The Oracle Internet Directory server is either ■ Down ■ Has stopped responding ■ Is listening on a different port</td>
<td>Restart the Oracle Internet Directory server if it is not running. Otherwise, restart the List Server and specify the correct host name and port number of the Oracle Internet Directory server.</td>
</tr>
<tr>
<td>Msg -id: 5004 (Error initializing process control)</td>
<td>Either the database or the Oracle Internet Directory server: ■ Is not running ■ Has stopped responding</td>
<td>Restart the database and Oracle Internet Directory server. If they are running, then restart the List Server.</td>
</tr>
<tr>
<td>Msg-id: 5021 (Error modifying user (sarg0) entry. Error = (narg0))</td>
<td>An Oracle Internet Directory error occurred while trying to process a command for the user.</td>
<td>Check whether if the user entry on the Oracle Internet Directory server is still valid.</td>
</tr>
<tr>
<td>Msg-id: 5031 (Failed to resolve message (narg0) for external list (sarg0). Error : (sarg1))</td>
<td>The cause for this error is available in the error message itself.</td>
<td></td>
</tr>
</tbody>
</table>
Table B–5 describes the NNTP error messages.

### NNTP Error Messages

**Table B–5  NNTP Error Messages**

<table>
<thead>
<tr>
<th>Error Number and Message</th>
<th>Cause of the Error</th>
<th>Action to Resolve the Error</th>
</tr>
</thead>
</table>
| 6000, 0, An error occurred while initializing the NNTP process. | This error can occur for the following reasons:  
- An error occurred while querying the directory server.  
- The server parameters had incorrect values. | Ensure that the directory server is running and all the server parameters have been set correctly. |
| 6001, 0, Unable to initialize directory services. Server DN (sarg0) | The directory server was not running or there was an error in the command-line parameters. | Check that the directory server is running and all command-line parameters have been specified correctly. |
| 6002, 0, Unable to initialize database services. Mail store (sarg0) | This error can occur for the following reasons:  
- The mail store database was down.  
- The listener was down. | Ensure that the database and the listener for the mail store to which the process is connected are running. |
| 6003, 0, Unable to allocate (narg0) bytes | The server could not obtain memory from the operating system. | Restart the server. If the problem persists, shut down other processes and also increase memory resources on the host computer. |
| 6004, 0, Database error (narg0): (sarg0) | This error can occur for the following reasons:  
- The mail store database was down.  
- The listener was down.  
Additional information is available in the error message. | Ensure that the database and the listener for the mail store to which the process is connected are running. |
<table>
<thead>
<tr>
<th>Error Number and Message</th>
<th>Cause of the Error</th>
<th>Action to Resolve the Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>6005, 0, Directory service error (\text{sarg0}): (\text{narg0})</td>
<td>The directory server was not running. Additional information is available in the error message.</td>
<td>Ensure that the directory server is running.</td>
</tr>
</tbody>
</table>
| 7000, 0, Unable to initialize Oracle Net Services. Presentation name \(\text{sarg0}\). Listener port \(\text{narg0}\) | This error can occur for the following reasons:  
- The Oracle Net Listener is not running.  
- It is not configured correctly.  
- The server parameters do not match the listener configuration. | Ensure that the server parameters match the listener configuration and that the Oracle Net Listener is running. |
| 7001, 0, Unable to obtain connection pool to mail store \(\text{sarg0}\) | The server could not initialize connection to the mail store. | Ensure that the mail store database instance is running and accepting connections. |
| 7100, 0, Incompatible parameters specified: \(\text{sarg0}\) and \(\text{sarg1}\) | The parameters that have been specified are not compatible. | Consult the server documentation for more information about how to specify compatible parameters. |
| 7101, 0, Authentication failed for \(\text{sarg0}\) | The server received an authentication request with invalid credentials. | Verify if this is an authentication attempt by a genuine user. |
| 7102, 0, Too many authentication failures | The server detected three successive authentication failures from the same host and the connection was terminated | Verify that these are authentication attempts by genuine users. |
| 7103, 0, Connection rejected. Disallowed domain \(\text{sarg0}\) | The server received a connection from a domain that is not allowed. | If connections from this domain must be allowed, the antispam configuration must be edited to allow this domain. |
| 7104, 0, Connection rejected. Disallowed IP address \(\text{sarg0}\) | The server received a connection from a host that is not allowed. | If connections from this host must be allowed, the antispam configuration must be edited. |
| 7105, 0, A database operation resulted in an error. OCI Error \(\text{narg0}:\) \(\text{sarg0}\) | A mail store operation failed. | None |
| 7106, 0, Unable to obtain database handle to mail store \(\text{sarg0}\). Error \(\text{narg0}\) | The server is unable to open new connections to the mail store. | Check whether the mail store database instance is running and accepting connections. |
| 7108, 0, Message rejected. Virus scan failed. \(\text{Subject:}\) \(\text{sarg0}\) \(\text{(Message-ID:}\) \(\text{sarg1}\) | The virus scanner detected a virus in an incoming message. The message was not delivered. | None |
| 7110, 0, Operation \(\text{sarg0}\) not allowed for reader \(\text{sarg1}\) | The server received a feed-related request from a newsreader client. | Edit the server configuration if you want to make this host a peer. |
| 7111, 0, Parameter \(\text{sarg0}\) not specified. Using default \(\text{sarg1}\) | A required parameter was not specified. The default value was used instead. | The server configuration must be edited to specify a value for the parameter. |
### Table B–5  (Cont.) NNTP Error Messages

<table>
<thead>
<tr>
<th>Error Number and Message</th>
<th>Cause of the Error</th>
<th>Action to Resolve the Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>7112, 0, Parameter (sarg0) not set</td>
<td>A parameter value was not specified.</td>
<td>Edit the server configuration to set the parameter value.</td>
</tr>
<tr>
<td>7113, 0, No peers configured or unable to initialize all peers</td>
<td>The server instance is configured to allow feed. But no peer servers have been specified.</td>
<td>Edit the configuration to specify feed servers.</td>
</tr>
<tr>
<td>7114, 0, Instance identity initialization failed. Unable to determine host name</td>
<td>The server could not determine the name of the host on which it is running.</td>
<td>The name lookup service must be configured to return the host name.</td>
</tr>
<tr>
<td>7115, 0, Unable to locate peer entry: (sarg0)</td>
<td>A peer specified in the server configuration is invalid.</td>
<td>The peer configuration must be edited to specify valid peers.</td>
</tr>
<tr>
<td>7116, 0, Unable to initialize metrics collection</td>
<td>The metrics subsystem could not be initialized.</td>
<td>None</td>
</tr>
<tr>
<td>7117, 0, Unable to initialize new client connection</td>
<td>A new client request could not be accepted.</td>
<td>None</td>
</tr>
<tr>
<td>7118, 0, Invalid local group name: (sarg0)</td>
<td>The server detected an invalid group in the directory.</td>
<td>Remove the group and reconfigure.</td>
</tr>
<tr>
<td>7119, 0, Unable to initialize process control subsystem</td>
<td>Unknown</td>
<td>Check whether the administration store specified in the server configuration is the same as the Oracle Collaboration Suite Database.</td>
</tr>
<tr>
<td>8000, 0, An error occurred when starting a new thread.</td>
<td>The operating system limit for the maximum number of threads within a process was reached.</td>
<td>Increase the maximum limit on the number of threads, or reduce the value of the maximum number of threads parameter for the process.</td>
</tr>
<tr>
<td>8001, 0, An error occurred while establishing an NNTP connection with peer (sarg0).</td>
<td>No route could be established to the specified peer.</td>
<td>Ensure that the host name and port specified for the peer are valid, and the NNTP server on the peer is running.</td>
</tr>
<tr>
<td>8002, 0, An operating system error occurred in the system call (sarg0). Error (narg0)</td>
<td>An operating system error occurred in a system call.</td>
<td>Check the operating system error and fix accordingly.</td>
</tr>
<tr>
<td>8003, 0, Authentication to peer (sarg0) failed. Error (narg0)</td>
<td>The authentication information available in the peer entry was not accepted by the peer.</td>
<td>Ensure that the values specified for the user name and password in the peer entry are valid.</td>
</tr>
<tr>
<td>8100, 0, Failed to return connection to the peer connection cache: (sarg0)</td>
<td>Unknown</td>
<td>None</td>
</tr>
<tr>
<td>8101, 0, Failed to send an IHAVE command to peer (sarg0)</td>
<td>Article transmission to peer host failed.</td>
<td>Check that the peer is running and accepting articles.</td>
</tr>
<tr>
<td>8102, 0, Failed to read a response to the IHAVE command from peer (sarg0)</td>
<td>Article transmission to peer host failed.</td>
<td>Check that the peer host is active and accepting articles.</td>
</tr>
</tbody>
</table>
Table B–5  (Cont.) NNTP Error Messages

<table>
<thead>
<tr>
<th>Error Number and Message</th>
<th>Cause of the Error</th>
<th>Action to Resolve the Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>8103, 0, Failed to transmit article with (sarg0) to peer (sarg1)</td>
<td>Article transmission to peer failed.</td>
<td>Check that the peer is active and accepting articles.</td>
</tr>
<tr>
<td>8104, 0, An error occurred while establishing an NNTP connection with peer (sarg0)</td>
<td>Connection to peer host failed.</td>
<td>Check that the peer is active and accepting articles.</td>
</tr>
<tr>
<td>8105, 0, An operating system error occurred in the system call (sarg0). Error (narg0)</td>
<td>An error occurred in the operating system.</td>
<td>Check the server configuration and verify that the operating system has enough resources to support the server.</td>
</tr>
</tbody>
</table>

### Virus Scrubber Error Messages

Table B–6 describes the Virus Scrubber error messages.

Table B–6  Virus Scrubber Error Messages

<table>
<thead>
<tr>
<th>Error Number and Message</th>
<th>Cause of the Error</th>
<th>Action to Resolve the Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>10001, 0, Failed to create database connections, error=(narg0).</td>
<td>The server is unable to establish a database connection.</td>
<td>Check the generic Oracle error before this message for the exact cause.</td>
</tr>
<tr>
<td>10002, 0, Fatal database occurred.</td>
<td>An irrecoverable (fatal) Oracle error prevented the process from functioning.</td>
<td>Check the generic Oracle error before this message and correct the database problem if needed. The process restarts itself.</td>
</tr>
<tr>
<td>10007, 0, Failed to log on to the directory server, error=(narg0).</td>
<td>LDAP authentication failed for the server.</td>
<td>This error is rare. Contact Oracle Support for more information.</td>
</tr>
<tr>
<td>10008, 0, Warning: External virus software not configured, scanning disabled.</td>
<td>Server parameter orclMailScannerInterfaces parameter is not set correctly</td>
<td>Not an error. If the external virus scanner is not configured, the server does not perform virus scanning. If scanning is intended, set the parameter correctly and refresh the process.</td>
</tr>
</tbody>
</table>

### Oracle WebMail Error Messages

Table B–7 describes the Oracle WebMail error messages.

Table B–7  Oracle WebMail Error Messages

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Cause of the Error</th>
<th>Action to Handle the Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>An error occurred while adding attachments</td>
<td>Oracle WebMail was unable to add the attachments.</td>
<td>Try again.</td>
</tr>
<tr>
<td>No folder name was specified</td>
<td>The user did not specify a folder name.</td>
<td>Enter a folder name.</td>
</tr>
<tr>
<td>An error occurred; unable to create the new folder</td>
<td>Oracle WebMail was unable to create the folder.</td>
<td>Try again.</td>
</tr>
</tbody>
</table>
Table B–7 (Cont.) Oracle WebMail Error Messages

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Cause of the Error</th>
<th>Action to Handle the Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>A folder by that name &lt;foldername here&gt; already exists</td>
<td>The user specified a folder name that is being used by another folder.</td>
<td>Name the folder with a new name or put the folder in a different location.</td>
</tr>
<tr>
<td>An error occurred while creating the message</td>
<td>Oracle WebMail could not create a new message object.</td>
<td>Re-create the message.</td>
</tr>
<tr>
<td>No valid To: recipients found</td>
<td>User did not specify a valid e-mail address in the To field.</td>
<td>Specify a valid e-mail address.</td>
</tr>
<tr>
<td>Error occurred during message creation</td>
<td>Oracle WebMail could not create a new message object.</td>
<td>Re-create the message.</td>
</tr>
<tr>
<td>Invalid parameter specified for attachment removal</td>
<td>Oracle WebMail experienced a problem when removing the attachment.</td>
<td>Contact your system administrator.</td>
</tr>
<tr>
<td>Invalid attachment index was received</td>
<td>Oracle WebMail attachment indexes are misaligned.</td>
<td>Re-create the message.</td>
</tr>
<tr>
<td>No message IDs were specified for deletion</td>
<td>The user did not select messages for deletion.</td>
<td>Select the message for deletion.</td>
</tr>
<tr>
<td>An error occurred during message deletion</td>
<td>The message does not exist.</td>
<td>Contact your system administrator.</td>
</tr>
<tr>
<td>An error occurred while compacting the folder</td>
<td>This problem lies with the voice-mail messages in the folder.</td>
<td>Contact your system administrator.</td>
</tr>
<tr>
<td>No message IDs were specified for forwarding</td>
<td>The user did not select a message before selecting Forward.</td>
<td>Select a message before selecting Forward.</td>
</tr>
<tr>
<td>More than one message specified for forwarding</td>
<td>Multiple messages were selected for forwarding.</td>
<td>Select one message at a time for forwarding.</td>
</tr>
<tr>
<td>Invalid message specified</td>
<td>The message selected could not be forwarded.</td>
<td>Try selecting another message. If that does not work, contact your system administrator.</td>
</tr>
<tr>
<td>An error occurred while preparing the message for forwarding</td>
<td>The selected message could not be processed for forwarding.</td>
<td>Try again or contact your system administrator.</td>
</tr>
<tr>
<td>The destination folder does not exist</td>
<td>The destination folder selected does not exist.</td>
<td>Select another destination folder.</td>
</tr>
<tr>
<td>No message IDs were specified for move</td>
<td>The user did not select a message before selecting Move.</td>
<td>Select a message before selecting Move.</td>
</tr>
<tr>
<td>An error occurred while performing message move</td>
<td>Oracle WebMail could not process the move request.</td>
<td>Try again or contact your system administrator.</td>
</tr>
<tr>
<td>There are no more messages in this folder</td>
<td>No messages exist before or after the current message.</td>
<td>Try another folder.</td>
</tr>
<tr>
<td>An error occurred opening the next message</td>
<td>Oracle WebMail could not open the next message.</td>
<td>Try again or contact your system administrator.</td>
</tr>
<tr>
<td>There are no messages before this one in this folder</td>
<td>No messages exist before or after the current message.</td>
<td>Try another folder.</td>
</tr>
<tr>
<td>An error occurred opening the previous message</td>
<td>Oracle WebMail could not open the previous message.</td>
<td>Try again or contact your system administrator.</td>
</tr>
<tr>
<td>Unable to find folder</td>
<td>The folder is not accessible.</td>
<td>Check the shared permissions or contact your system administrator.</td>
</tr>
<tr>
<td>Error Message</td>
<td>Cause of the Error</td>
<td>Action to Handle the Error</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>--------------------------------------------------------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>Folder does not exist</td>
<td>There is no such folder in the account.</td>
<td>Contact your system administrator.</td>
</tr>
<tr>
<td>An error occurred while opening the folder</td>
<td>Oracle WebMail experienced problems opening the folder.</td>
<td>Contact your system administrator.</td>
</tr>
<tr>
<td>Error occurred during communication with the message store</td>
<td>Possibly a network problem.</td>
<td>Contact your system administrator.</td>
</tr>
<tr>
<td>No message ID specified</td>
<td>Internal error</td>
<td>Contact your system administrator.</td>
</tr>
<tr>
<td>Error retrieving message</td>
<td>The message may have been deleted, but the browser is looking at cached or old pages.</td>
<td>Refresh the message list and try again.</td>
</tr>
<tr>
<td>No message IDs were specified for reply</td>
<td>The user did not check any messages before selecting Reply.</td>
<td>Select a message before selecting Reply.</td>
</tr>
<tr>
<td>More than one message specified for reply</td>
<td>The user selected multiple messages for reply.</td>
<td>Select only one message at a time.</td>
</tr>
<tr>
<td>Invalid message specified</td>
<td>Oracle WebMail could not process the message for reply.</td>
<td>Try again or contact your system administrator.</td>
</tr>
<tr>
<td>Error occurred while preparing the message for reply</td>
<td>Internal error</td>
<td>Contact your system administrator.</td>
</tr>
<tr>
<td>Error while sending message</td>
<td>Internal error</td>
<td>Contact your system administrator.</td>
</tr>
<tr>
<td>No folder was specified for editing</td>
<td>The user did not select a folder in the folder list before selecting Edit.</td>
<td>Select a folder from the folder list.</td>
</tr>
<tr>
<td>The specified folder does not exist in the mail store</td>
<td>The folder selected is not available.</td>
<td>Verify that the folder exists, or contact your system administrator.</td>
</tr>
<tr>
<td>An error occurred while preparing the folder for editing</td>
<td>Internal Error</td>
<td>Contact your system administrator.</td>
</tr>
<tr>
<td>You cannot rename special system folders</td>
<td>The user tried to rename the inbox.</td>
<td>None. The inbox cannot be renamed.</td>
</tr>
<tr>
<td>No new name was specified</td>
<td>The user did not specify a name for the folder.</td>
<td>Specify a name for the folder.</td>
</tr>
<tr>
<td>A folder with that name already exists</td>
<td>Internal error</td>
<td>Contact your system administrator.</td>
</tr>
<tr>
<td>Unable to rename folder</td>
<td>Internal error</td>
<td>Contact your system administrator.</td>
</tr>
<tr>
<td>An error occurred while trying to update the folder</td>
<td>Internal error</td>
<td>Contact your system administrator.</td>
</tr>
<tr>
<td>Error while setting previous state</td>
<td>Internal error</td>
<td>Contact your system administrator.</td>
</tr>
<tr>
<td>You are no longer connected to the mail store</td>
<td>The session has timed out.</td>
<td>Contact your system administrator.</td>
</tr>
</tbody>
</table>
This appendix discusses Oracle Mail shared folders and includes the following topics:

- **Overview of Shared Folders**
- **Understanding Access Control Lists for Shared Folders**
- **Managing Public Folders**
- **Creating Public Folders**

**Overview of Shared Folders**

User folders can be shared with other users, distribution lists, or with everyone in a user’s domain using access control lists (ACLs). Oracle Mail supports ACLs defined in RFC 2086.

RFC 2086 defines the following namespaces:

- **Other users’ namespace**: A namespace that consists of mailboxes from the personal namespaces of other users.
- **Shared namespace**: A namespace that consists of mailboxes that are intended to be shared among users.

In Oracle Mail, folders within other users’ namespaces are referred to as shared folders, and folders within shared namespaces are referred to as public folders.

If a folder is shared with everyone in a domain, it is called a public folder. Otherwise, if the folder is shared with one or more users or distribution lists, it is called a shared folder.

For IMAP, Oracle Mail uses the following prefixes for shared and public folders:

- **#Shared/**: All shared folders accessible to the user appear under this namespace in the folder listing
- **#Public/**: All the public folders appear under this namespace in the folder listing

**Understanding Access Control Lists for Shared Folders**

Access control lists (ACLs) are used to share folders with other identifiers in the Oracle Mail system. Oracle Mail identifiers are listed in Table C–1.

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users</td>
<td>Users are explicitly granted permissions to a folder.</td>
</tr>
</tbody>
</table>
Folders cannot be shared across domains. To share folders within a domain, you must have either domain or system administrator privileges. Users can share the folders they own with other users within the domain.

Table C–2 lists domain rights that can be granted.

<table>
<thead>
<tr>
<th>Domain Right</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>l – lookup</td>
<td>Allows folders to be listed</td>
</tr>
<tr>
<td>r – read</td>
<td>Allows messages to be read from a folder</td>
</tr>
<tr>
<td>s – seen/unseen flag</td>
<td>Allows seen and unseen flag changes to be kept across sessions</td>
</tr>
<tr>
<td>w – write</td>
<td>Enables flags other than seen and delete to be stored</td>
</tr>
<tr>
<td>i – insert</td>
<td>Enables messages to be appended or copied into a folder</td>
</tr>
<tr>
<td>d – delete</td>
<td>Enables deleted flags for messages to be stored in a folder or expunge the folder</td>
</tr>
<tr>
<td>a – administer</td>
<td>Enables ACLs to be set and deleted on folders that are owned by other users</td>
</tr>
</tbody>
</table>

Oracle Mail always grants lookup rights with other rights. All rights are grouped with lookup privileges. None of the other rights are tied together.

The following rules apply to folders:

- Folders cannot be shared across domains
- Folder owners have all rights on their folders
- Only owners can rename or delete shared folders
- Subfolders under a shared folder do not inherit any rights
- It is possible for multiple identifiers in an ACL to apply to a given user. For example, an ACL can include rights that are granted to a domain and mailing list of which the user is a member. In such cases, a union of rights are granted to the user. If a user is given specific rights, then only those rights at the user level are applicable.

For example, consider a user who is a member of group G1 and list L1, which have been granted the following rights:

<table>
<thead>
<tr>
<th>identifier</th>
<th>rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>G1</td>
<td>li</td>
</tr>
<tr>
<td>L1</td>
<td>lrs</td>
</tr>
</tbody>
</table>

In this case the user’s rights are a union of li and lrs, or lrsi, as derived from membership in group G1 and list L1, respectively.
User-level rights take precedence over other rights. For example, if a user has \( 1r \) rights at the user level, then the applicable rights are \( 1r \).

**Managing Public Folders**

You must have system or domain privileges to create public folders. Public folders are first created in an administrator’s private namespace. To make the folders public, the administrator must give rights to the domain identifier.

Once a public folder is created, it can be administered by other administrators without specifying any rights. Public folders must be created with a unique name, because they do not have a user name prefix. For example, if administrator \( A1 \) creates a public folder called \( \text{public1} \), then administrator \( A2 \) cannot create a public folder with the same name.

Public folders count toward the owner’s e-mail quota.

Administrators can grant more rights to other identifiers. For example, a user can be granted \( \text{insert} \) rights to add messages to a public folder. This folder appears twice in the user’s folder listing: as a public folder and as a shared folder.

**Creating Public Folders**

Users with domain or system privileges can share a folder with an entire domain.

Sharing folders across an entire domain using an IMAP mail client is done through Oracle Connector for Outlook, as follows:

1. Create a new folder in the IMAP store and right-click it, or right-click an existing folder you want to share.
2. Click **Properties**.
3. Click the **Permissions** tab.
4. Click Add to grant permissions.
5. Enter anyone in the name resolution field.
6. Specify whatever rights you want on the Permissions page.
Many Oracle Mail tasks can be performed using the command line instead of the user interface. This appendix lists various command-line utilities, their usage, and examples.

This appendix discusses the following command-line utilities:

- oesdl
- oesng
- oespri
- oesucr
- oesctl and opmnctl
- oesrl
- oesmon
- oeschart
- oesbkp
- oeschk
- oesutil
- esd_logscan.pl
- esd_check_quota_usage.pl
- esd_queue_examine.sql
- esd_find_message.sql
- esd_show_message.sql
- esd_copy_messages.sql
- esd_mail_queue.sql
- esd_list_user_folders.sql
- esd_list_folder_messages.sql
- esd_list_unopened_inbox.sql
- esd_show_sessions.sql
- esd_show_session_usage.sql
- utllockt.sql
Use this utility to add users to and remove users from distribution lists.

The oesdl utility takes a file as input. The file should contain a list of records, each followed by an empty line. Each record must have the name of the distribution list and a list of its users.

Users can also be added to a distribution list that does not yet exist, by creating the distribution list in the same command that specifies its users.

To create a new distribution list, an owner must be specified.

**utilityUsage**

```bash
% oesdl file
```

In this command, `file` is the path to the file containing the distribution list records.

Additionally, to show all of the members of a particular distribution list, use the following command:

```bash
% oesdl -showallmembers list_name
```

For example, to show all the members of the `list1@us.foo.com`:

```bash
% oesdl -showallmembers list1@us.foo.com
```

The following is an output example:

```
Fetching members of list list1@us.foo.com
-------------------------------
user1@us.foo.com   Subscribed
user2@us.foo.com   Subscribed
user3@us.foo.com   Suspended
```

If the specified distribution list is inactive or not present, the following message displays:

```
No such list present list_name
```

If there are no members for the specified distribution list, the following message displays:

```
There are no members for the list list_name
```

<table>
<thead>
<tr>
<th>Table D-1 oesdl File Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Attribute</strong></td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>listname</td>
</tr>
<tr>
<td>action</td>
</tr>
<tr>
<td>newlist</td>
</tr>
<tr>
<td>type</td>
</tr>
<tr>
<td>owner</td>
</tr>
</tbody>
</table>
### Oracle Mail Command-Line Reference

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>usertype</td>
<td>The type of user being added.</td>
<td>U: regular user</td>
</tr>
<tr>
<td></td>
<td></td>
<td>F: foreign user</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L: distribution list</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A: alias</td>
</tr>
<tr>
<td>users</td>
<td>Comma-delimited list of users on which the action (add or delete) is to be performed.</td>
<td>Any valid e-mail address</td>
</tr>
<tr>
<td>orclmailgrouprfc2369suppresshdr</td>
<td>List the header types to be suppressed in messages distributed to the distribution list.</td>
<td>Any number of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>s: List-subscribe</td>
</tr>
<tr>
<td></td>
<td></td>
<td>u: List-unsubscribe</td>
</tr>
<tr>
<td></td>
<td></td>
<td>h: List-help</td>
</tr>
<tr>
<td></td>
<td></td>
<td>o: List-owner</td>
</tr>
<tr>
<td></td>
<td></td>
<td>p: List-post</td>
</tr>
<tr>
<td>orclmailgroupautoreconfmtext</td>
<td>Establishes the list of subscription approvers. Applicable only if the distribution list subscription type is restricted. Enter a comma-delimited list of users' e-mail addresses.</td>
<td>Any valid e-mail address</td>
</tr>
<tr>
<td>orclmailgroupeditorslist</td>
<td>Establishes the editors for the distribution list. Applicable only if the distribution list group type is edited. Enter a comma-delimited list of users' e-mail addresses.</td>
<td>Any valid e-mail address</td>
</tr>
<tr>
<td>orclmailgroupmoderatorslist</td>
<td>Establishes the moderators for the distribution list. Applicable only if the distribution list group type is moderated. Enter a comma-delimited list of users' e-mail addresses.</td>
<td>Any valid e-mail address</td>
</tr>
<tr>
<td>orclmailgroupallowdigest</td>
<td>Set to true to enable the digest feature. Posts to a distribution list are held and only one e-mail message is sent containing all the posts to the distribution list to a list member at a member-specified frequency.</td>
<td>true or false</td>
</tr>
<tr>
<td>orclmailgroupbounceproc</td>
<td>If true, when a DSN is received from any member of a distribution list a specific number of times, the list owner receives a notification and can then unsubscribe the member from the list.</td>
<td>true or false</td>
</tr>
<tr>
<td>orclmailgroupviewmembers</td>
<td>Specifies which type of user is allowed to view and edit distribution list members.</td>
<td>owner, privileged, member, all</td>
</tr>
<tr>
<td></td>
<td>owner: Only the distribution list owner can view and edit.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>privileged: Owners, approvers, moderators, and editors can view and edit.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>member: Members, owners, approvers, moderators, and editors can view and edit.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>all: Anyone can view and edit.</td>
<td></td>
</tr>
<tr>
<td>orclmailallowforeignmemb</td>
<td>Specifies whether foreign users can be members of this distribution list.</td>
<td>true or false</td>
</tr>
<tr>
<td>orclmailgroupnotifyoption</td>
<td>Specifies who receives notifications upon successful subscription or unsubscription.</td>
<td>none, owner, member, both</td>
</tr>
<tr>
<td></td>
<td>none: No one receives notifications.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>owner: Only the owner receives notifications.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>member: Only the member receives notifications.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>both: Both owner and member receive notifications.</td>
<td></td>
</tr>
</tbody>
</table>
Table D–1 (Cont.) oesdl File Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>orclmailuserstate</td>
<td>Specifies the state of the distribution list.</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td></td>
<td>inactive</td>
</tr>
<tr>
<td></td>
<td></td>
<td>migrating</td>
</tr>
<tr>
<td>orclmailgroupunsubscribea</td>
<td>If false, allows only the distribution list owner to unsubscribe a member</td>
<td>true or false</td>
</tr>
<tr>
<td>llowed</td>
<td>from a list. If true, anyone can unsubscribe.</td>
<td></td>
</tr>
<tr>
<td>orclmailgroupisexternal</td>
<td>Set to true if the members of the distribution list are resolved by an</td>
<td>true or false</td>
</tr>
<tr>
<td>name</td>
<td>external procedure.</td>
<td></td>
</tr>
<tr>
<td>orclmailgroupexternalproc</td>
<td>Must be provided if orclmailgroupisexternal is set to true. The name of the</td>
<td>Any valid SQL procedure</td>
</tr>
<tr>
<td>name</td>
<td>SQL procedure to be called, provided in the format schema_name.procedure_name@database_</td>
<td></td>
</tr>
<tr>
<td></td>
<td>link.</td>
<td></td>
</tr>
<tr>
<td>orclmailgroupposttype</td>
<td>Type of posting control placed on the list, as described in Table 2–3,</td>
<td>open or</td>
</tr>
<tr>
<td></td>
<td>&quot;Distribution List Posting Types&quot; on page 2-16.</td>
<td>subscriber</td>
</tr>
<tr>
<td>orclmailgroupmergetag</td>
<td>A tag used to specify mail merge and scheduler tags, enabling a distribution</td>
<td>A tag used to specify mail</td>
</tr>
<tr>
<td></td>
<td>list owner to support mail merge or scheduled mail delivery.</td>
<td>merge and scheduler tags,</td>
</tr>
<tr>
<td></td>
<td>See Also: &quot;Mail Merge&quot; on page 3-38 for more information about mail merge</td>
<td>enabling a distribution</td>
</tr>
<tr>
<td></td>
<td>and scheduled mail delivery.</td>
<td>list owner to support mail</td>
</tr>
<tr>
<td></td>
<td>See Also: &quot;Mail Merge&quot; on page 3-38 for more information about mail merge</td>
<td>merge or scheduled mail</td>
</tr>
<tr>
<td></td>
<td>and scheduled mail delivery.</td>
<td>delivery.</td>
</tr>
<tr>
<td>orclmailgrouptype</td>
<td>Type of distribution list, as described in Table 2–1, &quot;Distribution List</td>
<td>discussion</td>
</tr>
<tr>
<td></td>
<td>Group Types&quot;.</td>
<td>announcement</td>
</tr>
<tr>
<td></td>
<td>The quick distribution list type is invalid when using oesdl. This type is</td>
<td>edited</td>
</tr>
<tr>
<td></td>
<td>differentiated using the type file attribute.</td>
<td>moderated</td>
</tr>
<tr>
<td>orclmailgroupsubscription</td>
<td>Type of subscription control placed on the list, as described in Table 2–2,</td>
<td>open or</td>
</tr>
<tr>
<td>type</td>
<td>&quot;Distribution List Subscription Types&quot;.</td>
<td>restricted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>closed</td>
</tr>
<tr>
<td>orclmailgrouptopic</td>
<td>Establishes the topic of the distribution list.</td>
<td>A single line of text</td>
</tr>
<tr>
<td>orclmaxmsgsizemaxsize</td>
<td>The maximum allowable size of a message in bytes posted to the distribution</td>
<td>Any integer greater than</td>
</tr>
<tr>
<td></td>
<td>list. Messages exceeding this value are rejected.</td>
<td>or equal to 0</td>
</tr>
<tr>
<td></td>
<td>A value of 0 indicates unlimited message size.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Any integer value greater than or equal to 0. No range check is done so</td>
<td></td>
</tr>
<tr>
<td></td>
<td>administrator must enter a valid value.</td>
<td></td>
</tr>
</tbody>
</table>

Examples
This section includes the following topics:

- Adding Users to an Existing Distribution List
- Adding Users to a New Distribution List
- Removing Users from a Distribution List
- Deleting a Distribution List

The following examples assume the file named list_file contains the various records.
**Adding Users to an Existing Distribution List**

To add users to an existing distribution list:

```
% oesdl list_file
```

The `list_file` file contains the following record:

```
listname=list1@foo.com
action=add
newlist=n
usertype=U
users=user1@foo.com,user2@foo.com,user3@foo.com
```

```
listname=list2@foo.com
action=add
newlist=n
usertype=L
users=list1@foo.com
```

This adds user1, user2, and user3 (usertype=U) to list1@foo.com
(usertype=L), which must already exist, because `newlist=n` (no). It also adds list1@foo.com to another distribution list called list2@foo.com.

**Adding Users to a New Distribution List**

To add users to a new distribution list:

```
% oesdl list_file
```

The `list_file` file contains the following record:

```
listname=list1@foo.com
action=add
newlist=y
owner=user1@foo.com
usertype=U
type=listserver
owner=user1@us.oracle.com
orclmailgroupprivileged=true
orclmailgroupprivileged=false
orclmailgroupprivileged=owner
orclmailallowforeignmembers=false
orclmailgroupprivilegeoptions=member
orclmailuserstate=active
orclmailgroupprivilegesubscribers=active
orclmailgroupprivilegesubscribers=subscriber
orclmailgroupprivilegesubscribers=member
orclmailgrouptopic=discussion
orclmailgrouptopic=subscription
orclmailgrouptopic=subscription
orclmailgrouptopic=subscription
orclmailgrouptopic=subscription
orclmailgrouptopic=subscription
orclmailgrouptopic=subscription
orclmailgrouptopic=subscription
orclmailgrouptopic=subscription
orclmailgrouptopic=subscription
orclmailgrouptopic=subscription
orclmailgrouptopic=subscription
orclmailgrouptopic=subscription
orclmailgrouptopic=subscription
orclmailgrouptopic=subscription
orclmailgrouptopic=subscription
orclmailgrouptopic=subscription
orclmailgrouptopic=subscription
orclmailgrouptopic=subscription
orclmailgrouptopic=subscription
orclmailgrouptopic=subscription
orclmailgrouptopic=subscription
orclmailmaxmsgsize=4000000
users=user1@foo.com,user3@foo.com
```

This creates a new distribution list called list1@foo.com, establishes the owner as user1@foo.com, and adds users user1@foo.com and user3@foo.com to the new distribution list.

The new distribution list also has various attributes set.

If the distribution list has restricted subscription, the following line can be included for adding approvers:
orclmailgroupautoreconfirmtext=user1@foo.com,user3@foo.com

If the distribution list is edited, the following line can be included for adding editors:
orclmailgroupeditorslist=user1@foo.com,user3@foo.com

If the distribution list is moderated, the following line can be included for adding moderators:
orclmailgroupmoderatorslist=user1@foo.com,user3@foo.com

Removing Users from a Distribution List
To remove users from a distribution list:
% oesdl list_file

The list_file file contains the following records:
listname=list1@foo.com
action=delete
usertype=U
users=user1@foo.com,user2@foo.com

listname=list2@foo.com
action=add
newlist=y
owner=user1@foo.com
usertype=U
users=user1@foo.com,user2@foo.com

This removes user1 and user2 from list1@foo.com. It also creates a new distribution list called list2@foo.com, establishes the owner as user1@foo.com, and adds user1 and user2 to the new distribution list, list2@foo.com.

Deleting a Distribution List
To delete a distribution list:
% oesdl list_file -d

The list_file file contains the following record:
listname=list1@us.oracle.com
listname=list2@us.oracle.com

If the deletion is successful, the following message displays:
Successfully deleted list: list_file

If there are any errors in deleting the list, the following error message displays:
Error in deleting list: list_file

This utility enables administrators to create and delete NNTP newsgroups in the Oracle Collaboration Suite system. This utility accepts a file as input and creates or deletes newsgroups according to the information specified in the file.
File Format

The file passed as input to the oesng command-line utility must contain a list of records, with each list followed by an empty line. Each record consists of a set of parameter=value pairs containing information about the newsgroup to be created or deleted. Names are not case-sensitive. Unless indicated otherwise, all parameters can be specified only once for a newsgroup. Lines that begin with the number sign (#) are treated as comments and are not processed by the utility.

For newsgroups that are being deleted, it is sufficient to specify the name of the newsgroup and the action as delete.

Parameters

Table D–2 lists parameters used by the oesng command-line utility.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Acceptable Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Name of the newsgroup to be created or deleted</td>
<td>Any valid newsgroup name</td>
<td>Mandatory (no default)</td>
</tr>
<tr>
<td>newsstore</td>
<td>Name of the news store on which this newsgroup is to be created</td>
<td>Any valid news store in the Oracle Collaboration Suite system</td>
<td>Mandatory for newsgroup creation</td>
</tr>
<tr>
<td>action</td>
<td>Creating or deleting the newsgroup</td>
<td>Create or Delete</td>
<td>Create</td>
</tr>
<tr>
<td>owner</td>
<td>Owner of the newsgroup</td>
<td>Any valid e-mail address in the Oracle Collaboration Suite system</td>
<td>None</td>
</tr>
<tr>
<td>description</td>
<td>Description for the newsgroup</td>
<td>Single line of text</td>
<td>None</td>
</tr>
<tr>
<td>moderatedroup</td>
<td>Boolean specifying whether the newsgroup is moderated</td>
<td>True or False</td>
<td>False</td>
</tr>
<tr>
<td>moderator</td>
<td>Names the moderator for the newsgroup. Can be specified more than once for a newsgroup.</td>
<td>Any valid e-mail address</td>
<td>None</td>
</tr>
<tr>
<td>postingallowed</td>
<td>Boolean telling whether posting is allowed to the newsgroup</td>
<td>True or False</td>
<td>False</td>
</tr>
<tr>
<td>retentiondayss</td>
<td>Number of days to retain an article in a newsgroup before being expired</td>
<td>Any positive integer</td>
<td>None</td>
</tr>
<tr>
<td>domain</td>
<td>Domain to which the newsgroup belongs, if the newsgroup being created or deleted is a private newsgroup</td>
<td>Any valid domain in the Oracle Collaboration Suite system</td>
<td>None</td>
</tr>
<tr>
<td>installation</td>
<td>Name of the installation where the newsgroup is to be created</td>
<td>Any valid installation name in the Oracle Collaboration Suite system</td>
<td>um_system</td>
</tr>
</tbody>
</table>

Usage

oesng file
In this example, file is the path to the file containing the newsgroups to be processed.

**Examples**
The following examples show how to use the oesng command-line utility.

This section includes the following topics:

- Creating a Simple Public Newsgroup
- Creating a Public Moderated Newsgroup
- Creating a Public Newsgroup
- Deleting a Public Newsgroup

**Creating a Simple Public Newsgroup**
The following example demonstrates how to create a simple public newsgroup.

oesng newsfile

In this example, newsfile contains the following:

name=newsgroup1
newsstore=db1.acme.com

**Creating a Public Moderated Newsgroup**
The following example demonstrates how to create a public moderated newsgroup that permits posting and retains articles for 15 days.

oesng newsfile

In this example, newsfile contains the following:

name=newsgroup2
newsstore=db1.acme.com
action=create
description=A new newsgroup
moderatedgroup=true
moderator=user1@acme.com
moderator=user2@acme.com
postingallowed=true
retentiondays=15

**Creating a Public Newsgroup**
The following example demonstrates how to:

- Create a public newsgroup that does not allow posting
- Delete an existing private newsgroup
- Create a private moderated newsgroup that allows posting

oesng newsfile

In this example, newsfile contains the following:

name=newsgroup3
newsstore=db1.acme.com
postingallowed=false
name=private.newsgroup1
domain=acme.com
action=delete

name=private.newsgroup2
domain=acme.com
newsstore=db1.acme.com
postingallowed=true
moderatedgroup=true
moderator=mod1@acme.com
moderator=mod2@acme.com

Deleting a Public Newsgroup

The following example demonstrates how to delete a public newsgroup.

oesng newsfile

In this example, newsfile contains the following

name=newsgroup5
action=delete

oespr

This utility enables administrators to create and delete news peers and to associate newsgroups with news peers in an Oracle Collaboration Suite system. It accepts a text file as input and creates or deletes peers according to the information specified in the file.

The file that is passed as input to the oespr utility must contain a list of records, each followed by an empty line. Each record consists of a set of parameter=value pairs that contain information about the newsgroup being created or deleted. Parameters are not case-sensitive. Unless indicated otherwise, all parameters can be specified only once for a peer.

Lines beginning with the number sign (#) are treated as comments and are not processed by the utility.

Table D–3 describes the parameters that can be specified in the file.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Acceptable Values</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>Fully qualified host name of the news peer being</td>
<td>Any valid peer host name</td>
<td>Mandatory (no default)</td>
</tr>
<tr>
<td></td>
<td>created or deleted</td>
<td></td>
<td></td>
</tr>
<tr>
<td>port</td>
<td>Port on which the NNTP server is running on the</td>
<td>Any valid port</td>
<td>119</td>
</tr>
<tr>
<td></td>
<td>peer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>action</td>
<td>Creating or deleting the peer</td>
<td>Create or Delete</td>
<td>Create</td>
</tr>
<tr>
<td>acceptgroup</td>
<td>List of groups accepted from this peer; can be</td>
<td>Any valid group name</td>
<td>NA</td>
</tr>
<tr>
<td></td>
<td>specified more than once for a peer.</td>
<td>Wildcard patterns can also</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>be specified.</td>
<td></td>
</tr>
</tbody>
</table>
Usage

oespr filename

In this example, filename is the path to the file containing the peers to be processed.

Examples

The following examples show how to use the oespr command-line utility.

This section includes the following topics:

- Creating a Simple Peer
- Creating a Peer Using Articles from Specific Newgroups
- Deleting a Peer

Creating a Simple Peer

To create a simple peer:

% oespr peer_file

The peer_file file contains the following record:

hostname=host1.foo.com

Creating a Peer Using Articles from Specific Newgroups

To create host1.foo.com as a peer that uses articles from the comp.lang.c and comp.lang.java groups on port 2119:

% oespr peer_file

The peer_file file contains the following record:

hostname=host1.foo.com
port=2119
feedgroup=comp.lang.c
feedgroup=comp.lang.java

Deleting a Peer

To delete a peer:

% oespr peer_file

Table D–3  (Cont.) oespr Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Acceptable Values</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>rejectgroup</td>
<td>List of groups to be rejected if offered by this peer; can be specified more than once for a peer.</td>
<td>Any valid group name. Wildcard patterns can also be specified.</td>
<td>NA</td>
</tr>
<tr>
<td>feedgroup</td>
<td>List of groups for which this peer should be fed; can be specified more than once for a peer.</td>
<td>Any valid public newsgroup name.</td>
<td>NA</td>
</tr>
<tr>
<td>installation</td>
<td>Name of the installation where the peer is to be created.</td>
<td>Any valid installation name in the Oracle Collaboration Suite system.</td>
<td>um_system</td>
</tr>
</tbody>
</table>
The peer_file file contains the following record:

hostname=host1.foo.com
action=delete

**oesucr**

The oesucr bulk provisioning utility is for creating and modifying large numbers of Oracle Mail users. When the Oracle Internet Directory command-line tool ldapadd is used to create the Oracle base user, the Oracle Mail user is also created in the process.

See Also: "Managing Entries by Using Command-Line Tools" in Chapter 6 of Oracle Internet Directory Administrator’s Guide for more information about ldapadd

**Usage**

% oesucr filename option option option ...

In this command, filename is the path to a text file containing e-mail user records and option can be any of the options listed in Table D–4.

Usage information is included in each of the following sections, as applicable.

**Table D–4  Options Used with the oesucr Command-Line Utility**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-v</td>
<td>Prints debug messages</td>
</tr>
<tr>
<td>-d</td>
<td>Deletes specified files or users</td>
</tr>
<tr>
<td>-change</td>
<td>Change e-mail addresses of a specified number of users in a file</td>
</tr>
<tr>
<td>-clean_user_mailstore_data</td>
<td>Clears data from the Oracle Collaboration Suite Database of users who have been deleted from the system but whose data has not yet been cleared.</td>
</tr>
<tr>
<td>-list_deleted_users</td>
<td>Lists currently deleted users whose data in the Oracle Collaboration Suite Database has not yet been cleared.</td>
</tr>
<tr>
<td>-encoding</td>
<td>Oracle recommends using the UTF-8 option to accommodate all languages.</td>
</tr>
</tbody>
</table>

Table D–5 lists the required and optional attributes to be specified in any text file containing e-mail user records passed to the oesucr utility.

**Table D–5  oesucr Attributes**

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Description</th>
<th>Options</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>mail</td>
<td>Specifies the user’s fully qualified e-mail address. The user’s e-mail ID must be the same as the User Name attribute for the base user.</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>orclmailquota</td>
<td>Specifies e-mail quota of a user in bytes.</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>baseuserdn</td>
<td>The DN where the base user is created.</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>orclmailstore</td>
<td>Specifies the Oracle Collaboration Suite Database to be used as mail store for the user.</td>
<td>NA</td>
<td>NA</td>
</tr>
</tbody>
</table>
### Examples

The following examples show how to use the `oesucr` command-line utility.

This section includes the following topics:
- Creating Oracle Mail Users
- Creating Oracle Mail Users at the Command Line
- Deleting Oracle Mail Users
- Clearing Data from the Oracle Collaboration Suite Database
- Listing Deleted Users Whose Data Has Not Been Cleared
- Changing the E-mail Address of an Oracle Mail User

### Creating Oracle Mail Users

To create Oracle Mail users:

```
% oesucr filename -v
```

The `-v` option prints out debug messages.

---

**Table D–5 (Cont.) oesucr Attributes**

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Description</th>
<th>Options</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>orclmailvoicequota</code></td>
<td>Specifies additional quota for voice mail in bytes.</td>
<td>NA</td>
<td>1000000</td>
</tr>
<tr>
<td><code>orclmailuserstate</code></td>
<td>Defines the user as active or inactive. If <strong>User State</strong> is active, the user can receive and send e-mail; if inactive, the user cannot receive and send e-mail</td>
<td>active, inactive, or migrating</td>
<td>active</td>
</tr>
<tr>
<td><code>orclforwardaddress</code></td>
<td>Stores the e-mail addresses for the automatic forwarding feature</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td><code>orclmailuserindextype</code></td>
<td>Specifies if text indexing should be performed on only the e-mail text or both the e-mail and the attachment.</td>
<td>0 = Disabled, 1 = Enabled</td>
<td>0</td>
</tr>
<tr>
<td><code>orcldomaincontrolacici</code></td>
<td>Specifies whether the user is a system administrator, domain administrator, or regular user.</td>
<td>system, domain, or regular</td>
<td>regular</td>
</tr>
<tr>
<td><code>orclwebmaildisplayallheaders</code></td>
<td>Specifies whether Oracle WebMail headers are displayed in a detail view for the user.</td>
<td>yes or no</td>
<td>yes</td>
</tr>
<tr>
<td><code>orclwebmailnumdisplay</code></td>
<td>Specifies the number of messages shown at a time for a user in Oracle WebMail.</td>
<td>NA</td>
<td>20</td>
</tr>
<tr>
<td><code>orclmailarchivingpolicyid</code></td>
<td>Specifies the archiving policy to be associated with the user.</td>
<td>name_of_policy</td>
<td>NA</td>
</tr>
</tbody>
</table>

Use the name of the policy created in "Creating an Archive Policy" on page D-27.

Leading and trailing spaces are ignored and embedded spaces in policy names are accepted, such as Policy A. The string need not be enclosed in quotation marks.

**Notes:** The policy must be created before it can be referenced using the oesucr utility.

**See Also:** Example D-1 on page D-13 for examples of users created with associated archiving policies
The file specified in filename is a text file that contains user records and must contain the following attributes:

- **mail=user_ID@domain.com**: Specify the user’s fully qualified e-mail address. The user’s e-mail ID must be the same as the User Name attribute for the base user. For example:
  
  mail=testuser1@foo.com

- **orclmailquota=number_of_bytes**: The size, in bytes, allocated to the user’s mailbox. For example:
  
  orclmailquota=10000000

- **baseuserdn=DN**: The DN where the base user was created. For example:
  
  baseuserdn=cn=testuser1,cn=users,dc=foo,dc=com

Optionally, you can specify a user’s privileges and create folders by including the following attributes in the file:

- **orclMailDomainControlAci=value**: Enter one of the following values to specify a user’s administration privilege:
  
  - system: Gives user system administrator privileges
  - domain: Gives user domain administrator privileges
  - regular: User has no administrative privileges

  By default, if orclMailDomainControlAci is not specified, the user is created as a regular user with no administrative privileges.

- **folder**: Comma-separated names of folders to be created while creating the user

To specify multiple user records to be created in a single file, use an empty line in between each user record, as shown in Example D–1.

**Example D–1  ** File Containing Multiple Users

```
mail=tuser1@us.foo.com
orclmailquota=400000000
baseuserdn=cn=tuser1,cn=users,dc=us,dc=foo,dc=com
orclmailarchivingpolicyid=Policy A

mail=tuser2@us.foo.com
orclmailquota=400000000
baseuserdn=cn=tuser2,cn=users,dc=us,dc=foo,dc=com
orclmailarchivingpolicyid=Policy A
orclmaildomaincontrolaci=system

mail=tuser3@us.foo.com
orclmailquota=400000000
baseuserdn=cn=tuser3,cn=users,dc=us,dc=foo,dc=com

mail=tuser4@us.foo.com
orclmailquota=400000000
baseuserdn=cn=tuser4,cn=users,dc=us,dc=foo,dc=com
orclmailarchivingpolicyid=Stratégie
```
Example
Create two e-mail users, user1@foo.com and user2@foo.com. Both users will have a 10 MB mailbox quota; each will have folders called Personal and Work; and user2 will be given domain administrator privileges.

1. Use Oracle Delegated Administration Services to check that the base user accounts for user1 and user2 exist.

2. Create a file containing the following information for user1 and user2. The file is called user_file for this example and contains the following lines of text:

   mail=user1@foo.com
   orclmailquota=10000000
   baseuserdn=cn=user1,cn=users,dc=foo,dc=com
   folder=personal,work

   mail=user2@foo.com
   orclmailquota=10000000
   baseuserdn=cn=user2,cn=users,dc=foo,dc=com
   orclMailDomainControlAci=domain
   folder=personal,work

   ________________________________________________________________________________

   Note: Each Oracle Mail user to be created is separated by an empty line.
   ________________________________________________________________________________

3. Execute the oesucr command:

   % oesucr user_file

Creating Oracle Mail Users at the Command Line

The following example shows how to create an Oracle Mail user using the command line, without creating a new file. Only one user can be created at a time with this method.

   % oesucr -cmd mail=user1@foo.com
   baseuserdn=cn=user1,cn=users,dc=foo,dc=com orclmailquota=40000000 other_optional_attributes

   All parameters are separated by a space, and have the same names as those used in the file. All mandatory attributes must be specified, while any valid optional attributes can be added.
Deleting Oracle Mail Users

To delete Oracle Mail users:

% oesucr filename -d -v

The file specified in *filename* is a text file that contains user IDs of Oracle Mail users to be deleted, as follows:

```plaintext
mail=user_ID@domain.com
```

Specify the user’s fully qualified e-mail address. The user’s e-mail ID must be the same as the **User Name** attribute for the base user. For example:

```plaintext
mail=testuser1@foo.com,testuser2@foo.com
```

To specify multiple user records to be deleted in a single file, use a comma to separate the addresses of the Oracle Mail users.

The `-d` option deletes Oracle Mail users.

The `-v` option prints out debug messages.

**Example**

Delete the Oracle Mail user accounts for *user1*, *user2*, and *user3*.

1. Create a file containing the Oracle Mail users to be deleted. The file is called *delete_user* for this example and contains the following line of text:

   ```plaintext
   mail=user1@foo.com,user2@foo.com,user3@foo.com
   ```

2. Execute the `oesucr` command:

   ```sh
   % oesucr delete_user -d
   ```

   The `-d` option deletes Oracle Mail users.

**Clearing Data from the Oracle Collaboration Suite Database**

Use the `-clean_user_mailstore_data` option to Clear data from the Oracle Collaboration Suite Database of users who have been deleted from the system and whose data has not yet been cleared, as follows:

Notes:

- Deleting Oracle Mail users using `oesucr` does not delete the base user in Oracle Internet Directory. To Delete a user from Oracle Internet Directory, you must use Oracle Delegated Administration Services.

- When an e-mail user is removed, any shared folders and public shared folders owned by that user are also deleted; however, user data stored in the Oracle Collaboration Suite Database is not removed.

- If the user being deleted owns a distribution list or newsgroup, the user deletion will not proceed. An error message displays that contains the names of the distribution lists or newsgroups owned by this user. The administrator must change the ownership for these lists and newsgroups in order to proceed with user deletion.
oesctl and opmnctl

% oesucr filename -clean_user_mailstore_data

The file specified in filename is a text file that contains user IDs of deleted Oracle Mail users, as follows:

mail=user1@foo.com,user2@foo.com,user3@foo.com,...

If a user has not yet been deleted, the following error message displays after the oesucr command is executed:

user1@foo.com has not been deleted. Cannot remove mail store data.

If there is an error while removing data from the Oracle Collaboration Suite Database, the following error message displays:

Error :- user1@foo.com mail store data has not been deleted.

Listing Deleted Users Whose Data Has Not Been Cleared

Use the -list_deleted_users option to list currently deleted users whose data in the Oracle Collaboration Suite Database has not yet been cleared. This option does not require a file name in the command and is executed, as follows:

oesucr -list_deleted_users

If there are no deleted users, the following message displays:

There are no deleted users present.

If there are deleted users, they are listed one user for each line in the following format:

User user_ID deleted on date_deleted

For example:

User user1@foo.com deleted on Fri July 29 08:12:44 EDT 2005

Changing the E-mail Address of an Oracle Mail User

To change the e-mail address of a user:

% oesucr filename -change

The file specified in filename is a text file that contains the following records, in the form old_username@domain.com=new_username@domain.com:

user1@foo.com=new_user1@foo.com
user2@foo.com=new_user2@foo.com

oesctl and opmnctl

The oesctl utility enables an Oracle Mail administrator to perform a subset of the configuration operations for Oracle Mail services that are available through the Oracle Enterprise Manager 10g interface. The utility is accessed through a command shell, such as /usr/csh in UNIX.

Oracle Mail in Oracle Collaboration Suite 10g is integrated with opmn for process control. This allows Oracle Mail server processes to be started and stopped using the same opmnctl script as is used to start processes for other Oracle Collaboration Suite components. opmnctl also restarts Oracle Mail server processes if they stop unexpectedly, which helps to satisfy high availability requirements.
Configuration tasks using `oesctl` include:

- Showing the list of Oracle Mail servers, such as IMAP and SMTP inbound servers
- Creating new process instances for Oracle Mail servers
- Deleting process instances from Oracle Mail servers
- Showing the list of process instances for Oracle Mail servers
- Enabling Oracle Mail servers
- Disabling Oracle Mail servers
- Synchronizing Oracle Mail server configuration in the LDAP server to `opmn.xml`
- Showing status for all instances of a particular Oracle Mail server

The `opmnctl` utility performs the following control tasks:

- Starting all process instances of an Oracle Mail server
- Starting a single process instance of an Oracle Mail server
- Stopping all process instances of an Oracle Mail server
- Stopping a single process instance of an Oracle Mail server
- Showing the status for all process instances of an Oracle Mail server
- Restarting one or all process instances of an Oracle Mail server
- Refreshing one or all process instances of an Oracle Mail server
- Dynamically starting and stopping Housekeeper tasks

### Usage

```
% oesctl command target instance
```

**Table D–6** lists `oesctl` commands. To get a list of commands from the command line, execute `oesctl` with no arguments.

```
% oesctl
```

**Table D–6  oesctl Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>startup</td>
<td>Start all the processes associated with the target or instance</td>
</tr>
<tr>
<td>shutdown</td>
<td>Shut down all the processes associated with the target or instance</td>
</tr>
<tr>
<td>create instance</td>
<td>Create an instance of a target</td>
</tr>
<tr>
<td>delete instance</td>
<td>Delete an instance of a target</td>
</tr>
<tr>
<td>refresh</td>
<td>Cause the target or instance to reload parameters from LDAP</td>
</tr>
<tr>
<td>show targets</td>
<td>Display a list of possible targets</td>
</tr>
<tr>
<td>show status</td>
<td>Display the status of the target</td>
</tr>
<tr>
<td>show processes</td>
<td>Show the processes associated with the target</td>
</tr>
<tr>
<td>enable</td>
<td>Enable the target</td>
</tr>
<tr>
<td>disable</td>
<td>Disable the target</td>
</tr>
<tr>
<td>sync_opmn_conf</td>
<td>Read process configuration from LDAP server and update <code>opmn</code> configuration</td>
</tr>
</tbody>
</table>
Examples
The following examples show how to use the oesctl and opmnctl command-line utilities.

This section includes the following topics:

- Listing Oracle Mail Servers
- Creating a New Oracle Mail Server Instance
- Deleting an Instance from an Oracle Mail Server
- Listing Oracle Mail Server Instances
- Enabling an Oracle Mail Server
- Disabling an Oracle Mail Server
- Synchronizing Oracle Mail Server Configuration in Oracle Internet Directory to opmn.xml
- Starting All Instances of an Oracle Mail Server
- Starting a Single Instance of an Oracle Mail Server
- Restarting One or All Instances of an Oracle Mail Server
- Refreshing One or All Instances of an Oracle Mail Server
- Stopping All Instances of an Oracle Mail Server
- Stopping a Single Instance of an Oracle Mail Server
- Dynamically Starting and Stopping Housekeeper Tasks
- Showing Status for All Instances of an Oracle Mail Server

Listing Oracle Mail Servers

To display a list of Oracle Mail servers:

% oesctl show targets
TARGET: appserver.foo.com:um_system:gc
TARGET: appserver.foo.com:um_system:imap
TARGET: appserver.foo.com:um_system:list
TARGET: appserver.foo.com:um_system:nntp_in
TARGET: appserver.foo.com:um_system:nntp_out
TARGET: appserver.foo.com:um_system:pop
TARGET: appserver.foo.com:um_system:smtp_in
TARGET: appserver.foo.com:um_system:smtp_out
TARGET: appserver.foo.com:um_system:vs

Creating a New Oracle Mail Server Instance

To create a new server instance:

% oesctl create instance target

In this example, target is one of the servers listed by executing oesctl show targets.

For example:

% oesctl create instance appserver.foo.com:um_system:smtp_in
Successfully created a new instance for a total of: 2
This command creates a new server instance entry in the Oracle Internet Directory server and also updates opmn.xml by adding a new opmn process-set entry so that the server can be controlled by opmn. When the server instance is started, it uses the default server instance parameter settings.

**See Also:** “Managing Oracle Mail Servers and Instances” on page 3-3 for more information about server parameters

### Deleting an Instance from an Oracle Mail Server

To delete a server instance:

```
% oesctl delete instance target
```

In this example, `target` is one of the servers listed by executing `oesctl show targets`.

For example:

```% oesctl delete instance appserver.foo.com:um_system:imap
```

Successfully deleted an instance for a total of: 0

This command selects one of the instances of the server and deletes the instance entry from the Oracle Internet Directory server. The corresponding opmn process-set entry is removed from opmn.xml.

To delete a specific instance, use Application Server Control Console for Collaboration Suite.

**See Also:** “Deleting a Server Instance” on page 3-7 for more information about deleting server instances using Application Server Control Console for Collaboration Suite.

### Listing Oracle Mail Server Instances

To display a list of server instances:

```
% oesctl show processes target
```

In this example, `target` is one of the servers listed by executing `oesctl show targets`.

For example:

```% oesctl show processes appserver.foo.com:um_system:smtp_in
appserver.foo.com:um_system:smtp_in:11179697423528299
appserver.foo.com:um_system:smtp_in:11180005391552521
```

The numbers assigned to each server instance are selected at instance creation time so that each instance has a unique name.

### Enabling an Oracle Mail Server

To enable an Oracle Mail server:

```% oesctl enable target
```

In this example, `target` is one of the servers listed by executing `oesctl show targets`.

For example:
% oesctl enable appserver.foo.com:um_system:pop

Enabling a server configures opmn so that the server can be started using either oesctl or opmnctl.

Once a server is enabled, it can be started by the following command:
% opmnctl startall

**Disabling an Oracle Mail Server**

To disable an Oracle Mail server:

% oesctl disable target

In this example, target is one of the servers listed by executing oesctl show targets.

For example:
% oesctl disable appserver.foo.com:um_system:pop

Disabling a server configures opmn so that the server cannot be started.

Once a server is disabled, it cannot be started by the following command:
% opmnctl startall

Disabling a server that is currently running will first stop the server, then disable it.

**Synchronizing Oracle Mail Server Configuration in Oracle Internet Directory to opmn.xml**

To synchronize the Oracle Mail server configuration information to opmn:
% oesctl sync_opmn_conf

For example:
% oesctl sync_opmn_conf
Update OPMN configuration for appserver.acme.com:um_system:gc
Update OPMN configuration for appserver.acme.com:um_system:imap
Update OPMN configuration for appserver.acme.com:um_system:list
Update OPMN configuration for appserver.acme.com:um_system:nttp_in
Update OPMN configuration for appserver.acme.com:um_system:nttp_out
Update OPMN configuration for appserver.acme.com:um_system:pop
Update OPMN configuration for appserver.acme.com:um_system:smtp_in
Update OPMN configuration for appserver.acme.com:um_system:smtp_out
Update OPMN configuration for appserver.acme.com:um_system:vs

Synchronizing the Oracle Mail server information in Oracle Internet Directory and in opmn.xml will first delete every Oracle Mail server entry in opmn.xml and then create new entries based on the entries found in Oracle Internet Directory.

Typically it is not necessary to synchronize the server information in Oracle Internet Directory and opmn.xml. They are both updated as server instances are created and deleted. However, unanticipated system failures can result in a configuration where the Oracle Mail server information in Oracle Internet Directory and in opmn.xml does not agree. The sync_opmn_conf option for oesctl is provided to recover from such situations.
Starting All Instances of an Oracle Mail Server

To start all instances of an Oracle Mail server:

% opmnctl startproc process-type=type

In this example, type is one of the following:

e-mail_housekeeper
e-mail_imap
e-mail_listserver
e-mail_nntp_in
e-mail_nntp_out
e-mail_pop
e-mail_smtp_in
e-mail_smtp_out
e-mail_virus_scrubber

For example:
% opmnctl startproc process-type=email_imap

This command starts all IMAP server instances that are not already running.

Starting a Single Instance of an Oracle Mail Server

To start a single instance of an Oracle Mail server:

% opmnctl startproc process-set=instance_number

In this example, instance_number is the numeric portion of the server instance name displayed by the oesctl show processes command.

Restarting One or All Instances of an Oracle Mail Server

Restarting a server instance causes the running server to stop running and then creates a new running server instance. If clients have open connections to the running server instance, they will be disconnected and must reconnect. Usually it is not necessary to restart a single server instance, but the facility is provided in case the need arises.

The opmnctl command syntax for restarting one or all instances of an Oracle Mail server uses the same process-type values and process-set values that are used for starting and stopping.

To restart all instances of an Oracle Mail server:

% opmnctl restartproc process-type=type emailRefresh=false

To restart a specific instance of an Oracle Mail server:

% opmnctl restartproc process-set=instance_number emailRefresh=false

Refreshing One or All Instances of an Oracle Mail Server

Refreshing a running server instance causes it to reload its configuration settings. Refresh a running server instance when the log level and debug flags of a running server instance are changed.

By changing either the log level, debug flags, or both, and refreshing the server instance, the administrator can change the behavior of the running server instance without disconnecting any clients that have open connections to the server. The log
level and debug flags are set using Application Server Control Console, as described in Chapter 3.

The opmnctl command syntax for refreshing one or all instances of an Oracle Mail server uses the same process-type values and process-set values as are used for starting and stopping.

To refresh all instances of an Oracle Mail server:

% opmnctl restartproc process-type=type

To refresh a specific process instance of an Oracle Mail server:

% opmnctl restartproc process-set=instance_number

---

**Note:** Even though the command syntax uses the keyword restartproc, server instances are not restarted. Running server instances continue to run without interruption. When the restartproc keyword is used but the emailRefresh=false argument is not given, the opmnctl restartproc command causes Oracle Mail server process instances to refresh, not restart.

---

**Stopping All Instances of an Oracle Mail Server**

To stop all instances of an Oracle Mail server:

% opmnctl stopproc process-type=type

In this example, type is one of the following:

email_housekeeper
email_imap
email_listserver
email_nntp_in
email_nntp_out
email_pop
email_smtp_in
email_smtp_out
email_virus_scrubber

For example:

% opmnctl stopproc process-type=email_imap

This command stops all IMAP server instances that are running.

**Stopping a Single Instance of an Oracle Mail Server**

To stop a single instance of an Oracle Mail server:

% opmnctl stopproc process-set=instance_number

In this example, instance_number is the numeric portion of the server instance name displayed by the oesctl show processes command.

**Dynamically Starting and Stopping Housekeeper Tasks**

An administrator can use opmnctl to dynamically start and stop the Housekeeper tasks described in "Configuring Housekeeper Tasks" on page 3-24 from the command line.
When `opmnctl` is used to dynamically start and stop these tasks, a notification is sent to running Housekeeper server instances. The notification informs a running server instance which task is affected and whether the task should be started or stopped.

To dynamically start or stop a Housekeeper server task for all Housekeeper server instances:

```
% opmnctl restartproc process-type=email_housekeeper esgc-action=action
  esgc-task=task
```

In this example, `action` is one of the following:
- `start-task`
- `stop-task`

In this example, `task` is one of the following:
- `expiration`
- `pruning`
- `collection`
- `index-synch`
- `index-optimize`
- `tertiary-store`

The following command stops the pruning task for all Housekeeper servers:

```
% opmnctl restartproc process-type=email_housekeeper esgc-action=stop-task
  esgc-task=pruning
```

Giving the `opmnctl` argument `process-type=email_housekeeper` sends the task notification to all running instances of the Housekeeper server. As with all other `opmnctl` commands for Oracle Mail servers, the scope of the command can be restricted to a specific server instance by using `process-set=instance_number`.

To dynamically start or stop a Housekeeper server task for a specific Housekeeper server instance:

```
% opmnctl restartproc process-set=instance_number esgc_action=action
  esgc_task=task
```

In this example, `instance_number` is the numeric portion of the process instance name displayed by the `% oesctl show processes` command.

The following command stops the pruning task for a particular Housekeeper server:

```
% opmnctl restartproc process-set=111179697423568489 esgc-action=stop-task
  esgc-task=pruning
```

### Showing Status for All Instances of an Oracle Mail Server

To show the status of all instances for a given Oracle Mail server, use `oesctl`, as in the following example:

```
% oesctl show status appserver.acme.com:um_system:smtp_in
appserver.foo.com:um_system:smtp_in:111180005391552521 ----Heartbeat-----
appserver.foo.com:um_system:smtp_in:111205631039366429 <stopped>
appserver.foo.com:um_system:smtp_in:111205632368920420 ----Heartbeat-----
```

The `opmnctl` utility can also be used to view the status of the servers controlled and monitored by `opmn`. 
For example:

```
% opmnctl status
```

Processes in Instance: OCS_Apps.appserver.foo.com

<table>
<thead>
<tr>
<th>ias-component</th>
<th>process-type</th>
<th>pid</th>
<th>status</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP_Server</td>
<td>HTTP_Server</td>
<td>N/A</td>
<td>Down</td>
</tr>
<tr>
<td>WebCache</td>
<td>WebCache</td>
<td>N/A</td>
<td>Down</td>
</tr>
<tr>
<td>WebCache</td>
<td>WebCacheAdmin</td>
<td>N/A</td>
<td>Down</td>
</tr>
<tr>
<td>dcm-daemon</td>
<td>dcm-daemon</td>
<td>7661</td>
<td>Alive</td>
</tr>
<tr>
<td>email</td>
<td>email_housekeeper</td>
<td>N/A</td>
<td>Down</td>
</tr>
<tr>
<td>email</td>
<td>email_imap</td>
<td>N/A</td>
<td>Down</td>
</tr>
<tr>
<td>email</td>
<td>email_listserver</td>
<td>N/A</td>
<td>Down</td>
</tr>
<tr>
<td>email</td>
<td>email_nntp_in</td>
<td>N/A</td>
<td>Down</td>
</tr>
<tr>
<td>email</td>
<td>email_nntp_out</td>
<td>N/A</td>
<td>Down</td>
</tr>
<tr>
<td>email</td>
<td>email_smtp_in</td>
<td>10156</td>
<td>Alive</td>
</tr>
<tr>
<td>email</td>
<td>email_smtp_in</td>
<td>10169</td>
<td>Alive</td>
</tr>
<tr>
<td>email</td>
<td>email_smtp_out</td>
<td>N/A</td>
<td>Down</td>
</tr>
<tr>
<td>email</td>
<td>email_virus_scrub~</td>
<td>N/A</td>
<td>Down</td>
</tr>
</tbody>
</table>

**oesrl**

The **oesrl** utility enables an Oracle Mail administrator to create and manage server-side rules. It takes Java or XML format input from a file. This command can also be used to print out existing rules in XML format to standard output.

**See Also:** “Creating Server-Side Rules” on page 9-8 for more information about using **oesrl**

**Usage**

- `-p` prints a rule.
- `-c filename` creates a rule from a properties file.
- `-r` reads a rule from a directory to see if the rule is correct in the Oracle Collaboration Suite Database.
- `-x filename` creates a rule from an XML file.
- `-v` verifies that a rule is present on a database.

This section includes examples of server-side rules that perform a variety of functions. These rules can be placed in a file and called with the `oesrl -x filename` command.

This section includes the following topics:

- Deleting Server-Side Rules
- Blocking Messages Containing Suspicious Attachments
- Rejecting Messages Based on Text Strings
- Capturing Outbound Messages Regardless of Domain
- Copying Outgoing Messages to a Specific Account
- Discarding All Messages from One Sender
- Copying Messages into a Folder
Rejecting Messages with Too Many Recipients

Tips for Managing Server-Side Rules

Deleting Server-Side Rules

To delete server-side rules:

1. Print a list of rules for a particular user or domain with the following command:
   
   ```
   $ oesrl -p user1@domain.com
   ```

2. Remove the `<rule></rule>` block from the XML file for each rule you want to delete.

Blocking Messages Containing Suspicious Attachments

This systemwide rule blocks messages containing attachments containing particular file types. In this example, the rule blocks attachments containing .exe files.

```xml
<account qualifiedName="UM_SYSTEM" ownerType="system">
  <rulelist event="reception">
    <rule description="block exe">
      <condition>
        <attribute tag="xheader" param="Content-Disposition"/>
        <operator op="contains"/>
        <operand>exe</operand>
      </condition>
      <action>
        <command tag="reject">
          <parameter>Please do not send e-mails with .exe attachments. Your e-mail is rejected.</parameter>
        </command>
      </action>
    </rule>
  </rulelist>
</account>
```

Rejecting Messages Based on Text Strings

This systemwide rule rejects messages based on text strings contained in Subject headers. In this example, the rule rejects messages that contain the word Viagra in the Subject.

```xml
<account qualifiedName="UM_SYSTEM" ownerType="system">
  <rulelist event="reception">
    <rule description="Deliver Detail" group="all" active="yes" visible="no">
      <condition negation="no" junction="and">
        <attribute tag="rfc822subject"/>
        <operator caseSensitive="no" op="contains"/>
        <operand>viagra</operand>
      </condition>
      <action>
        <command tag="reject">
          <parameter>We do not need your SPAM here, thank you.</parameter>
        </command>
      </action>
    </rule>
  </rulelist>
</account>
```

Alternatively, use `<command tag="discard">` to send nothing back to the spammer. Depending on the number of spam words you want to block, you can write
a separate rule for each or you can write a simple PL/SQL function that queries your own table of spam words, and use this as your condition check in the rule.

Capturing Outbound Messages Regardless of Domain

An outbound message cannot be associated with a domain because users can write whatever they want in the From header, thus making the domain information meaningless. You can capture all outbound messages regardless of domain by using the relay event, as long as the messages are addressed to an outside user. Messages sent between local users will not trigger the relay event.

```plaintext
ruleowner=um_system
ruletype=system
event1=relay
relay.rule1=Capture From
relay.rule1.attr1=rfc822from
relay.rule1.op1=contains
relay.rule1.operand1=perfitcomputer.com
relay.rule1.action1=call
relay.rule1.action1.param1=perfit_custom_rules.incoming_forward
relay.rule1.action1.param2=from rule
relay.rule1.action1.param3=parameter2
```

You can either do the forwarding using your procedure, or just use the "forward" or "bcc" action. As for creating rules for users, you will need to write Java code that uses the shipped SDK `oracle.mail.sdk.rule.*` classes in `esmail_sdk.jar`. To prevent people from disabling it, you can set the "visible" attribute for each rule to be "no", but a systemwide rule, such as the preceding, is preferred.

See Also: "XML Representation of Rules" in Chapter 2 of Oracle Mail Application Developer's Guide for more information about creating rules using Java

Copying Outgoing Messages to a Specific Account

This systemwide rule copies outgoing messages to a specific account.

```xml
<account qualifiedName="UM_SYSTEM" ownerType="system">
  <rulelist event="relay">
    <rule description="Detail Records" group="all" active="yes" visible="yes">
      <action>
        <command tag="bcc"/>
        <parameter>outgoing@foo.com</parameter>
      </action>
    </rule>
  </rulelist>
</account>
```

Discarding All Messages from One Sender

This rule discards all messages from one specific sender.

```xml
<account qualifiedName="sysadmin@foo.com" ownerType="user" id="0">
  <rulelist event="deliver">
    <rule description="Delete from u1@mhornspe1" group="all" active="yes" visible="yes">
      <condition negation="no" junction="and">
        <condition negation="no" junction="and">
          <attribute tag="rfc822from"/>
          <operator caseSensitive="no" op="contains"/>
        </condition>
      </condition>
    </rule>
  </rulelist>
</account>
```
Copying Messages into a Folder

This is a simple example illustrating a complete XML definition that moves messages sent to a specific e-mail address to a subfolder of the user’s mailbox. The triggering event is deliver, so it will take effect whether the user is logged in or not.

```xml
<account qualifiedName="username@example.com" ownerType="user" id="0">
  <rulelist event="deliver">
    <rule description="dummy" group="all" active="yes" visible="yes">
      <condition negation="no" junction="and">
        <attribute tag="rfc822to"/>
        <operator caseSensitive="no" op="contains"/>
        <operand>an-email@address.com</operand>
      </condition>
      <action>
        <command tag="moveto"/>
        <parameter>/username/file-this</parameter>
      </action>
    </rule>
  </rulelist>
</account>
```

Note: The `/user/file-this` folder must exist for the rule action to be successful. Typically, such rules are created through an end-user interface like Oracle WebMail or Outlook so the syntax of this is not important for the user.

Rejecting Messages with Too Many Recipients

This more complex rule checks the number of recipients of a message, and rejects the message if that number is too high. This is a systemwide rule, and one that applies to relay events to stop users from trying to send messages to large groups of people. The condition is an external procedure to illustrate how to call external PL/SQL from within a server-side rule.

```xml
<account qualifiedName="um_system" ownerType="system" id="0">
  <rulelist event="relay">
    <rule description="TooMany" group="all" active="yes" visible="yes">
      <condition negation="no" junction="and">
        <procCall>RulesPackage.count_recipients</procCall>
      </condition>
      <action>
        <command tag="reject"/>
      </action>
    </rule>
  </rulelist>
</account>
```
In this example, the condition is an external call to a user-defined PL/SQL function called `RulesPackage.count_recipients`. Following is the PL/SQL function that defines this package. For external conditions, two internal parameters are passed to the function—a session ID and a mail message object—that allow examination of the message data.

In this example, some rudimentary checking is performed on the To: and Cc: strings, and the maximum recipient count is part of the code of the function. More information about the PL/SQL APIs for e-mail are provided in the product documentation set.

```sql
CREATE OR REPLACE PACKAGE RulesPackage AS

FUNCTION count_recipients( p_data varchar2 ) return number;
-- conditions return 0 = Positive rule match
FUNCTION countRecipients(p_sessionid in integer,
 p_msgobj in mail_message_obj)
    return integer;
END RulesPackage;

CREATE OR REPLACE PACKAGE BODY RulesPackage AS

FUNCTION count_recipients ( p_data   VARCHAR2)
RETURN number IS
  v_count   NUMBER          := 1;
BEGIN
  FOR i IN 1 .. LENGTH (p_data) LOOP
    IF substr (p_data, i, 1) = ',' THEN
      v_count := v_count + 1;
    END IF;
  END LOOP;
  RETURN v_count;
END count_recipients;

FUNCTION countRecipients(p_sessionid in integer,
 p_msgobj in mail_message_obj)
return integer
is
  max_recipients    integer:=50;
  to_str            varchar2(1024);
  cc_str            varchar2(1024);
  to_count          integer:=0;
  cc_count          integer:=0;
begin
  -- Condition == 0 => condition is TRUE
  -- Condition !== 0 => condition is FALSE
  mail_message.get_header(p_sessionid, p_msgobj, 'TO', to_str);
  mail_message.get_header(p_sessionid, p_msgobj, 'CC', cc_str);

```
if to_str is not null
then
    to_count:=count_recipients(to_str);
end if;

if cc_str is not null
then
    cc_count:=count_recipients(cc_str);
end if;

if to_count + cc_count > max_recipients then
    return 0; -- There are too many recipients
else
    return 1; -- Recipient count is OK, just return anything other than 0
end if;

end countRecipients;
END RulesPackage;

**Tips for Managing Server-Side Rules**

Consider the following tips when managing server-side rules:

1. Do not use oidadmin to delete server-side rules. Because rules are stored in multiple places, using only oidadmin to delete them causes data inconsistencies. A rule may appear to have been deleted but it can be executed nonetheless if oidadmin is the only method used to delete rules.

2. To delete all the rules associated with a user or domain, or all the systemwide rules, create a file with an empty rule, as follows:

   ```
   <account qualifiedName="foo.com" ownerType="domain"/>
   ```

   Use oesrl -x to load the file to remove all existing rules.

3. To delete a particular rule or rules, first use oesrl -p to retrieve the rules into a file, edit out the rules that you want to delete, and reload the edited XML file. A rule is defined within the following XML element:

   ```
   <rule>...</rule>
   ```

4. The problem with creating a BCC rule as a domainwide rule is that this operation is not allowed at the reception event. Technically, the reception event does not have information about a domain. Therefore, no domain rules can be executed. Instead, create the rule at the deliver event, or create a systemwide rule instead of a domainwide rule.

5. The order to execute rules is:
   a. System-defined server-side rules.
   b. User-defined server-side rules.
   c. User-defined client-side rules.

6. Automatic reply is not a server-side rule. It is a feature of the SMTP server. Automatic reply is performed before any rules (system or user) are applied and after any systemwide or domainwide rules.

7. In Oracle Internet Directory, rule information is stored under the related mail account for user rules as orclmailrulescope=User_Rule using the
orclmailruledata attribute. In the Oracle Collaboration Suite Database, a related package for the rule is created containing the orclobjectid of the mail account.

oesmon

This utility enables an Oracle Mail administrator to obtain raw metric data from the Oracle Mail server processes for system monitoring purposes. The output of the oesmon command is in ASCII characters.

See Also: "Using oesmon" on page 7-9 for oesmon usage information

oeschart

This utility enables an Oracle Mail administrator to create graphs illustrating the system's current load and performance. The images are only created when the command is run. Therefore, to have dynamically updated charts, administrators must schedule periodic invocations of the program, such as with cron on UNIX systems or as a DBMS job.

See Also: "Using oeschart" on page 7-11 for oeschart usage information

oesbkp

This utility restores backed-up items at different levels of granularity. For example, you can restore either an entire user account or a single folder, which is particularly useful for backing up and restoring critical information.

See Also: "Backing Up and Restoring User Data with oesbkp" on page 10-2 for oesbkp usage information

oeschk

This utility identifies, reports, and corrects the schema entries and entry-level inconsistencies that occur due to absent transaction support in Oracle Collaboration Suite.

There are transactions identified that concern multiple entities and have the potential for leaving incomplete data due to absent transaction support. To build transaction support for all these entities can severely affect performance. The oeschk utility performs negative checks as the operation progresses and ensures there are no invalid entities or inconsistent data. It also reports the invalid entries found during the checks and corrects those entries, if possible.

Oracle Collaboration Suite components use Oracle Internet Directory to store information store-related schema, process-related schema, and directory-related schema. However, different components use different SDKs and they do not have transactional support for operations that involve multiple round-trips to Oracle Internet Directory.

Therefore, inconsistent data can be present in Oracle Internet Directory, as well as the database, making it difficult for administrators to diagnose problems. This utility lists the inconsistent entries across the Oracle Collaboration Suite-related entries both in Oracle Internet Directory and the Oracle Collaboration Suite Database.
Usage

Use this utility from the Oracle Collaboration Suite Applications tier only, as follows:

% oeschk entrytype=value domain=value filter=value fix=value

Table D–7 lists oeschk attributes and descriptions for each.

Table D–7  oeschk Attributes

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Description</th>
<th>Options</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>entrytype</td>
<td>Indicates the entries to be checked</td>
<td>all, user, list, alias, foreign, folder, process, newsgroup, newspeer, rule, addressbook, policy</td>
<td>all</td>
</tr>
<tr>
<td>domain</td>
<td>Domain under which the entries to be checked reside</td>
<td>Any string</td>
<td>NA</td>
</tr>
<tr>
<td>filter</td>
<td>User-defined filters to check for</td>
<td>Any string</td>
<td>***</td>
</tr>
<tr>
<td></td>
<td>Note: Because C shell is sensitive to wildcard characters, surround the filter attribute and its value with double quotation marks (**).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>fix</td>
<td>Determines whether entries are corrected or not</td>
<td>true or false</td>
<td>false</td>
</tr>
</tbody>
</table>

Note: All attributes are to be specified as name=value pairs. All attributes should appear only once on the command line but can appear in any order. Only the entrytype and domain attributes are mandatory.

Examples

The following command displays all the user entry inconsistencies in the Oracle Collaboration Suite installation to the console:

oeschk entrytype=users domain=foo.com

The following command displays all Oracle Mail schema entry inconsistencies in the Oracle Collaboration Suite installation to the console:

oeschk entrytype=all domain=foo.com

The following command displays inconsistencies of an Oracle Mail user in the Oracle Collaboration Suite installation to the console:

oeschk entrytype=user domain=foo.com "filter=orcladmin@ocs.foo.com"

The following command displays inconsistencies of all lists with names beginning with the word list in the Oracle Collaboration Suite installation to the console, and corrects any invalid list entries.

oeschk entrytype=list domain=foo.com "filter=list*@ocs.foo.com" fix=true
The `oeschk` utility checks on the following schema entries for inconsistencies caused by absent transactional support in Oracle Internet Directory:

- Users
- Distribution Lists
- Aliases
- Foreign Users
- Processes
- Newsgroups
- News Peers
- Shared Folders
- Server-Side Rules
- Private Address Books

Each of the subsequent sections contains information about various checks that the `oeschk` utility carries out with each of the schema entries, including Oracle Internet Directory checks, Oracle Collaboration Suite Database checks, and details of corrections that the utility can perform.

The utility prints warnings, errors, and messages to the console and does not log any files (although an administrator can redirect output to a file).

**Users**

The following high-level operations can lead to user inconsistencies:

- Oracle Mail user creation
- Oracle Mail user deletion
- Oracle Mail user modifications
- Oracle Mail user renaming
- Base user deletion
- Granting domain administrator rights to a user

Figure D–1 shows which entries are checked as part of a user inconsistency.
Figure D–1 User Entry Checks

Oracle Internet Directory Checks
Perform the following Oracle Internet Directory checks:

- Ensure that the `orclMailCreationStatus` attribute for each user entry is empty. This will be reported as a warning.

- `targetdn` attribute checks include:
  - Check that for every Oracle Mail user, the base user entry exists and also that the `mail` attribute of the base user is filled with an Oracle Collaboration Suite e-mail address
  - Ensure that the e-mail address of the Oracle Mail user is present in the user's base user entry mail attribute values

- When `orclMailDomainControlAci` for a user is set to `domain`, checks include:
  - Ensure that the `cn=DomainAdminsGroup` entry is referenced in `cn=MailStoreAdminsGroup uniquemember` attribute
  - Ensure that a domain administrator's DN is included in the `uniquemember` attribute of the `cn=DomainAdminsGroup` entry the administrator's domain
  - Ensure that a domain administrator's DN is included in the `uniquemember` attribute of the `cn=EmailAdminsGroup` entry

- `orclMailUserdlDN` attribute checks include ensuring that the entries present in the `orclMailUserdlDN` are all valid
■ orclMailStore attribute checks include checking the validity of the entry for the Oracle Collaboration Suite Database

■ DomainAdminsGroup entry checks include ensuring that all entries in the uniquemember attribute are valid and that orclMailDomainControlAci is set to domain

**Oracle Collaboration Suite Database Checks**
Check whether or not the user has a default Inbox folder in the database.

**Correction Details**
Perform the following corrections, as applicable:

■ Enter the Oracle Mail user’s e-mail address in the mail attribute if it is not present in the target DN’s mail attribute

■ Remove any inactive lists present in the orclMailUserdlDN attribute of an Oracle Mail user entry

**Distribution Lists**
High-level operations that can lead to distribution list inconsistencies include:
Archived distribution list without archive
Subscription information
Suspension information
Deleting a distribution list

*Figure D–2* shows which entries are checked as part of a distribution list inconsistency.
Oracle Internet Directory Checks

Perform the following Oracle Internet Directory checks:

- Ensure that `orclMailCreationStatus` attribute for each distribution list entry is empty
- `orclNewsGroupDn` attribute checks include ensuring that for each archived distribution list there is a corresponding newsgroup
- `uniqueMember` attribute checks include ensuring that the nested distribution lists associated with a distribution list are all present
- Suspension information checks include:
  - Ensure that the suspension information stored with the distribution list entries is all present
  - Because the subscription and suspension information is stored separately, ensure that no suspended entry should be subscribed
- `orclMailFolderDn` checks include ensuring that the folder exists in the system
- `orclMailParentDlDn` checks include ensuring that the values in the `orclMailParentDlDn` are valid entries
- `orclMailStore` checks include ensuring that the Oracle Collaboration Suite Database DN associated with each distribution list is valid
- `orclMailUserState` checks include checking the validity of the `orclMailUserState` attribute.

- `orclMailOwner` and owner attribute checks include:
  - If the `orclMailOwner` is set for a distribution list, ensure that the associated e-mail address is valid.
  - If the owner is set for a distribution list, ensure that the associated DN is valid and confirm that this is the target DN of the mailuser entry.

- Additional checks are done for the values of List Server distribution list attributes, including:
  - Check for the validity of the `orclMailGroupAdminMailid`.
  - Check the validity of the `orclMailGroupBounceMailId`.
  - Check the validity of the `orclMailGroupPostType`.
  - Ensure the `orclMailGroupIsSecure` attribute value is either true or false.
  - Ensure the `orclMailGroupArchiveOnly` attribute value is either true or false.
  - Ensure the `orclMailGroupAutoRespond` attribute value is either true or false.
  - Ensure the `orclMailGroupIsExternal` attribute value is either true or false.
  - Ensure the `orclMailGroupAutoReconfirm` attribute value is either true or false.

**Correction Details**

Perform the following corrections, as applicable:

- Remove the nonexistent distribution list DNs of a distribution list.
- Remove the incorrect suspension information DNs of a distribution list.

**Aliases**

Figure D–3 shows which entries are checked as part of an alias inconsistency.
**Oracle Internet Directory Checks**

Perform the following Oracle Internet Directory checks:

- `orclmailemail` attribute checks include:
  - Check the validity of the `orclmailemail` values for each alias
  - If the alias e-mail address is with a local domain, ensure that it exists in the user entries, else check in foreign entries

- `orclMailUserdlDN` attribute checks include ensuring that the distribution lists pointed to by this attribute are present in the system

**Correction Details**

Delete the alias entry if it is pointing to an invalid entry for its mail attribute.

**Foreign Users**

*Figure D–4* shows which entries are checked as part of a foreign user inconsistency.
Figure D–4 Foreign User Entry Checks

Oracle Internet Directory Checks

Perform the following Oracle Internet Directory checks:

- Ensure that every foreign user entry has at least one valid distribution list DN in the orclMailUserdlDN attribute
- Check for any foreign user entry with an empty orclMailUserdlDN attribute; it should be flagged for deletion

Correction Details

Delete the foreign user entries that are not part of any distribution list entries.

Processes

Figure D–5 shows which entries are checked as part of a process inconsistency.
Figure D–5  Process Entry Checks

Oracle Internet Directory Checks
Perform the following Oracle Internet Directory checks:

- Ensure that every process has a valid Oracle Collaboration Suite Database DN
- Ensure that the value of `localdomain` configured in the process entry is an existing domain
- Ensure that for every process instance the connection pool parameters are valid, meaning the value for minimum number connections is greater than zero and that the maximum number is greater than the minimum

Newsgroups
High-level operations leading to newsgroup inconsistencies include creating newsgroups.

Figure D–6 shows which entries are checked as part of a newsgroup inconsistency.


**Figure D–6  Newsgroup Entry Checks**

**Oracle Internet Directory Checks**

Perform the following Oracle Internet Directory checks:

- Ensure that every newsgroup entry in Oracle Internet Directory has the `orclMailNewsFolderCreateTime` attribute set
- Ensure that the `orclMailStoreDn` entry associated with each newsgroup exists
- Ensure that the `orclMailMailNNTPOutboundPeers` attribute has valid peer entries

**Oracle Collaboration Suite Database Checks**

Perform the following Oracle Collaboration Suite Database checks:

- Ensure that for every newsgroup entry in Oracle Internet Directory, the corresponding record in `es_folder` table is created
- Ensure that there are no orphan records in `es_folder` with user ID 119 (for newsgroups) and no matching Oracle Internet Directory entry

**Correction Details**

Remove all nonexistent peer entries that are part of outbound feed peers of a newsgroup.
News Peers

High-level operations leading to news peer inconsistencies include association with newsgroups, both on the inbound feed (accepted and rejected newsgroups) and on the outbound feed.

Figure D–7 shows which entries are checked as part of a newsgroup inconsistency.

**Figure D–7  News Peer Entry Checks**

Oracle Internet Directory Checks

Ensure that the newsgroup DN is stored in accepted and rejected newsgroup fields of every existing peer.

Correction Details

Remove any nonexistent outbound feeds and reject newsgroups present for a peer.

Shared Folders

High-level operations leading to shared folder inconsistencies include:

- Shared folder creation
- Shared folder subscriptions
Shared folder foreign key references for es_subs_folder
Shared folder renaming on subfolders
Shared folder ACI changes

Figure D–8 shows which entries are checked as part of a shared folder inconsistency.

**Figure D–8  Shared Folder Entry Checks**

---

**Oracle Internet Directory Checks**

Perform the following Oracle Internet Directory checks:

- Ensure there are no orphan shared folder entries in Oracle Internet Directory
- orclMailCreationStatus attribute checks include reporting a warning if this attribute is not empty
- orclMailStore attribute checks include ensuring that every shared folder entry has a mailstore attribute
- orclMailAci attribute checks include:
  - Ensure that the entries to which ACI has been granted exist and are in the same domain as the folder
  - For user and list grantees, ensure that the orclMailFolderGroupDN attribute contains the DN of the shared folder
- orclMailOwner checks include:
  - Ensure that the owner of every shared folder has an existing orclMailUser entry in the same domain as the folder
  - Ensure that the default_folder entries under each domain have the same mailstore DN as the shared folders

**Oracle Collaboration Suite Database Checks**
Perform the following Oracle Collaboration Suite Database checks:
- Ensure that every shared folder entry in Oracle Internet Directory has an entry in the es_folder entry of the Oracle Collaboration Suite Database specified
- Ensure that for every shared folder entry es_folder.flags is marked as 4 (shared)
- Ensure that every es_folder record with flags set to 4 (shared) has an LDAP entry as shared folder under the proper owner

**Correction Details**
There are no correction details for this release.

**Server-Side Rules**
High-level operations leading to server-side rule inconsistencies include:
Create Rule API
Modify Rule API
Delete Rule API

**Oracle Internet Directory Checks**
Ensure that for every rule in LDAP, a PL/SQL procedure exists in the appropriate Oracle Collaboration Suite Databases and is valid.

**Oracle Collaboration Suite Database Checks**
There are no Oracle Collaboration Suite Database checks for this release.

**Correction Details**
There are no correction details for this release.

**Policies and Filters**
The following Oracle Internet Directory checks are done for all filters that are available in the system:
- Filters must be applied to a direction instead of to a few services of a direction
- Ensure that process parameters and filters applied are in synchronization, meaning the value of the orclmailsmtpexternalfilter attribute should be true if a filter is applied
- Check the validity of the orclmailprocfilterprocguid attribute for each filter
- Check if any filter is applied to a service at instance level (this will issue a warning)
- Ensure that every filter applied to a direction has proper attributes
- Ensure file name correctness
- Ensure `orclmailprocfilterordernumber` correctness
- Ensure that the `orclmailmessagemodification` attribute has either true or false value
- Ensure that the `orclmailisenabled` attribute is true if it is applied to a direction
- Ensure `orclmailprocfilterlibrary` correctness

Private Address Books

High-level operations leading to private address book inconsistencies include:
Create private address book lists with existing lists
Modify private address book lists with existing lists

Figure D–9 shows which entries are checked as part of a private address book inconsistency.

**Figure D–9  Private Address Book Entry Checks**

**Oracle Internet Directory Checks**

Perform the following Oracle Internet Directory checks:
Ensure that every private address book list reference in uniquemember attribute is pointing to an existing list

Check that the owner of the address book exists; if not, delete any address book entries for nonexistent users

**Correction Details**
Perform the following corrections, as applicable:

- Remove inactive contacts in a list
- Remove inactive lists in a list
- Remove the address book entries if the owner does not exist

**oesutil**

This utility enables administrators to delete domains and to identify users who have exceeded a certain percentage of their mail quota. The utility prints the e-mail addresses of users who have exceeded the given percentage of their quota.

---

**Note:** In addition to the quota checking functionality of the oesutil utility, there is also a script, esd_check_quota_usage.pl, that provides the same functionality. The oesutil utility uses other constraints, however.

---

**See Also:** "esd_check_quota_usage.pl" on page D-48 for more information about this script

**Usage**

When deleting domains, use the following syntax:

```
% oesutil -v -delete_domain type=value domain=valid_domain installation=valid_installation_name
```

Following are brief explanations for each parameters:

- **-v:** Prints debug messages
- **-delete_domain:** Used when deleting domains
- **type:** Specify one of the following values, depending upon what is to be deleted from the domain
  - **user:** Deletes all users in a specified domain
  - **alias:** Deletes all aliases in a specified domain
  - **list:** Deletes all lists in a specified domain
  - **news:** Deletes all newsgroups in a specified domain
  - **all:** Deletes everything in a specified domain
- **domain:** Specify a valid domain.
- **installation:** A valid installation name to be used only when type=all

When checking mail quota, use the following syntax:

```
% oesutil -v -check_user_quota domain=valid_domain quota=number user=valid_username
```
Following are brief explanations for each parameters:

- `-v`: Prints debug messages
- `-check_user_quota`: Used when checking user quota
- `domain`: Specify a valid domain.
- `quota`: Specify a number greater than 1 and less than 100 signifying a percentage of quota used.
- `user`: Enter either the user ID or full e-mail of a valid user. Wildcard characters can be used.

**Examples**

The following examples illustrate deleting domains:

```bash
% oesutil -delete_domain type=user domain=edu
% oesutil -v -delete_domain type=list domain=com
% oesutil -delete_domain type=all domain=edu installation=um_system
% oesutil -delete_domain type=news domain=idc.oracle.com
```

The following examples illustrate checking user quota:

```bash
% oesutil -check_user_quota domain=us.oracle.com quota=50 user=hnatraja1@foo.com
% oesutil -check_user_quota domain=us.oracle.com quota=50 user=hnatraja1
% oesutil -check_user_quota domain=us.oracle.com quota=50 user="hnat*"
```

**esd_logscan.pl**

The `esd_logscan.pl` script, located in the `$ORACLE_HOME/oes/admin` directory, is provided to generate reports from the raw information in Oracle Mail server log files.

This script takes a search pattern as the first argument, followed by any number of Oracle Mail server log files. Each file is searched for the pattern, and wherever the pattern is found, the information from the log files is collated, sorted, and formatted for readability.

Any string can be used as a pattern. The pattern can be an e-mail message ID, a user name, an error code (such as ESSM-203), or a portion of the log message such as `message delivered`. Enclose multiword patterns in quotation marks. The period (.) character is a wildcard that matches any single character. For example, the pattern `a.c` will return `abc`, `acc`, `a9c`, and so on. Pattern match is not case-sensitive, so searching for `John.Doe` is the same as searching for `john.doe` or `JOHN.DOE`.

The script uses the execID information to find and collate the information in the log files. The execID is found on each line of a log file and is labeled with the field identifier `execid`. The execID is the same for all lines of the log file that are related to the same event, such as processing a given message.

The script generates reports that are grouped by the execID. Each section of the output is labeled with the corresponding execID. Within each section, the log information is sorted by time, making it easier to view messages generated a single thread of events. In the raw log files, the log messages generated by multiple threads are interleaved because many threads of activity run in parallel and are all logging simultaneously.

**Usage**

```bash
% perl $ORACLE_HOME/oes/admin/esd_logscan.pl pattern path_to_log_files
```
**Examples**

**Example D–2** shows the results of searching the log files for log messages with log message ID ESSM-213, which is a notification message logged when delivery fails. The SMTP outbound server is configured to log at the trace level, which logs more detail and will generate log information that may only be meaningful to Oracle Support and development engineers. This example shows that delivery failures were caused by the fact that the user’s Inbox was locked, a common occurrence that typically corrects itself with no action on the part of the administrator. As shown in the example, delivery was retried a number of times, and finally succeeded at 12:28:50.455 MDT.

**Note:** Oracle recommends using the version of Perl shipped with Oracle Collaboration Suite. To use this version on UNIX systems, set your `PATH` environment variable to have `$ORACLE_HOME/perl/bin` at the front, and set the UNIX environment variable `PERL5LIB` to `$ORACLE_HOME/perl/lib`.

---

**Example D–2  esd_logscan.pl Example**

```bash
% perl ORACLE_HOME/oes/admin/esd_logscan.pl essm-213 $ORACLE_HOME/oes/log/um_system/smtp_in/*/log*
```

<table>
<thead>
<tr>
<th>Date</th>
<th>Seq#</th>
<th>Component-#</th>
<th>Type</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/23/2005 12:26:37.283 MDT</td>
<td>1</td>
<td></td>
<td>trace</td>
<td>26650/26650.log.000:thread started</td>
</tr>
<tr>
<td>06/23/2005 12:26:37.843 MDT</td>
<td>2</td>
<td></td>
<td>trace</td>
<td>26650/26650.log.000:msg_id=107614342</td>
</tr>
<tr>
<td>06/23/2005 12:26:37.886 MDT</td>
<td>3</td>
<td></td>
<td>trace</td>
<td>26650/26650.log.000:return value=0</td>
</tr>
<tr>
<td>06/23/2005 12:26:37.891 MDT</td>
<td>4</td>
<td></td>
<td>trace</td>
<td>26650/26650.log.000:In essmo_insert_queue: msg_id=107614342 queue=3</td>
</tr>
<tr>
<td>06/23/2005 12:26:38.063 MDT</td>
<td>5</td>
<td></td>
<td>trace</td>
<td>26650/26650.log.000:return value=0</td>
</tr>
<tr>
<td>06/23/2005 12:26:38.063 MDT</td>
<td>6</td>
<td></td>
<td>trace</td>
<td>26650/26650.log.000:msg_id=107614342</td>
</tr>
<tr>
<td>06/23/2005 12:26:38.071 MDT</td>
<td>7</td>
<td></td>
<td>trace</td>
<td>26650/26650.log.000:return value=0</td>
</tr>
<tr>
<td>06/23/2005 12:26:38.071 MDT</td>
<td>8</td>
<td></td>
<td>trace</td>
<td>26650/26650.log.000:msg_id=107614342 queue=1</td>
</tr>
<tr>
<td>06/23/2005 12:26:38.076 MDT</td>
<td>9</td>
<td></td>
<td>trace</td>
<td>26650/26650.log.000:return value=0</td>
</tr>
<tr>
<td>06/23/2005 12:26:38.122 MDT</td>
<td>10</td>
<td>ESSM-258</td>
<td>notification</td>
<td>26650/26650.log.000:no system rules applied for the message: msg_id=107614342</td>
</tr>
<tr>
<td>06/23/2005 12:26:38.150 MDT</td>
<td>12</td>
<td>ESSM-205</td>
<td>internal_err</td>
<td>26650/26650.log.000:failed to deliver to user inbox: <a href="mailto:john.doe@foo.com">john.doe@foo.com</a></td>
</tr>
<tr>
<td>06/23/2005 12:26:38.150 MDT</td>
<td>13</td>
<td>ESSM-213</td>
<td>notification</td>
<td>26650/26650.log.000:local delivery failed for user: <a href="mailto:john.doe@foo.com">john.doe@foo.com</a></td>
</tr>
<tr>
<td>06/23/2005 12:26:38.156 MDT</td>
<td>14</td>
<td></td>
<td>trace</td>
<td>26650/26650.log.000:msg_id=107614342</td>
</tr>
</tbody>
</table>
This script, located in the $ORACLE_HOME/oes/admin directory, is for listing users who have reached a given percentage of their quotas, such as 90%. The result of running this script is an output file listing the users who have reached the specified percentage. The output file is given to another script that sends e-mail messages to the users warning them about their usage.
Usage

SQL> $ORACLE_HOME/oes/admin/esd_queue_examine.sql

esd_find_message.sql

This script, located in the $ORACLE_HOME/oes/admin directory, finds lost messages in the Oracle Collaboration Suite Database.

The messages searched are limited based on a time period when they were inserted into the database, or a user ID, or both.

Usage

SQL> $ORACLE_HOME/oes/admin/esd_find_message.sql
The script prompts for the following:

- The number of hours to go back in time (from the present time, UTC) to start the search. The default is 1, indicating the search time period begins at the current coordinated universal time (UTC) minus 1 hour. A value of 24 indicates the search time period begins at the current UTC minus 1 day. A value of 0 indicates the search is not limited by time.

- The number of hours to go back in time (from the present time, UTC) for the end of the time period. The default is 0, indicating present time, UTC. This value must be less than the hours entered for the search period start time.

- A user name associated with the account to search. The default is an empty string.

- A user name to restrict the search to messages in folders belonging to the user. This is optional when the hour entered for search period start time is greater than 0 but is required if the message search is not limited by time. A start time of 0, combined with an empty user name string will result in the search being performed on every message in the database.

- An optional sender substring.

- An optional recipient substring.

- An optional subject substring.

The input strings for sender, recipient, and subject are used to do case-insensitive substring matches. For example, entering a sender substring of rob returns all messages where the sender string contains any occurrence of rob, returning any messages by Robert, Robin, and ROBOT, for example.

---

**Caution:** Because the query criteria use columns that are not indexed, this script can be very expensive to run if a large number of messages is searched. Oracle recommends first running the script using the default time period, which searches messages inserted into the database within the past hour.

A query that returns too much data could cause performance problems, especially if the script is run at times of peak database load.

---

The script outputs to the console the message ID for each matching message found and also lists header information for each matching message, as shown in Example D–3.

**Example D–3**  

<table>
<thead>
<tr>
<th>MSG_ID</th>
<th>SENT</th>
<th>To</th>
<th>SENDER</th>
<th>SUBJECT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>03-MAY-05</td>
<td><a href="mailto:tuser1@us.foo.com">tuser1@us.foo.com</a></td>
<td><a href="mailto:jdoe@us.foo.com">jdoe@us.foo.com</a></td>
<td>Test Message - temime1.inp</td>
</tr>
<tr>
<td>1001</td>
<td>04-MAY-05</td>
<td><a href="mailto:tuser1@us.foo.com">tuser1@us.foo.com</a></td>
<td><a href="mailto:jdoe@us.foo.com">jdoe@us.foo.com</a></td>
<td>Test Message - temime10.inp</td>
</tr>
</tbody>
</table>

**esd_show_message.sql**

This script, located in the $ORACLE_HOME/oes/admin directory, displays message metadata including header, extended header, recipient, envelope, and shell information for the message and lists all folders containing the message.
**Note:** To view the message, use the `esd_copy_messages.sql` script to copy messages to a destination folder.

**See Also:** "esd_copy_messages.sql" on page D-53 for more information about this script

**Usage**

```sql
SQL> @?/oes/admin/esd_show_message.sql
```

The script prompts for a message ID.

**Example**

Example D–4 shows sample output for message ID 1283.

**Example D–4  esd_show_message.sql Output Example**

```
METADATA FOR MESSAGE ID 1283
=================================================================
MESSAGE HEADER DETAILS
======================
HEADER                VALUE
---------- --------------------------------------------------------------
Date: May 21 2005 12:30:21
From: tuser1 <tuser1@foo.com>
To: tuser2@foo.com
CC: tuser3@foo.com, tuser4@foo.com
Reply To: 
Subject: This is a test message
Int Date: May 21 2005 12:30:23
Msg Size: 1274
Msg ID: <428E811D.7070705@foo.com>
Sender: 
Ref: 
```

**MESSAGE EXTENSION HEADER DETAILS**

```
EXT_HEADER           VALUE
-------------------- ----------------------------------------------------------------------
Return-Path          <tuser1@foo.com>
Received             from desktop.foo.com by mailserver.acme.com with ESMTP id 1283116635422; Fri, 20 May 2005 17:30:22 -0700
User-Agent           Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.5.1) Gecko/20031223
X-Accept-Language    en-us, en
MIME-Version         1.0
Content-Type         multipart/alternative; boundary="------------0300010104060707030000606"
Content-Type         text/plain; charset=us-ascii; format=flowed
Content-Type         text/html; charset=us-ascii
```

**MESSAGE ENVELOPE DETAILS**

```
HEADER          VALUE
--------------- ----------------------------------------------------------------------
Note: To view the message, use the `esd_copy_messages.sql` script to copy messages to a destination folder.
See Also:   "esd_copy_messages.sql" on page D-53 for more information about this script
```
esd_show_message.sql

Received Date: May 21 2005 12:30:23
Peer Host: desktop.foo.com
Mail From: <tuser1@foo.com>

MESSAGE FOLDER DETAILS
========================
FOLDER_ID FOLDER_NAME
--------- --------------------------
1067 /tuser2/INBOX
1068 /tuser3/INBOX
1069 /tuser4/INBOX

MESSAGE RECIPIENTS DETAILS
============================
RECIPIENTS PARAMETER
----------- ---------------------
tuser2@us.foo.com

tuser3@us.foo.com

tuser4@us.foo.com

MESSAGE SHELL DETAILS
=========================
ORDER NO SHELL
---------- --------------------------
1 Return-Path: <tuser1@foo.com>
Received: from desktop.foo.com by mailserver.foo.com with ESMTP id 12831116635422; Fri, 20 May 2005 17:30:22 -0700
Message-ID: <428E811D.7070705@acme.com>
Date: Fri, 20 May 2005 17:30:21 -0700
From: tuser1 <tuser1@foo.com>
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.5.1) Gecko/20031223
X-Accept-Language: en-us, en
MIME-Version: 1.0
To: tuser2@foo.com
CC: tuser3@foo.com, tuser4@foo.com
Subject: This is a test message
Content-Type: multipart/alternative;
            boundary="------------030001010406070703000606"

This is a multi-part message in MIME format.
------------030001010406070703000606
Content-Type: text/plain; charset=us-ascii; format=floowed
Content-Transfer-Encoding: 7bit

!X-ORCL-BODY!: O:806 S:28 L:3 V:1
------------030001010406070703000606
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: 7bit

!X-ORCL-BODY!: O:952 S:279 L:12 V:2
------------030001010406070703000606--
**esd_copy_messages.sql**

This script, located in the `$ORACLE_HOME/oes/admin` directory, copies the targeted messages to a destination folder, the name of which the script takes as input. Once the message is in the destination folder, the administrator can use any existing client to view the message.

The script also takes all the same arguments as the `esd_find_message.sql` script and searches for the messages in the same manner. Once the messages are found, the copy script copies all of those messages into the destination folder.

**See Also:**  "esd_find_message.sql" on page D-49 for a list of arguments

**Note:** Copying a message does not mean a new copy is made. Instead, there is a single copy of the message to which many folders can have a pointer or a reference. Running the `esd_copy_messages.sql` script creates new references to existing messages.

The `esd_copy_messages.sql` script does not produce any output other than that to the destination folder.

**Usage**

```
SQL> @?/oes/admin/esd_copy_messages.sql
```

**esd_mail_queue.sql**

This script, located in the `$ORACLE_HOME/oes/admin` directory, first displays the possible queue choices to display and then prompts for a queue to list. If the administrator replies to the prompt with a specific queue, the script lists the current contents of that queue. If the administrator replies to the prompt by pressing the Enter key without giving a queue identifier, the script defaults to listing the submit queue.

Queue ID numbers used by `esd_mail_queue.sql` are as follows:

1: submit
2: relay
3: local
4: archive
5: List Server
6: NNTP
9: Housekeeper

In the report produced by `esd_mail_queue.sql`, first the total number of messages in the queue is given. Each message in the queue is then listed with the following information:

- **Message ID**: The ID used to uniquely identify the message within the database
- **Size**: The size, in bytes, of the message
- **Queue Time**: The time the message was inserted into the queue
- **Next Retry**: The next time delivery will be tried for a message that could not yet be delivered
- **Sender**: The sender of the message, truncated to the first 20 characters
Recipient: The recipient of the message, truncated to the first 20 characters

Subject: The subject of the message, truncated to the first 40 characters

If a message has multiple recipients, it will be listed multiple times. Each recipient of a message is listed on a separate line.

Messages are listed from most recent queue time to oldest queue time. The message at the end of the list has been in the queue for the largest amount of time.

The final section of the report lists all messages in the selected queue that are deferred and have a description explaining why they were deferred. For example, relay messages destined for a remote MTA can get deferred if the remote MTA was not accepting connections at the time relay delivery was last attempted. If there are no deferred messages in the selected queue, or if there are deferred messages but there is no explanation why they are deferred, the final section of the report is not generated.

The preceding description applies to all queues except the Housekeeper queue. Using esd_mail_queue.sql to check the Housekeeper queue lists three types of message records that are cleaned up by the Housekeeper, as shown in the following example:

Summary of Housekeeper Queues

Delivery Complete Queue has 4374 messages for cleanup
Pruning Queue has 415650 messages for cleanup
Collection Queue has 44033 messages for cleanup

esd_list_user_folders.sql

This script, located in the $ORACLE_HOME/oes/admin directory, lists folders for a specified user.

For each folder the script lists the folder ID and the name of the folder. Folders listed are sorted alphabetically by folder name. The output will also list the size of each folder in bytes and at the end it will list the total size in megabytes of all folders.

Usage

Run the script when connected as the ES_DIAG database user. The script takes a user name as input.

SQL> @?/oes/admin/esd_list_user_folders.sql username

esd_list_folder_messages.sql

This script, located in the $ORACLE_HOME/oes/admin directory, lists information for messages in a specified folder. For each message, the script lists the message ID, date, sender, size, and subject. Messages listed are sorted by date from oldest to newest.

Usage

Run the script when connected as the ES_DIAG database user. The script takes a folder name as input.

SQL> @?/oes/admin/esd_list_folder_messages.sql foldername

esd_list_unopened_inbox.sql

This script, located in the $ORACLE_HOME/oes/admin directory, detects user accounts that are not being accessed by checking whether the Inbox has been recently modified. User activity for an account modifies the user’s Inbox folder.
Usage
The script takes as input a number of days, \( N \), and lists Inbox folders that have a MODIFY_DATE earlier than SYSDATE-\( N \).

```
SQL> @?/oes/admin/esd_list_unopened_inbox.sql \( N \)
```

**esd_show_sessions.sql**

This script, located in the \$ORACLE_HOME/oes/admin directory, displays database session information for sessions connected as the ES_MAIL database user. These are sessions that originate from Oracle Mail servers, such as the IMAP server and the Housekeeper, as well as sessions that originate from Oracle Collaboration Suite Applications, such as Oracle WebMail.

The session information displayed by the script includes:

- The Applications tier hosts from which sessions originate
- The mail servers or applications that have opened the sessions
- The total number of sessions opened by Oracle Mail servers and applications on an Applications tier host
- The cumulative total number of sessions

SQL*Plus sessions, however, are not displayed, even if an administrator has used SQL*Plus to connect to the database using the ES_MAIL account.

Usage
The script takes no input.

```
SQL> @?/oes/admin/esd_show_sessions.sql
```

Example

*Example D–5* shows sample output for the esd_show_sessions.sql script, grouped by program and Applications tier host.

**Example D–5  Sample esd_show_sessions.sql Output**

<table>
<thead>
<tr>
<th>MACHINE</th>
<th>PROGRAM</th>
<th>SESSIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYDNEY-OVF\SYDNEY-OVF-1</td>
<td>java.exe</td>
<td>13</td>
</tr>
<tr>
<td>SYDNEY-OVF\SYDNEY-OVF-2</td>
<td>java.exe</td>
<td>13</td>
</tr>
<tr>
<td>beacon-rmdc</td>
<td>emagent@beacon-rmdc (TNS V1-V3)</td>
<td>2</td>
</tr>
<tr>
<td>rmgm103</td>
<td>imap</td>
<td>189</td>
</tr>
<tr>
<td></td>
<td>smtp_out</td>
<td>32</td>
</tr>
<tr>
<td></td>
<td>listservar</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>smtp_in</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>housekeeper</td>
<td>8</td>
</tr>
<tr>
<td>web218</td>
<td>java@rmgm103 (TNS V1-V3)</td>
<td>1</td>
</tr>
<tr>
<td>web218.acme.com</td>
<td>? @web218 (TNS V1-V3)</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>JDBC Thin Client</td>
<td>32</td>
</tr>
</tbody>
</table>

Total Sessions

---------
319
esd_show_session_usage.sql

This script accepts optional input that can restrict which Applications tier hosts and which programs are included in the report. In a large deployment with many Applications tier hosts, restricting the report to a single host at a time is recommended because the script will take less time to run.

The Applications tier host name, if entered, is used as an exact match to restrict the output. Run the esd_show_sessions.sql script to see all Applications tier host names.

See Also: "esd_show_sessions.sql" on page D-55 for script usage information

The program name, if entered, can include the % character for a SQL pattern match. Names such as listserver and imap can also be entered. If the program name is entered and is not one of the friendly names, the % character will be appended by the script. For example, entering es as the program name will search for all sessions in the database session table that match es% in the PROGRAM column.

This script assists in determining the usage of the connection pool. Using this information, helps administrators to determine whether they can safely decrease the minimum Oracle Collaboration Suite Database connection pool size. This information cannot, by itself, be used to determine if the connection pool size should be decreased, however, as the efficiency and remaining resource capacity must be considered.

This script can also be used to determine if there are excessive numbers of idle sessions. An idle session is supposed to be closed after it has been idle for a specified period of time determined by the Oracle Collaboration Suite Database connection pool settings.

This script reports all the database connections by tier and Oracle Mail server, and their usage. The first column lists the Applications tier host name. The second column lists the server, such as smtp_in (the SMTP inbound server). The third column lists the total number of database sessions from those servers. The fourth column, SESSIONS95, lists the first X sessions that account for 95% of all work.

The database connection load balancing algorithm for Oracle Mail servers is not round robin but on a first come basis. The server will always try to use connection #1; if #1 is busy, #2, and so on. The number in the SESSIONS95 column reports that 95% of all requests are handled by the first X connections. In the case of imap in Example D-6, the first 43 sessions have accounted for 95% of all work, which means there are many hardly used or unused connections from 44-180.

Usage

The esd_show_session_usage.sql script accepts Applications tier host names and program names as optional input.

SQL> @?/oes/admin/esd_show_session_usage.sql

When prompted, enter the Applications tier host name and the program name. If no information is entered at either of these two prompts, press Enter to list all Applications tier hosts and programs, respectively.
Note: This script shows only sessions that are doing mail-related processing. Oracle Mail server instances can have additional sessions that are performing administrative tasks. These sessions are not affected by the database connection pool settings and so are not shown in the results.

Example D–6  Sample esd_show_session_usage.sql Output

<table>
<thead>
<tr>
<th>MACHINE</th>
<th>PROGRAM</th>
<th>SESSIONS</th>
<th>SESSIONS95</th>
</tr>
</thead>
<tbody>
<tr>
<td>rgmum103</td>
<td>imap</td>
<td>180</td>
<td>43</td>
</tr>
<tr>
<td></td>
<td>smtp_out</td>
<td>30</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>listsserver</td>
<td>12</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>smtp_in</td>
<td>10</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>housekeeper</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>java@rgmum103 (TNS V1-V3)</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

utillockt.sql

This script, located in the $ORACLE_HOME/rdbms/admin directory, prints the sessions in the system that are waiting for locks, and the locks for which they are waiting.

See Also: Chapter 2, "SQL Processing for Application Developers" in Oracle Database Application Developer’s Guide - Fundamentals
This appendix lists the request for comments (RFCs) that are supported by Oracle Mail in Table E–1.

<table>
<thead>
<tr>
<th>RFC Number</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 850</td>
<td>Standard for Interchange of USENET Messages</td>
</tr>
<tr>
<td>RFC 0977</td>
<td>Network News Transfer Protocol</td>
</tr>
<tr>
<td>RFC 1034</td>
<td>Domain Names - Concepts and Facilities</td>
</tr>
<tr>
<td>RFC 1035</td>
<td>Domain Names - Implementation and Specification</td>
</tr>
<tr>
<td>RFC 1036</td>
<td>Standard for Interchange of USENET Messages</td>
</tr>
<tr>
<td>RFC 1123</td>
<td>Requirements for Internet hosts - application and support</td>
</tr>
<tr>
<td>RFC 1652</td>
<td>SMTP Service Extension for 8bit-MIME transport</td>
</tr>
<tr>
<td>RFC 1869</td>
<td>SMTP Service Extensions</td>
</tr>
<tr>
<td>RFC 1870</td>
<td>SMTP Service Extension for Message Size Declaration</td>
</tr>
<tr>
<td>RFC 1891</td>
<td>SMTP Service Extension for Delivery Status Notifications</td>
</tr>
<tr>
<td>RFC 1893</td>
<td>Enhanced Mail System Status Codes</td>
</tr>
<tr>
<td>RFC 1894</td>
<td>An Extensible Message Format for Delivery Status Notifications (DSNs)</td>
</tr>
<tr>
<td>RFC 1939</td>
<td>Post Office Protocol - Version 3</td>
</tr>
<tr>
<td>RFC 2034</td>
<td>SMTP Service Extension for Returning Enhanced Error Codes</td>
</tr>
<tr>
<td>RFC 2045</td>
<td>MIME Part 1: Format of Internet Message Bodies</td>
</tr>
<tr>
<td>RFC 2046</td>
<td>MIME Part 2: Media Types</td>
</tr>
<tr>
<td>RFC 2047</td>
<td>MIME Part 3: Message Header Extensions for Non-ASCII Text</td>
</tr>
<tr>
<td>RFC 2048</td>
<td>MIME Part 4: Registration Procedures</td>
</tr>
<tr>
<td>RFC 2049</td>
<td>MIME Part 5: Conformance Criteria and Examples</td>
</tr>
<tr>
<td>RFC 2060</td>
<td>Internet Message Access Protocol - Version 4rev1</td>
</tr>
<tr>
<td>RFC 2086</td>
<td>IMAP ACL extension</td>
</tr>
<tr>
<td>RFC 2087</td>
<td>IMAP QUOTA extension</td>
</tr>
<tr>
<td>RFC 2088</td>
<td>IMAP nonsynchronous literals</td>
</tr>
<tr>
<td>RFC 2177</td>
<td>IMAP IDLE command</td>
</tr>
<tr>
<td>RFC Number</td>
<td>Title</td>
</tr>
<tr>
<td>------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>RFC 2342</td>
<td>IMAP Namespace</td>
</tr>
<tr>
<td>RFC 2821</td>
<td>Simple Mail Transfer Protocol (a more recent version of RFC 821)</td>
</tr>
<tr>
<td>RFC 2822</td>
<td>Standard for the format of ARPA Internet text messages (a more recent version of RFC 822)</td>
</tr>
<tr>
<td>RFC 2859</td>
<td>IMAP UIDPLUS extension</td>
</tr>
<tr>
<td>RFC 2980</td>
<td>Common NNTP Extensions</td>
</tr>
<tr>
<td>RFC 3463</td>
<td>Enhanced Mail System Status Codes (obsoletes RFC 1893)</td>
</tr>
</tbody>
</table>
Oracle Mail Server Parameters and Log Files

This appendix provides server and debug level parameter definitions for the Oracle Mail servers, in addition to log file locations.

The Oracle Mail servers can be accessed through the Application Server Control Console for Collaboration Suite.

**See Also:** Chapter 1, "Introduction to Oracle Mail Administration" for information about accessing the Application Server Control Console for Collaboration Suite

### Oracle Mail Server Parameter Definitions

The parameters listed in this section can be displayed by clicking either the instance in the **Instance** column on a particular server home page, or the **Default Settings** link in the **Target** section on the same page.

In most cases, set parameters at the target level on the Default Settings page. Because the use of multiple server instances, each configured in different ways, can be confusing to manage (and separate instances configured differently can directly contradict each other), managing server parameter settings at the target level maintains one source of truth for the various server instances.

In the case of the Housekeeper and SMTP outbound servers, however, managing server instance parameters at the instance level is required when using multiple instances of these servers.

**See Also:**

- "Housekeeper Server" on page 3-23 for more information about multiple instances of the Housekeeper server
- "Enabling Message Archiving" on page 8-29 for more information about creating an additional instance of the SMTP outbound server

Clicking the instance displays the settings for that particular process instance of the server. Clicking **Default Settings** displays the default values for the settings. The default settings apply to any newly created server process instance and can be changed, as necessary, by the administrator. After editing the default settings, click **Apply** to apply the changes or **Revert** to reset the default settings to the factory defaults.

Table F–1 and Table F–2 list LDAP connection pool and LDAP connection retry parameters, respectively, that are common to all servers except for Housekeeper and Virus Scrubber.
This section lists and discusses parameter settings for the following Oracle Mail servers:

- Oracle Mail Housekeeper
- Oracle Mail IMAP Server
- Oracle Mail NNTP Inbound Server
- Oracle Mail NNTP Outbound Server
- Oracle Mail POP Server
- Oracle Mail Virus Scrubber
- Oracle Mail List Server
- Oracle Mail SMTP Inbound Server
- Oracle Mail SMTP Outbound Server

### Oracle Mail Housekeeper

This section lists the instance setting and debug parameter definitions for the Oracle Mail Housekeeper process. It contains the following topics:

- Oracle Mail Housekeeper Instance Setting Parameters
- Oracle Mail Housekeeper Debug Parameters
Oracle Mail Housekeeper Instance Setting Parameters

In the Mail Collaboration Suite Database section, the Collaboration Suite Database list displays available Oracle Collaboration Suite Databases.

In the Thread Parameters section, the number in the Concurrency Level field sets the degree of parallelism that a process should use when running the configured tasks. For example, if this number is set to 10, the process runs 10 threads of the task, concurrently, increasing throughput. The default value is 10.

Table F–3 lists descriptions of the parameters in the Housekeeping Operations section.

<table>
<thead>
<tr>
<th>Table F–3</th>
<th>Housekeeping Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>Option</td>
</tr>
<tr>
<td>Operation Mode</td>
<td>None, Statistics Cleanup, Process Control Message Cleanup, or Tertiary Store</td>
</tr>
<tr>
<td>Expiration</td>
<td>Enabled or Disabled</td>
</tr>
<tr>
<td>Pruning</td>
<td>Enabled or Disabled</td>
</tr>
<tr>
<td>Collection</td>
<td>Enabled or Disabled</td>
</tr>
<tr>
<td>Statistics Cleanup</td>
<td>Enabled or Disabled</td>
</tr>
<tr>
<td>Process Control Message Cleanup</td>
<td>Enabled or Disabled</td>
</tr>
<tr>
<td>Tertiary Store</td>
<td>Enabled or Disabled</td>
</tr>
<tr>
<td>Text Synchronization</td>
<td>Enabled or Disabled</td>
</tr>
<tr>
<td>Text Optimization</td>
<td>Enabled or Disabled</td>
</tr>
</tbody>
</table>

Table F–4 lists descriptions for the parameters in the General Parameters section.
### Table F–4  Housekeeper General Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency of Execution of Housekeeper Process</td>
<td>Enter a nonnegative number</td>
<td>Number of minutes between two consecutive starts of the Housekeeper process. If the task finishes before the time allotted, the Housekeeper process sleeps for the duration. If the task takes more than the allotted time, the process does not sleep but instead runs continuously. The default value is 60.</td>
</tr>
<tr>
<td>Age Threshold</td>
<td>Enter a nonnegative number</td>
<td>Number of days, minimum, before messages are archived. If the Tertiary Store task is enabled, the Housekeeper tries to archive messages older than this parameter. Oracle recommends setting at least 30. The default value is 30.</td>
</tr>
</tbody>
</table>
| Run Task                           | On Demand or At Periodic Intervals | - On Demand: The server will start in an idle mode and wait for task commands from the opmn console. No tasks will be performed until a command is received.  
- At Periodic Intervals: The server will start processing the configured tasks immediately upon startup and subsequently perform the tasks at periodic intervals. |
| Index Optimization Level           | Fast, Full, or Rebuild        | - Fast: Fastest option to optimize text search performance. It does not remove data no longer needed in the index.  
- Full: The same optimization method used in Fast mode plus deleting of obsolete data in the index. It is the default and recommended option in most cases.  
- Rebuild: |
| Index Optimization Max Time (hours)| Enter a nonnegative number    | Determines how long the index optimization task runs continuously. Optimization requires CPU resources and may be scheduled during off hours. If the task does not finish by the end of the allotted time, the task stops until the next period. The default value is 1. |
| Support Log Miner Recovery         | Enabled or Disabled           | If Enabled, keeps the deleted message in redo logs, so that the LogMiner-based recovery feature can be enabled. It can also slow down the Housekeeper process Collection task. The default value is Disabled. |
Oracle Mail Housekeeper Debug Parameters

When debug parameters are enabled, more analysis data is included in the log file, depending upon the level set in the Process Log Level parameter of the General Parameters section. The Housekeeper process log file is located in the $ORACLE_HOME/oes/log/um_system/gc directory.

Table F–5 lists the descriptions of the Housekeeper debug parameters.

### Table F–4 (Cont.) Housekeeper General Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Log Level</td>
<td>Internal Error,</td>
<td>Determines the level of detail the server writes to the log file, as follows:</td>
</tr>
<tr>
<td></td>
<td>Error, Warning,</td>
<td>■ Internal Error: internal errors only: Administrator should file a bug with Oracle Support.</td>
</tr>
<tr>
<td></td>
<td>Notification, Trace, Dump</td>
<td>■ Error: all information included in Internal Error plus regular errors: Error condition exists and must be corrected by administrator.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Warning: everything up to Error plus warnings: Conditions exist that may require attention.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Notification: everything up to Warning plus Notification: An informational message only, no additional action needed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Levels beyond Notification are intended for Oracle Support to analyze a defect situation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Trace: everything up to Notification plus trace logs: Program traces that aid support debugging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Dump: everything up to Trace, in addition to printing information from the program to aid in analyzing a problem. Extended debugging information that can aid debugging</td>
</tr>
<tr>
<td>Maximum Log Size (MB)</td>
<td>Enter a nonnegative number</td>
<td>Determines how big a log file can grow before the server writes to a new log file. The default value is 5.</td>
</tr>
<tr>
<td>Maximum Number of Log Files</td>
<td>Enter a nonnegative number</td>
<td>If the number of log files for an IMAP server instance reaches this limit, no new log files will be generated. The existing log files will be written to in rotation. The default value is 10.</td>
</tr>
</tbody>
</table>

See Also: "Log Files" on page 3-3 for more information about log files
This section lists the instance setting, debug parameter, and Oracle Collaboration Suite Database connection parameter definitions for the Oracle Mail IMAP server process. It contains the following topics:

- Oracle Mail IMAP Server Instance Setting Parameters
- Oracle Mail IMAP Server Debug Parameters
- Oracle Mail IMAP Oracle Collaboration Suite Database Connection Parameters

Oracle Mail IMAP Server Instance Setting Parameters

In the Mail Collaboration Suite Database section are two lists showing available Oracle Collaboration Suite Databases and Oracle Collaboration Suite Databases currently being serviced.

Available Collaboration Suite Database(s) is the list of all the mail-enabled Oracle Collaboration Suite Databases in the system to which servers can potentially connect.

Collaboration Suite Database(s) currently being serviced lists Oracle Collaboration Suite Databases to which the IMAP server will connect, and serve requests from e-mail users who have mailboxes on any of the nodes in the list. Additionally, access to shared and public folders is limited to these Oracle Collaboration Suite Databases through this IMAP instance.

The LDAP connection pool is a pool of open connections to Oracle Internet Directory. Table F–1 lists the descriptions of the parameters in the LDAP Connection Pool Parameters section.

Table F–2 lists the descriptions of the parameters in the LDAP Connection Retry Parameters section.

Thread parameters control the behavior of the worker thread pool in protocol servers. Each request from a client is serviced by one of the threads form the worker pool. While a thread is servicing a request, it is considered busy and cannot service any more requests until the current one is complete.

Table F–6 lists descriptions of the parameters in the Thread Parameters section.

---

Table F–5 Housekeeper Debug Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Queue Cleanup</td>
<td>Enabled or Disabled</td>
<td>If Enabled, cleans up accumulated data generated from process control consoles. Administrators control the startup, shutdown, or statistics inquiry of server processes by using administration consoles, such as Oracle Enterprise Manager 10g Grid Control Console, that interact with server processes by sending and receiving notification messages against the server process. Oracle recommends that at least one instance of Housekeeper is configured with this parameter enabled for each Oracle Collaboration Suite Database. The default value is Disabled.</td>
</tr>
<tr>
<td>Statistics Logging</td>
<td>Enabled or Disabled</td>
<td>If Enabled, process statistics are logged to the level set in the Process Log Level parameter (subject to a minimum level of 25). The default value is Disabled.</td>
</tr>
<tr>
<td>LDAP (DS) Call Tracing/Logging</td>
<td>Enabled or Disabled</td>
<td>If Enabled, writes an internal debug log for any calls made to Oracle Internet Directory. The default value is Disabled.</td>
</tr>
</tbody>
</table>
Table F–6  IMAP Thread Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeout (seconds)</td>
<td>0–65535</td>
<td>Number of seconds a thread is idle before it is removed from the pool. The default is 1860.</td>
</tr>
<tr>
<td>Increment</td>
<td>1–999</td>
<td>Number of Oracle Internet Directory connections to be added to the pool when the existing connections in the pool are exhausted, to the limit of the Maximum parameter value. The default value is 1.</td>
</tr>
<tr>
<td>Minimum</td>
<td>Enter a nonnegative number</td>
<td>Number of Oracle Internet Directory connections in the pool at startup. The default value is 1.</td>
</tr>
<tr>
<td>Maximum</td>
<td>Enter a nonnegative number</td>
<td>Maximum number of Oracle Internet Directory connections in the pool not to be exceeded. The default value is 20.</td>
</tr>
</tbody>
</table>

Table F–7 lists descriptions for the parameters in the Shared Message Flags section.

See Also: RFC3501 and RFC3503 on the Internet for further information about the flags listed in the following table

Table F–7  IMAP Shared Message Flags

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Seen Messages</td>
<td>Enabled or Disabled</td>
<td>When enabled, shows that messages have been read.</td>
</tr>
<tr>
<td>Flagged Messages</td>
<td>Enabled or Disabled</td>
<td>When enabled, shows that messages have been flagged for urgent or special attention.</td>
</tr>
<tr>
<td>Answered Messages</td>
<td>Enabled or Disabled</td>
<td>When enabled, shows that messages have been answered.</td>
</tr>
<tr>
<td>Deleted Messages</td>
<td>Enabled or Disabled</td>
<td>When enabled, shows that messages have been deleted for removal by a later expunge operation.</td>
</tr>
<tr>
<td>Draft Messages</td>
<td>Enabled or Disabled</td>
<td>When enabled, shows that messages have not completed composition and will be marked as a draft.</td>
</tr>
</tbody>
</table>

Table F–8 lists descriptions for parameters in the Rules and Routing Control Parameters section.
Table F–8  IMAP Rules and Routing Control Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spam Flood Interval (Minutes)</td>
<td>Enter a nonnegative number</td>
<td>Number of minutes used to detect spam flooding. The default value is 10.</td>
</tr>
<tr>
<td>Spam Maximum Flood Count</td>
<td>Enter a nonnegative number</td>
<td>SMTP server signals flooding if the number of messages and connections from a single host exceeds the value of this parameter within the Spam Flood Interval. The default value is 40.</td>
</tr>
</tbody>
</table>

Table F–9 lists descriptions for the parameters in the General Parameters section.

Table F–9  IMAP General Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Presentation Name</td>
<td>Custom, IMAP, or IMAPSSL</td>
<td>The name of the IMAP service in the listener configuration file. Selecting Custom enables you to specify the presentation name. The default is IMAP. IMAPSSL is for encrypted connections over SSL.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: When this parameter’s default value is changed, you must change the listener configuration to the same value.</td>
</tr>
<tr>
<td>Custom Name</td>
<td>String</td>
<td>Enables you to choose a custom name for the IMAP service. Applies only if the Presentation Name is set to Custom. If nothing is entered in this field, the default is Custom.</td>
</tr>
<tr>
<td>SSL Enabled</td>
<td>True or False</td>
<td>Applies only if Presentation Name is set to Custom.</td>
</tr>
<tr>
<td>Debug User</td>
<td>User ID without domain</td>
<td>Name of a user about whom more debug information will be put in the log files by the server.</td>
</tr>
<tr>
<td>Maximum size of shell</td>
<td>Enter a nonnegative number</td>
<td>The shell comprises all the headers of the MIME parts in the message. Maximum size of shell, in bytes, for a message allowed to be saved on the server. The default value is 1000000.</td>
</tr>
<tr>
<td>Maximum Number of Headers Allowed in a Message</td>
<td>Enter a nonnegative number</td>
<td>The maximum number of headers allowed in a single message that can be saved on the server. The default value is 1000.</td>
</tr>
<tr>
<td>Default Domain</td>
<td>String</td>
<td>Domain used if a user logging in does not provide a domain. The default is set during installation and can be changed any time thereafter.</td>
</tr>
<tr>
<td>Maximum Number of Clients</td>
<td>0–1000</td>
<td>Maximum number of clients allowed to connect to each server instance simultaneously. The default value is 1000.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter a nonnegative, nonzero number</td>
<td>The port on which the listener listens for the IMAP service. The default value is 143. Note: When the port value in the listener configuration for this server is changed, it is recommended that this parameter’s value be set to the same value.</td>
</tr>
<tr>
<td>Allow Admin to Access Any Account</td>
<td>True or False</td>
<td>If True, this feature enables administrators to access any user account using IMAP in the same manner as an actual user. To use this feature, administrators must change their user ID in the IMAP client to include the user ID of the user they want to proxy in as, beginning with #SU. For example, an administrator with user ID <a href="mailto:admin1@foo.com">admin1@foo.com</a> can proxy in as <a href="mailto:user1@foo.com">user1@foo.com</a> by changing the user ID to <a href="mailto:admin1@foo.com">admin1@foo.com</a>#<a href="mailto:SUuser1@foo.com">SUuser1@foo.com</a>.</td>
</tr>
</tbody>
</table>
**Oracle Mail Server Parameter Definitions**

### Table F–9  (Cont.) IMAP General Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Clear Text Login</td>
<td>True or False</td>
<td>If True, enables the LOGIN command and insecure SASL authentication mechanisms, PLAIN and LOGIN, that transmit the password in plain text. If False, the SASL Authentication parameter must be enabled or the Support STARTTLS Command parameter must be set to True in order to log in to the IMAP server and prevent password snooping.</td>
</tr>
<tr>
<td>Cache Size</td>
<td>Small or Medium</td>
<td>Caching level. When Small, no mail information is cached in the IMAP server. When Medium, certain parts of mail are cached. Increasing the cache size increases the memory requirements on the Applications tier. The default value is Small.</td>
</tr>
<tr>
<td>Protocol Banner</td>
<td>String</td>
<td>This parameter determines the message that the server sends when accepting new incoming client requests. The text of this parameter must be encoded in US-ASCII. The following macros are also permitted and will be applied to all IMAP servers on the particular Applications tier:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <code>%s</code> (server type)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <code>%h</code> (host name)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <code>%v</code> (version information)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default value is Server Ready. Note: Any value entered in this field is also entered in the Protocol Banner parameter of all protocol servers.</td>
</tr>
<tr>
<td>Maximum Message Size (KB)</td>
<td>Enter a nonnegative number</td>
<td>Maximum message size allowed to be saved to the server. The default value of 0 denotes unlimited size.</td>
</tr>
<tr>
<td>New Mail Poll Interval (seconds)</td>
<td>0-65535</td>
<td>Number of seconds the IMAP server waits before checking for new mail. Large numbers of check new mail requests from clients affect performance. The default value is 120.</td>
</tr>
<tr>
<td>Session Timeout (seconds)</td>
<td>0-65535</td>
<td>Number of seconds for the auto-logout timeout interval. If no client operations occur in this time, the client is disconnected. The default value is 1800.</td>
</tr>
<tr>
<td>Public Folder Caching</td>
<td>Disabled, Cache Once, and Enabled</td>
<td>Defines the frequency at which the IMAP server caches the public folder list and refreshes it from Oracle Internet Directory. Alternatively, enter one of the following values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Disabled to disable caching and get a current listing from Oracle Internet Directory for every client request. Use this if your public folder hierarchy is dynamic and it is critical for users to see the changes immediately. The Oracle Internet Directory server must have spare cycles.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Cache Once to cache once on first request and never refresh. This list is used for the lifetime of the server. Use this setting if your public folder hierarchy is mostly static and it is not critical for users to see the changes, immediately. You must bounce the IMAP server for IMAP users to see any changes in the public folder hierarchy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Enabled: After selecting this option, enter a positive number in the Public Folder Cache Refresh Interval (minutes) parameter if the public folder hierarchy does not change frequently, and it is acceptable for users to wait for this number of minutes to see new changes to the public folder hierarchy and permissions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default value is Enabled.</td>
</tr>
</tbody>
</table>

Oracle Mail Server Parameters and Log Files  F-9
### Table F–9  (Cont.) IMAP General Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Public Folder Cache Refresh Interval (minutes)| Enter a nonnegative number, -1 or 0 | Enter the refresh interval in minutes if you enabled Public Folder Caching. The default value is 30.  
**Note:** Setting this parameter to -1 places a larger load on the Oracle Internet Directory server, which can affect performance. |
| Password Change Allowed                       | False, True, or Using SSL only | If False, users cannot change passwords using IMAP. If True, all users can change passwords using IMAP. If Using SSL only, users can change passwords only when connected to IMAP using SSL.  
The default value is Using SSL only. |
| SASL Protection                                | None, Integrity, or Confidentiality | Applicable only to server-to-server communication within local servers (using the XAUTH command).  
- None: Password authentication only is protected during communication  
- Integrity: Adds integrity checking (to detect tampering of the communication)  
- Confidentiality: The communication is encrypted (and also implies Integrity)  
The default value is None. |
| SASL Authentication                            | Enabled or Disabled            | If Enabled, SASL authentication is permitted. The default value is Disabled. |
| Support STARTTLS Command                       | True or False                  | For this parameter to be enabled, a wallet location must be specified in the Wallet Location for TLS Support parameter. The default value is True. |
| Wallet Location for TLS Support                | Directory path                 | Enter file: followed by the absolute path to the directory in which the SSL wallet is located. It is only relevant if the Support STARTTLS Command is True.  
for example file:/directory_path |
| Process Log Level                              | Internal Error, Error, Warning, Notification, Trace, Dump | Determines the level of detail the server writes to the log file, as follows:  
- Internal Error: internal errors only: Administrator should file a bug with Oracle Support  
- Error: all information included in Internal Error plus regular errors: Error condition exists and must be corrected by administrator  
- Warning: everything up to Error plus warnings: Conditions exist that may require attention  
- Notification: everything up to Warning plus Notification: An informational message only, no additional action needed  
Levels beyond Notification are intended for Oracle Support to analyze a defect situation.  
- Trace: everything up to Notification plus trace logs: Program traces that aid support debugging  
- Dump: everything up to Trace, in addition to printing information from the program to aid in analyzing a problem. Extended debugging information that can aid debugging  
The default value is Warning. |
Oracle Mail IMAP Server Debug Parameters

When debug parameters are enabled, more analysis data is included in the log file, depending upon the level set in the Process Log Level parameter of the General Parameters section.

**Note:** Enable these parameters as directed by Oracle Support. Information generated by enabling in these parameters is for use by Oracle Support only.

The IMAP process log file is located in the $ORACLE_HOME/oes/log/um_system/imap directory.

Table F–10 lists the descriptions of the IMAP debug parameters.

### Table F–9 (Cont.) IMAP General Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Log Size (MB)</td>
<td>Enter a nonnegative number</td>
<td>Determines how big a log file can grow before the server writes to a new log file. The default value is 5. See Also: &quot;Log Files&quot; on page 3-3 for more information about log files.</td>
</tr>
<tr>
<td>Maximum Number of Log Files</td>
<td>Enter a nonnegative number</td>
<td>Maximum number of log files for an IMAP server instance. The default value is 10. See Also: &quot;Log Files&quot; on page 3-3 for more information about log files.</td>
</tr>
<tr>
<td>Process Flags</td>
<td>-wb, -fsf, -uato=120, or -cbl=12</td>
<td>These are special flags that can be passed to the IMAP server to change the behavior. Each flag must be on its own line. -wb: Enables wastebasket functionality so that all deleted mails are moved to a folder called WasteBasket. Mails in WasteBasket still count toward user quota. -fsf: Speeds shared folder access by not searching for folders shared with distribution lists. -uato=120: Defines the time (in seconds) before an unauthenticated IMAP connection should be dropped and closed. As each connection counts toward the maximum limit of connections and consumes resources on the server side, this flag, in conjunction with -cbl, removes suspicious connections from the server as quickly as possible. -cbl=12: Defines how many commands the server will accept before the user is authenticated.</td>
</tr>
</tbody>
</table>

### Oracle Mail IMAP Server Debug Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Connections</td>
<td>Enabled or Disabled</td>
<td>If Enabled, writes an internal debug log for database connections. The default value is Disabled.</td>
</tr>
<tr>
<td>Folder Open</td>
<td>Enabled or Disabled</td>
<td>If Enabled, writes an internal debug log for the folder open function. The default value is Disabled.</td>
</tr>
<tr>
<td>Start/End of Client Requests</td>
<td>Enabled or Disabled</td>
<td>If Enabled, writes an internal debug log for client requests. The default value is Disabled.</td>
</tr>
<tr>
<td>I/O Between IMAP Server and Clients</td>
<td>Enabled or Disabled</td>
<td>If Enabled, writes an internal debug log for I/O between the IMAP server and clients. The default value is Disabled.</td>
</tr>
</tbody>
</table>

Table F–10 IMAP Debug Parameters
Oracle Mail IMAP Oracle Collaboration Suite Database Connection Parameters

*Table 3–1 on page 3-2 lists descriptions of parameters for open connections to the Oracle Collaboration Suite Database.*

Oracle Mail NNTP Inbound Server

This section lists the instance setting, debug parameter, and Oracle Collaboration Suite Database connection parameter definitions for the Oracle Mail NNTP inbound server process. It contains the following topics:

- **Oracle Mail NNTP Inbound Server Instance Setting Parameters**
- **Oracle Mail NNTP Inbound Server Debug Parameters**
- **Oracle Mail NNTP Inbound Oracle Collaboration Suite Database Connection Parameters**

Oracle Mail NNTP Inbound Server Instance Setting Parameters

In the News Collaboration Suite Database section are two lists showing available news Oracle Collaboration Suite Databases and news Oracle Collaboration Suite Databases currently being serviced.

**Available Collaboration Suite Database(s)** is the list of all the news-enabled Oracle Collaboration Suite Databases in the system to which servers can potentially connect.

**Collaboration Suite Database(s) currently being serviced** lists Oracle Collaboration Suite Databases to which the NNTP server will connect.

The LDAP connection pool is a pool of open connections to Oracle Internet Directory. *Table F–1* lists descriptions for parameters in the LDAP Connection Pool Parameters section. *Table F–2* lists descriptions for the parameters in the LDAP Connection Retry Parameters section. *Table F–11* lists descriptions for parameters in the Thread Parameters section.

---

**Table F–10 (Cont.) IMAP Debug Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Logins</td>
<td>Enabled or Disabled</td>
<td>If Enabled, writes an internal debug log for client logins. The default value is Disabled.</td>
</tr>
<tr>
<td>Memory Management</td>
<td>Enabled or Disabled</td>
<td>If Enabled, writes an internal debug log for memory management. The default value is Disabled.</td>
</tr>
<tr>
<td>Folder Synchronization</td>
<td>Enabled or Disabled</td>
<td>If Enabled, writes an internal debug log for folder synchronization. The default value is Disabled.</td>
</tr>
<tr>
<td>LDAP (DS) Call Tracing/Logging</td>
<td>Enabled or Disabled</td>
<td>If Enabled, writes an internal debug log for any calls made to Oracle Internet Directory. The default value is Disabled.</td>
</tr>
</tbody>
</table>
Table F–12 lists descriptions for parameters in the Access and Routing Control Management section.

### Table F–12 NNTP Inbound Access and Routing Control Management Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Control</td>
<td>Enabled or Disabled</td>
<td>If Enabled, turns on routing control checks. If Disabled, all routing control checks are turned off, including Reject and Trusted lists (domains, senders, recipients, and IPs). If Oracle Internet Directory does not have this value set to default, NNTP enables routing control. The default value is Disabled.</td>
</tr>
<tr>
<td>Allow Peer Feed</td>
<td>True or False</td>
<td>If True, this instance permits incoming feed from peers. The default value is False.</td>
</tr>
<tr>
<td>Allow Streaming Feed</td>
<td>True or False</td>
<td>If True, streaming is permitted, such as MODE STREAM in NNTP is enabled. The default value is False.</td>
</tr>
<tr>
<td>DNS Check on Client Domains</td>
<td>True or False</td>
<td>If True, checks whether the client domain name exists in the DNS server. If False, the connection is rejected. The default value is False.</td>
</tr>
<tr>
<td>Allow Client Posting</td>
<td>True or False</td>
<td>Specifies whether clients can post messages to the server. If False all newsgroups on the server will be read-only. The default value is True.</td>
</tr>
<tr>
<td>DNS Check on Sender Domain</td>
<td>True or False</td>
<td>If True, checks whether the domain in the sender’s address exists in the DNS server. The default value is False.</td>
</tr>
<tr>
<td>Maximum Number of Cross Posts Allowed</td>
<td>Enter a nonnegative number</td>
<td>Specifies an upper limit for the number of newsgroups to which any one message can be posted at a time. The default value is 3.</td>
</tr>
<tr>
<td>Spam Flood Interval (Minutes)</td>
<td>Enter a nonnegative number</td>
<td>Number of minutes used to detect spam flooding. The default value is 10.</td>
</tr>
<tr>
<td>Spam Maximum Flood Count</td>
<td>Enter a nonnegative number</td>
<td>NNTP server signals flooding if the number of messages and connections from a single host exceeds the value of this parameter within the Spam Flood Interval. The default value is 10000.</td>
</tr>
<tr>
<td>Trusted Domains</td>
<td>Multivalue string of trusted domains, wildcards allowed</td>
<td>List of allowed domains or subdomains from which news is received, if Routing Control is Enabled, regardless of any further routing control checks.</td>
</tr>
<tr>
<td>Trusted IPs</td>
<td>Multivalue string of trusted IP addresses, wildcards allowed</td>
<td>List of IP addresses from which connections are permitted, if Routing Control is Enabled, regardless of any further routing control checks.</td>
</tr>
</tbody>
</table>
In the **General Parameters** section are two lists displaying available and current peer servers.

Table F–13 lists descriptions for the parameters in the **General Parameters** section.

### Table F–13  NNTP Inbound General Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Control</td>
<td>Enabled or Disabled</td>
<td>If Enabled, turns on routing control checks. If Disabled, all routing control checks are turned off, including Reject and Trusted lists. If Oracle Internet Directory does not have this value set to default, NNTP enables routing control. The default value is Disabled.</td>
</tr>
<tr>
<td>Allow Peer Feed</td>
<td>True or False</td>
<td>If True, this instance permits incoming feed from peers. The default value is False.</td>
</tr>
<tr>
<td>Allow Streaming Feed</td>
<td>True or False</td>
<td>If True, streaming is permitted, such as MODE STREAM in NNTP is enabled. The default value is False.</td>
</tr>
<tr>
<td>DNS Check on Client Domains</td>
<td>True or False</td>
<td>If True, checks whether the client domain name exists in the DNS server. If False, the connection is rejected. The default value is False.</td>
</tr>
<tr>
<td>Allow Client Posting</td>
<td>True or False</td>
<td>Specifies whether clients can post messages to the server. If False all newsgroups on the server will be read-only. The default value is True.</td>
</tr>
<tr>
<td>DNS Check on Sender Domain</td>
<td>True or False</td>
<td>If True, checks whether the domain in the sender’s address exists in the DNS server. The default value is False.</td>
</tr>
<tr>
<td>Maximum Number of Cross Posts Allowed</td>
<td>Enter a nonnegative number</td>
<td>Specifies an upper limit for the number of newsgroups to which any one message can be posted at a time. The default value is 3.</td>
</tr>
<tr>
<td>Spam Flood Interval (Minutes)</td>
<td>Enter a nonnegative number</td>
<td>Number of minutes used to detect spam flooding. The default value is 10.</td>
</tr>
</tbody>
</table>
Oracle Mail NNTP Inbound Server Debug Parameters

When debug parameters are enabled, more analysis data is included in the log file, depending upon the level set in the Process Log Level parameter of the General Parameters section. The NNTP inbound process log file is located in the $ORACLE_HOME/oes/log/um_system/nntp_in directory.

Table F–14 lists the descriptions of the NNTP inbound server debug parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spam Maximum Flood Count</td>
<td>Enter a nonnegative number</td>
<td>NNTP server signals flooding if the number of messages and connections from a single host exceeds the value of this parameter within the Spam Flood Interval. The default value is 10000.</td>
</tr>
<tr>
<td>Trusted Domains</td>
<td>Multivalue string of trusted domains, wildcards allowed</td>
<td>List of allowed domains or subdomains from which news is received, if Routing Control is Enabled, regardless of any further routing control checks.</td>
</tr>
<tr>
<td>Trusted IPs</td>
<td>Multivalue string of trusted IP addresses, wildcards allowed</td>
<td>List of IP addresses from which connections are permitted, if Routing Control is Enabled, regardless of any further routing control checks.</td>
</tr>
<tr>
<td>Trusted Senders</td>
<td>Multivalue string of trusted senders</td>
<td>List of sender addresses against which the sender address is checked, if Routing Control is Enabled.</td>
</tr>
<tr>
<td>Trusted Sender Domains</td>
<td>Multivalue string of trusted sender domains</td>
<td>List of allowed domains against which the domain part of the sender’s e-mail address is checked, if Routing Control is Enabled.</td>
</tr>
<tr>
<td>Disallowed Domains</td>
<td>Multivalue string of disallowed domains, wildcards allowed</td>
<td>If Routing Control is Enabled, this parameter rejects connections from specified domains.</td>
</tr>
<tr>
<td>Disallowed Senders</td>
<td>Multivalue string of disallowed senders</td>
<td>Identifies senders to reject, if Routing Control is Enabled.</td>
</tr>
<tr>
<td>Disallowed IP Addresses</td>
<td>Multivalue string of disallowed IP addresses, wildcards allowed</td>
<td>Identifies IP addresses to disallow connections from, if Routing Control is Enabled.</td>
</tr>
</tbody>
</table>

Oracle Mail NNTP Inbound Server

Oracle Mail NNTP Outbound Server

This section lists the instance setting, debug parameter, and Oracle Collaboration Suite Database connection parameter definitions for the Oracle Mail NNTP outbound server process. It contains the following topics:

- Oracle Mail NNTP Outbound Server Instance Setting Parameters
Oracle Mail NNTP Outbound Server Debug Parameters

Oracle Mail NNTP Outbound Oracle Collaboration Suite Database Connection Parameters

Oracle Mail NNTP Outbound Server Instance Setting Parameters

In the News Collaboration Suite Database section, the News Collaboration Suite Database list displays available Oracle Collaboration Suite Databases.

Table F–1 lists descriptions for parameters in the LDAP Connection Pool Parameters section.

Table F–2 lists descriptions for the parameters in the LDAP Connection Retry Parameters section.

Table F–15 lists descriptions for parameters in the Thread Parameters section.

Table F–15 NNTP Outbound Thread Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum</td>
<td>0–1000</td>
<td>Maximum number of threads available for peer connection handling. The default value is 50.</td>
</tr>
</tbody>
</table>

Table F–16 lists descriptions of parameters in the General Parameters section.

Table F–16 NNTP Outbound General Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Socket Timeout (minutes)</td>
<td>0–30</td>
<td>Number of minutes before a cached connection times out. The default value is 30.</td>
</tr>
<tr>
<td>Feed Retry Interval (minutes)</td>
<td>0–60</td>
<td>Number of minutes before trying a message feed again. The default value is 60.</td>
</tr>
<tr>
<td>Feed Recovery Interval (minutes)</td>
<td>30–180</td>
<td>Number of minutes before a queued message marked as in process is moved back to pending, which aids in failure recovery for the NNTP outbound server. The default value is 90.</td>
</tr>
<tr>
<td>Number of Cache Connections</td>
<td>Enter a nonnegative number</td>
<td>Number of attempts the NNTP outbound server makes to relay an article to another NNTP server. The NNTP outbound server tries to transmit a message up to the allotted number of times and then ceases. The default value is 3.</td>
</tr>
</tbody>
</table>
Oracle Mail Server Parameter Definitions

Oracle Mail NNTP Outbound Server Debug Parameters

When debug parameters are enabled, more analysis data is included in the log file, depending upon the level set in the Process Log Level parameter of the General Parameters section. The NNTP outbound process log file is located in the $ORACLE_HOME/oes/log/um_system/nntp_out directory.

Table F–17 lists the descriptions of the NNTP outbound server debug parameters.

**Table F–17  NNTP Outbound Debug Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP (DS) Call Tracing/Logging</td>
<td>Enabled or Disabled</td>
<td>If Enabled, writes an internal debug log for any calls made to Oracle Internet Directory. The default value is Disabled.</td>
</tr>
</tbody>
</table>

Oracle Mail NNTP Outbound Oracle Collaboration Suite Database Connection Parameters

Table 3–1 on page 3-2 lists descriptions of parameters for open connections to the Oracle Collaboration Suite Database.
Oracle Mail POP Server

This section lists the instance setting, debug parameter, and Oracle Collaboration Suite Database connection parameter definitions for the Oracle Mail POP server process. It contains the following topics:

- Oracle Mail POP Server Instance Setting Parameters
- Oracle Mail POP Server Debug Parameters
- Oracle Mail POP Server Oracle Collaboration Suite Database Connection Parameters

Oracle Mail POP Server Instance Setting Parameters

In the Mail Collaboration Suite Database section are two lists showing available Oracle Collaboration Suite Databases and Oracle Collaboration Suite Databases currently being serviced. Use the buttons between the two lists to shuttle Oracle Collaboration Suite Databases from one list to the other.

Available Collaboration Suite Database(s) is the list of all the mail-enabled Oracle Collaboration Suite Databases in the system to which servers can potentially connect.

Collaboration Suite Database(s) currently being serviced lists Oracle Collaboration Suite Databases to which the POP server will connect, and serve requests from e-mail users who have mailboxes on any of the nodes in the list. Additionally, access to shared and public folders is limited to these Oracle Collaboration Suite Databases through this POP instance.

The LDAP connection pool is a pool of open connections to Oracle Internet Directory. Table F–1 lists descriptions for parameters in the LDAP Connection Pool Parameters section.

Table F–2 lists descriptions for the parameters in the LDAP Connection Retry Parameters section.

Table F–18 lists descriptions for parameters in the General Parameters section.

<table>
<thead>
<tr>
<th>Table F–18</th>
<th>POP General Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>Option</td>
</tr>
<tr>
<td>Presentation Name</td>
<td>Custom, POP, or POPSSL</td>
</tr>
<tr>
<td>Custom Name</td>
<td>String</td>
</tr>
<tr>
<td>SSL Enabled</td>
<td>True or False</td>
</tr>
<tr>
<td>Default Domain</td>
<td>String</td>
</tr>
</tbody>
</table>
### Table F–19 (Cont.) POP General Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Admin to Access Any Account</td>
<td>True or False</td>
<td>If True, this feature enables administrators to access any user account using POP in the same manner as an actual user. To use this feature, administrators must change their user ID in the POP client to include the userID of the user they want to proxy in as, beginning with #SU. For example, an administrator with user ID <a href="mailto:admin1@foo.com">admin1@foo.com</a> can proxy in as <a href="mailto:user1@foo.com">user1@foo.com</a> by changing the user ID to <a href="mailto:admin1@foo.com">admin1@foo.com</a>#<a href="mailto:SUuser1@foo.com">SUuser1@foo.com</a>.</td>
</tr>
<tr>
<td>Maximum Number of Clients</td>
<td>0–1000</td>
<td>Maximum number of clients allowed to connect to each server instance simultaneously. The default value is 1000.</td>
</tr>
<tr>
<td>POP3 Delete Allowed</td>
<td>Yes or No</td>
<td>If Yes, enables server to delete read messages. If No, the server does not delete messages from the Oracle Collaboration Suite Database. The default value is No.</td>
</tr>
<tr>
<td>POP3 Retrieval</td>
<td>ALL or UNREAD</td>
<td>ALL means all mails are to be retrieved from the server; for UNREAD, only unread messages are retrieved. The default value is UNREAD.</td>
</tr>
<tr>
<td>Wallet Location for TLS Support</td>
<td>Directory path</td>
<td>Enter file: followed by the absolute path to the directory in which the SSL wallet is located. It is only relevant if the Support STARTTLS Command is True. For example, enter file:/directory_path</td>
</tr>
</tbody>
</table>
| SASL Protection                   | None, Integrity, or Confidentiality | Applicable only to server-to-server communication within local servers (using the XAUTH command).  
- None: Password authentication only is protected during communication  
- Integrity: Adds integrity checking (to detect tampering of the communication)  
- Confidentiality: The communication is encrypted (and also implies Integrity)  
The default value is None. |
| Support STARTTLS Command          | True or False| For this parameter to be enabled, a wallet location must be specified in the Wallet Location for TLS Support parameter. The default value is True. |
| Allow Clear Text Login            | True or False| If True, enables the LOGIN command and insecure SASL authentication mechanisms, PLAIN and LOGIN, that transmit the password in plain text, whether SASL authentication is enabled or not. If False, the SASL Authentication parameter must be enabled or the Support STARTTLS Command parameter must be set to True in order to log in to the POP server and prevent password snooping. |
| Protocol Banner                   | String       | This parameter determines the message that the server sends when accepting new incoming client requests. The text of this parameter must be encoded in US-ASCII.  
The following macros are also permitted and will be applied to all POP servers on the particular Applications tier:  
- %s (server type)  
- %h (host name)  
- %v (version information)  
The default value is Server Ready.  
**Note:** Any value entered in this field is also entered in the Protocol Banner parameter of all protocol servers. |
Oracle Mail POP Server Debug Parameters

When debug parameters are enabled, more analysis data is included in the log file, depending upon the level set in the Process Log Level parameter of the General Parameters section. The POP process log file is located in the $ORACLE_HOME/oes/log/um_system/pop directory.

Table F–19 lists the descriptions of the POP server debug parameters.
Table F–19  POP Debug Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Connections</td>
<td>Enabled or Disabled</td>
<td>If Enabled, writes an internal debug log for database connections. The default value is Disabled.</td>
</tr>
<tr>
<td>Folder Open</td>
<td>Enabled or Disabled</td>
<td>If Enabled, writes an internal debug log for the folder open function. The default value is Disabled.</td>
</tr>
<tr>
<td>Start/End of Client Requests</td>
<td>Enabled or Disabled</td>
<td>If Enabled, writes an internal debug log for client requests. The default value is Disabled.</td>
</tr>
<tr>
<td>I/O Between POP Server and Clients</td>
<td>Enabled or Disabled</td>
<td>If Enabled, writes an internal debug log for I/O between the POP server and clients. The default value is Disabled.</td>
</tr>
<tr>
<td>Client Logins</td>
<td>Enabled or Disabled</td>
<td>If Enabled, writes an internal debug log for client logins. The default value is Disabled.</td>
</tr>
<tr>
<td>Memory Management</td>
<td>Enabled or Disabled</td>
<td>If Enabled, writes an internal debug log for memory management. The default value is Disabled.</td>
</tr>
<tr>
<td>LDAP (DS) Call Tracing/Logging</td>
<td>Enabled or Disabled</td>
<td>If Enabled, writes an internal debug log for any calls made to Oracle Internet Directory. The default value is Disabled.</td>
</tr>
</tbody>
</table>

Oracle Mail POP Server Oracle Collaboration Suite Database Connection Parameters

Table 3–1 on page 3-2 lists descriptions of parameters for open connections to the Oracle Collaboration Suite Database.

Oracle Mail Virus Scrubber

This section lists the instance setting, debug parameter, and Oracle Collaboration Suite Database connection parameter definitions for the Oracle Mail Virus Scrubber server. It contains the following topics:

- Oracle Mail Virus Scrubber Instance Settings
- Oracle Mail Virus Scrubber Debug Parameters
- Oracle Mail Virus Scrubber Oracle Collaboration Suite Database Connection Parameters

Oracle Mail Virus Scrubber Instance Settings

In the Mail Collaboration Suite Database section, the Collaboration Suite Database list displays available Oracle Collaboration Suite Databases.

In the Thread Parameters section, the number in the Number of Threads field establishes the number of Virus Scrubber connections to the database. The number chosen is dependent upon such factors as how much memory each thread uses and how many connection each thread makes, and whether a connection pool is being used. A large number of threads can affect resource performance.

Table F–20 lists descriptions for parameters in the General Parameters section.
**Table F–20 Virus Scrubber General Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Pre-Scan Mode     | Disabled, Enabled, or Pre-scan Only | - Disabled: Only those messages that have been isolated by a previous pre-scan operation are sent through the filters for scrubbing.  
                     |                                  | - Enabled: First, all messages are prescanned and messages that match the pre-scan criteria are isolated. Then, only those isolated messages are sent through the filters for scrubbing.  
                     |                                  | - Pre-scan Only: All messages are prescanned only. Messages that match the pre-scan criteria are isolated.                                    |
| Pre-Scan Criteria |                                 | The IMAP SEARCH command style conditions that are executed to identify the list of messages to pass through the third-party scanner. Messages matching this criteria are removed from the mailbox of the respective users until the third-party scanner verdict is harmless/not-affected.  
                     |                                  | All IMAP search commands except new, old, and recent can be used in the filter.                                                               |
| Scan Interval (Minutes) | Enter a nonnegative number | Time interval between two successive scans.                                                                                               |
| Repair Mode       | Purge or Quarantine             | Determines what action to perform to messages identified as infected. Select Purge to delete the infected messages immediately; Quarantine to save it to a special folder specified in following parameters. |
| Quarantine Destination E-mail Address | String | If the repair mode is set to Quarantine, this parameter, in conjunction with Quarantine Destination Folder, uniquely identifies an IMAP folder where the message will be quarantined. |
| Quarantine Destination Folder | String | If the repair mode is Quarantine, this parameter, in conjunction with Quarantine Destination E-mail Address, uniquely identifies an IMAP folder where the message will be quarantined. |
Notification Message to Virus Sender

Table F–20 (Cont.) Virus Scrubber General Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Notification Message to Virus Sender | String | If a message is infected, the sender will be notified. The text entered in this parameter will be sent embedded in a standard mail. When composing notification message templates to virus senders (or recipients), you can use macros that can be substituted with actual message-specific values when the Virus Scrubber generates and sends the notifications. Supported macros include:

- `%internaldate%`: Received date of the message
- `%messagesize%`: Message size in bytes
- `%rfc822date%`: The Date header value of the message
- `%rfc822from%`: The From header value of the message
- `%rfc822subject%`: The Subject header value of the message
- `%rfc822to%`: The To header value of the message
- `%rfc822cc%`: The CC header value of the message
- `%rfc822sender%`: The Sender header value of the message
- `%rfc822replyto%`: The Reply-To header value of the message
- `%rfc822msgid%`: The Message-ID header value of the message
- `%xpriority%`: The X-Priority header value of the message

For example, consider the following notification text:

A message you sent on %internaldate% to %rfc822to% with subject %rfc822subject% has been identified as virus-infected. Please run a virus scan on your computer immediately.

The actual notification message received by the recipient will have the preceding text with the macros substituted by the actual values from the virus-infected message.

Notification Message to Virus Recipient

If a message is infected, the recipient will be notified. The text entered in this parameter will be sent embedded in a standard mail.

See Notification Message to Virus Sender for a list of supported macros.
Oracle Mail Virus Scrubber Debug Parameters

When debug parameters are enabled, more analysis data is included in the log file, depending upon the level set in the Process Log Level parameter of the General Parameters section. The Virus Scrubber server log file is located in the $ORACLE_HOME/oes/log/um_system/vs directory.

Table F–21 lists the descriptions of the Virus Scrubber debug parameters.

### Table F–20 (Cont.) Virus Scrubber General Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Log Level</td>
<td>Internal Error, Error, Warning, Notification, Trace, Dump</td>
<td>Determines the level of detail the server writes to the log file, as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Internal Error: internal errors only: Administrator should file a bug with Oracle Support.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Error: all information included in Internal Error plus regular errors: Error condition exists and must be corrected by administrator.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Warning: everything up to Error plus warnings: Conditions exist that may require attention.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Notification: everything up to Warning plus Notification: An informational message only, no additional action needed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Levels beyond Notification are intended for Oracle Support to analyze a defect situation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Trace: everything up to Notification plus trace logs: Program traces that aid support debugging.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Dump: everything up to Trace, in addition to printing information from the program to aid in analyzing a problem. Extended debugging information that can aid debugging.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default value is Error.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Maximum Log Size (MB)</th>
<th>Enter a nonnegative number</th>
<th>Determines how big a log file can grow before the server writes to a new log file. The default value is 5.</th>
</tr>
</thead>
<tbody>
<tr>
<td>See Also</td>
<td>&quot;Log Files&quot; on page 3-3 for more information about log files</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Maximum Number of Log Files</th>
<th>Enter a nonnegative number</th>
<th>If the number of log files for an IMAP server instance reaches this limit, no new log files will be generated. The existing log files will be written to in rotation. The default value is 10.</th>
</tr>
</thead>
<tbody>
<tr>
<td>See Also</td>
<td>&quot;Log Files&quot; on page 3-3 for more information about log files</td>
<td></td>
</tr>
</tbody>
</table>

### Oracle Mail Virus Scrubber Debug Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statistics Logging</td>
<td>Enabled or Disabled</td>
<td>If Enabled, process statistics are logged to the level set in the Process Log Level parameter (subject to a minimum level of 25). The default value is Disabled.</td>
</tr>
</tbody>
</table>

| LDAP (DS) Call Tracing/Logging | Enabled or Disabled | If Enabled, writes internal debug log for any calls made to Oracle Internet Directory. The default value is Disabled. |

### Oracle Mail Virus Scrubber Oracle Collaboration Suite Database Connection Parameters

Table 3–1 on page 3-2 lists descriptions of parameters for open connections to the Oracle Collaboration Suite Database.
Oracle Mail List Server

This section lists the instance setting, debug parameter, and Oracle Collaboration Suite Database connection parameter definitions for the List Server.

- Oracle Mail List Server Target-Level Settings
- Oracle Mail List Server Instance Debug Parameters
- Oracle Mail List Server Oracle Collaboration Suite Database Connection Parameters

Oracle Mail List Server Target-Level Settings

In the Mail Collaboration Suite Database section, choose an Oracle Collaboration Suite Database from the Queue Processing and Reconfirm Subscription Collaboration Suite Database lists.

In the Delivery Collaboration Suite Database section are two lists showing available Oracle Collaboration Suite Databases and Oracle Collaboration Suite Databases currently being serviced. Use the buttons between the two lists to shuttle Oracle Collaboration Suite Databases from one list to the other.

Available Collaboration Suite Database(s) is the list of all the mail-enabled Oracle Collaboration Suite Databases in the system to which servers can potentially connect.

Collaboration Suite Database(s) currently being serviced lists Oracle Collaboration Suite Databases to which the List Server will connect.

The List Server performs many operations with the LDAP server in multiple threads. To improve performance, a pool of connections to the database and the LDAP server is maintained to ensure that no thread must wait for a connection to access database or LDAP services.

Table F–1 lists descriptions for parameters in the LDAP Connection Pool Parameters section.

Table F–2 lists descriptions of parameters in the LDAP Connection Retry Parameters section.

Table F–22 lists descriptions of parameters in the SMTP Protocol Timeouts section.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial ready response</td>
<td>Enter a nonnegative number</td>
<td>Amount of time in minutes that SMTP outbound server waits for a 220 greeting reply from a remote MTA after sending a connect request. The default value is 5.</td>
</tr>
<tr>
<td>response timeout</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EHLO/HELO response</td>
<td>Enter a nonnegative number</td>
<td>Amount of time in minutes that the SMTP outbound server waits for a reply from a remote MTA to an \texttt{ehlo} or \texttt{helo} command. The default value is 5.</td>
</tr>
<tr>
<td>response timeout</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAIL FROM response</td>
<td>Enter a nonnegative number</td>
<td>Amount of time in minutes that the SMTP outbound server waits for a reply from a remote MTA to a \texttt{mail from} command. The default value is 10.</td>
</tr>
<tr>
<td>response timeout</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RCPT TO response</td>
<td>Enter a nonnegative number</td>
<td>Amount of time in minutes that the SMTP outbound server waits for a reply from a remote MTA to a \texttt{rcpt to} command. The default value is 10.</td>
</tr>
<tr>
<td>response timeout</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DATA response</td>
<td>Enter a nonnegative number</td>
<td>Amount of time in minutes that the SMTP outbound server waits for a reply from a remote MTA to a \texttt{data} command. The default value is 5.</td>
</tr>
<tr>
<td>timeout</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table F–23 lists descriptions of parameters in the **DSN Parameters** section.

### Table F–23  List Server DSN Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Postmaster DSNs</td>
<td>All, None, Failures, or</td>
<td>Type of delivery status notifications (DSNs) the postmaster wants to receive. The default value is All.</td>
</tr>
<tr>
<td></td>
<td>Undeliverables</td>
<td></td>
</tr>
<tr>
<td>Postmaster E-mail</td>
<td>Valid e-mail address</td>
<td>Enter the e-mail address of the postmaster.</td>
</tr>
<tr>
<td>Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Temporary DSN</td>
<td>Enter a nonnegative number</td>
<td>Determines how often a DSN must be sent for temporary errors. The default value is 24.</td>
</tr>
<tr>
<td>Interval (hours)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DSN Language</td>
<td>Default or User Preferred</td>
<td>Determines whether DSNs are sent in the default or user-preferred language.</td>
</tr>
</tbody>
</table>

- **Default**: DSNs are sent in the language selected from the **Default DSN Language** list
- **User Preferred**: DSNs appear in the user-preferred language according to the language header in the original message

The default value is **User Preferred**.
Table F–23 (Cont.) List Server DSN Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default DSN Language</td>
<td>NA</td>
<td>The following languages are available for DSNs:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>American</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Arabic</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Czech</td>
</tr>
<tr>
<td></td>
<td></td>
<td>German</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Danish</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Spanish</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Greek</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Latin American Spanish</td>
</tr>
<tr>
<td></td>
<td></td>
<td>French</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Canadian French</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hungarian</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Italian</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hebrew</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Japanese</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Korean</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Norwegian</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dutch</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Polish</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Portuguese</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Brazilian Portuguese</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Romanian</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Russian</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Swedish</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Finnish</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Slovak</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Thai</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Turkish</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Simplified Chinese_China</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Traditional Chinese</td>
</tr>
<tr>
<td>Include Complete Error Message in DSN</td>
<td>True or False</td>
<td>If True, any error message is included with the DSN. The default value is True.</td>
</tr>
<tr>
<td>Success DSN Preamble</td>
<td>String</td>
<td>Enter text to be displayed upon successful delivery of a message into a user’s inbox. This text will display to a user who chooses to receive delivery receipts. The text of this parameter must be encoded in UTF-8.</td>
</tr>
<tr>
<td>Failure DSN Preamble</td>
<td>String</td>
<td>Enter text to be displayed upon failure of delivery of a message into a user’s inbox. This text will display to a user in a return message announcing delivery failure. The text of this parameter must be encoded in UTF-8.</td>
</tr>
<tr>
<td>Delay DSN Preamble</td>
<td>String</td>
<td>Enter text to be displayed upon delay of delivery of a message into a user’s inbox. This text will display to a user in a return message announcing a delay in the delivery of the message. The text of this parameter must be encoded in UTF-8.</td>
</tr>
</tbody>
</table>

Table F–24 lists descriptions of parameters in the Rules and Routing Control Parameters section.
### Table F–24 List Server Rules and Routing Control Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Rewriting Rules Separators</td>
<td>String</td>
<td>Defines the list of characters that should be treated as separators in address rewriting rules. The default value is <code>.:%@!^-/\[]&lt;&gt;</code>.</td>
</tr>
<tr>
<td>Sender Rewriting Rules</td>
<td>Multivalue</td>
<td>Rewrite rules for senders; used only by the SMTP outbound server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>See Also</strong>: &quot;SMTP Address Rewriting Rules&quot; on page 3-17 for information about rewriting rules</td>
</tr>
<tr>
<td>Recipient Rewriting Rules</td>
<td>Multivalue</td>
<td>Rewrite rules for recipients.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>See Also</strong>: &quot;SMTP Address Rewriting Rules&quot; on page 3-17 for information about rewriting rules</td>
</tr>
</tbody>
</table>
External Filter

If True, enables external filter processing. The default value is False.

External Filter Process

Note: Effective only if the External Filter parameter is set to ocsv2, and will be used for Oracle Collaboration Suite Release 9.0.4 filters only.

Specifies the path for the executable of the external process in four parts:

- name: The name of the external filter
- path_to_external_process: The complete path of the process to be called
- when_to_call: The time to call the external filter: ENV, DATA, RELAY, or NEVER, as follows:
  - ENV: After receiving the message envelope
  - DATA: After receiving the complete message and before local delivery
  - RELAY: Just before relaying a message
  - NEVER: Essentially disables the callout
- system_flags: No value should be entered unless Oracle Collaboration Suite Release 9.0.3 filters are being used, in which case set this option to version=ocsv1
Table F–25 (Cont.) List Server Rules and Routing Control Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scanner Interfaces</td>
<td></td>
<td>Specifies C callouts for virus scanning. The form is:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>name:shared_library_path, when_to_call, host_&amp;_port, (function_set), repairmsg scanner_flags, system_flags</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In this form, the parts are as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>name: The name of the external filter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>shared_library_path: The full path of the C shared library loaded by the server at startup</td>
</tr>
<tr>
<td></td>
<td></td>
<td>when_to_call, such as the time to call the external filter: ENV, DATA, RELAY, or NEVER, as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ ENV: After receiving the message envelope</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ DATA: After receiving the complete message and before local delivery</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ RELAY: Just before relaying a message</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ NEVER: Essentially disables the callout</td>
</tr>
<tr>
<td></td>
<td></td>
<td>host_&amp;_port, as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ If the scanner needs a host and port, enter them as host:port_number, such as SMTP machine:3602</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ If host and port are not needed, use INTERNAL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>function_set</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(The functions each filter callout should implement, which are called by the server to pass data to the scanner and to receive back the status and repaired messages)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>init, register_callback, scan_msg, send_msg, receive_msg, close</td>
</tr>
<tr>
<td></td>
<td></td>
<td>repairmsg</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If set to 1, callout can send the repaired message back to the server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If set to 0, server does not read any repaired message back from the callout and rejects the mail if the scanner returns failure.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>system_flags</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Should be set to 0.</td>
</tr>
</tbody>
</table>

Table F–25 lists descriptions of parameters in the General Parameters section.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Archive Processing                            | Enabled or Disabled              | When enabled, incoming messages are checked for archive eligibility. A message is eligible for archiving if any of the senders or recipients is a local user with an archive policy set. The default value is Enabled.  

**Note:** Whatever value is chosen for this parameter, is also applied to the List Server and SMTP inbound processes. |
| Number of Mails Processed Concurrently        | Enter a nonnegative number       | Number of messages to be processed simultaneously by the List Server. The server will use one thread for each message for processing. A very high value produces too many threads in the process. The default value is 50.  

**Note:** Ensure that the maximum number of database connections in the database connection pool parameters matches or exceeds this value. |
| Number of Recipients Per Batch                | Enter a nonnegative number       | Number of users to which each user thread delivers messages. The default value is 1000.          |
| Number of Threads Per Mail                    | Enter a nonnegative number       | Specifies the maximum number of threads that can be spawned at a time to distribute a message to the members of a distribution list. Because each thread uses database and Oracle Internet Directory connections, this value should be increased with caution. The default value is 10. |
| Recovery Interval (minutes)                   | Enter a nonnegative number       | Number of minutes before messages marked as being processed are picked up for retrial by the server. The default value is 90. |
| Allow only SMTP-authenticated user to post    | Yes or No                        | If Yes, the List Server processes only those messages whose senders have been authenticated by the SMTP inbound server. If No, authentication is not required. The default value is No. |
| Checkpoint Interval                           | Enter a nonnegative, number      | Number of recipients processed in a single relay delivery attempt. The default value is 20.        |
| Fallback MX Host                              | String                           |                                                                                                  |
| Maximum Hop Count                             | Enter a nonnegative, number      | Maximum number of hops a message can go through. The default value is 25.                        |
| Use Errors-To Header to Specify the Mail Address for DSNs | True or False                    | The default value is False.                                                                      |
| Maximum Number of Connections in the Connection Pool | Enter a nonnegative, number      | The default value is 10.                                                                          |
| PLSQL Timeout (minutes)                       | Enter a nonnegative number       | Number of minutes before a List Server’s PL/SQL call will be canceled if the call is not returned. Used during PL/SQL mail-merge and external list processing. The default value is 10. |
| Allow List Owners to Enable Archive           | Yes or No                        | The default value is No.                                                                          |
### Table F–25 (Cont.) List Server General Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bounce Threshold</td>
<td>Enter a nonnegative number</td>
<td>Specifies the number of times a message is bounced by a member before the member is unsubscribed from the list. Indicates the number of DSNs processed for a particular recipient before the list owner is notified about the recurring DSNs. Once this number of DSNs is received for a recipient on a list, a mail is sent to the list owner notifying the owner about recurring DSNs for the user. The owner can then take further action to remove the user from the list.</td>
</tr>
<tr>
<td>Maintain Bounce History for (days)</td>
<td>Enter a nonnegative number</td>
<td>Specifies the number of days for which the List Server maintains the number of DSNs for a recipient before it is purged. If the bounce threshold number of DSNs is not reached for a recipient in this period, the count is reset to 0 at the end of this period. The default value is 30.</td>
</tr>
<tr>
<td>Queue Polling Interval (seconds)</td>
<td>Enter a nonnegative number</td>
<td>Specifies the number of seconds between the List Server’s polling the queue to check for new messages to be processed. The default value is 30.</td>
</tr>
<tr>
<td>IP Address of Network Interface to Use</td>
<td>String</td>
<td>If the host running the SMTP server has multiple network cards with individual IP addresses, enter the IP address that is used to make outgoing connections.</td>
</tr>
</tbody>
</table>
| SASL Protection            | None, Integrity, or Confidentiality | Applicable only to server-to-server communication within local servers (using the XAUTH command).  
  - None: Password authentication only is protected during communication  
  - Integrity: Adds integrity checking (to detect tampering of the communication)  
  - Confidentiality: The communication is encrypted (and also implies Integrity)  
  The default value is None. |
| Enable server to server authentication and security | True or False | Set to True so that the SMTP inbound server authenticates itself to other inbound servers, when there are multiple Oracle Collaboration Suite Databases and separate SMTP servers serving each database.  
When the SMTP inbound server mandates authentication, all clients send their e-mail user ID and password as credentials. In the present scenario, this will pose a problem for all other outbound servers that are trying to relay messages to this inbound server. Because the protocol servers do not have passwords of their own, the relay fails. To overcome this, outbound server instances use the umadmin user name and password as credentials.  
The default value is False. |
| Relay Hosts                | Fully qualified host names  | Contains the host names of the MTAs to which all relay messages sent out of the List Server should be routed. Messages addressed to local users are not affected. If this parameter is not filled, then an MX record lookup is performed while relaying messages. |
| Disclaimer Message         | String                      | Enter disclaimer text that will display in messages sent outside the domain, that is relayed to an external domain.  
The disclaimer message displays inline beneath the body of the message.  
The text of this parameter must be encoded in UTF-8. |
When debug parameters are enabled, more analysis data is included in the log file, depending upon the level set in the Process Log Level parameter of the General Parameters section of the Default Settings page. The List Server process log file is located in the $ORACLE_HOME/oes/log/um_system/ls directory.

Table F–26 lists the descriptions of the List Server debug parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Process Log Level                  | Internal Error, Error, Warning, Notification, Trace, Dump | Determines the level of detail the server writes to the log file, as follows:
- Internal Error: internal errors only: Administrator should file a bug with Oracle Support
- Error: all information included in Internal Error plus regular errors: Error condition exists and must be corrected by administrator
- Warning: everything up to Error plus warnings: Conditions exist that may require attention
- Notification: everything up to Warning plus Notification: An informational message only, no additional action needed
Levels beyond Notification are intended for Oracle Support to analyze a defect situation.
- Trace: everything up to Notification plus trace logs: Program traces that aid support debugging
- Dump: everything up to Trace, in addition to printing information from the program to aid in analyzing a problem. Extended debugging information that can aid debugging
The default value is Error. |
| Maximum Log Size (MB)              | Enter a nonnegative number      | Determines how big a log file can grow before the server writes to a new log file. The default value is 5.                                                                                                                   |
|                                    |                                 | See Also: "Log Files" on page 3-3 for more information about log files                                                                                                                                                                                                             |
| Maximum Number of Log Files        | Enter a nonnegative number      | If the number of log files for a List Server instance reaches this limit, no new log files will be generated. The existing log files will be written to in rotation. The default value is 10.                                                                                   |
|                                    |                                 | See Also: "Log Files" on page 3-3 for more information about log files                                                                                                                                                                                                             |
| Process Flags                      | -l, -cp=value                   | Sets the local mailer flag and check point value. The values are:
- l (local mailer flag): Messages to unknown local users are relayed to the next node instead of being rejected.
- -cp=value (check point value): Messages are delivered to local recipients in one transaction. 0 delivers to all recipients in one transaction.
The default values are no local mailer flag and check point value is 0. |
Oracle Mail List Server Oracle Collaboration Suite Database Connection Parameters

Table 3–1 on page 3-2 lists descriptions of parameters for open connections to the Oracle Collaboration Suite Database.

Oracle Mail SMTP Inbound Server

This section lists the instance setting, debug parameter, and Oracle Collaboration Suite Database connection parameter definitions for the Oracle Mail SMTP inbound server process. It contains the following topics:

- Oracle Mail SMTP-Inbound Instance Settings
- Oracle Mail SMTP-Inbound Instance Debug Parameters
- Oracle Mail SMTP-Inbound Oracle Collaboration Suite Database Connection Parameters

Oracle Mail SMTP-Inbound Instance Settings

In the Collaboration Suite Database section, the Message Insertion Mode list contains the following selections:

- RoundRobin:
- Failover:
- Auto:
There are two lists showing available Oracle Collaboration Suite Databases and Oracle Collaboration Suite Databases currently being serviced.

**Available Collaboration Suite Database(s)** is the list of all the mail-enabled Oracle Collaboration Suite Databases in the system to which servers can potentially connect.

**Selected Collaboration Suite Database(s)** lists Oracle Collaboration Suite Databases to which the SMTP server will connect, and service requests from e-mail users who have mailboxes on any of the nodes in the list.

In the **Collaboration Suite Database for Direct Delivery** section are two lists showing available Oracle Collaboration Suite Databases and Oracle Collaboration Suite Databases currently being serviced.

**Available Collaboration Suite Database(s)** is the list of all the mail-enabled Oracle Collaboration Suite Databases in the system to which servers can potentially connect.

**Selected Collaboration Suite Database(s)** lists Oracle Collaboration Suite Databases to which the List Server will connect.

The LDAP connection pool is a pool of open connections to Oracle Internet Directory.

Table F–1 lists the descriptions of the parameters in the **LDAP Connection Pool Parameters** section.

Table F–2 lists descriptions of parameters in the **LDAP Connection Retry Parameters** section.

Table F–27 lists descriptions of parameters in the **Thread Parameters** section.

### Table F–27  SMTP Inbound Thread Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeout (seconds)</td>
<td>0–65535</td>
<td>Number of seconds a thread is idle before it is removed from the pool. The default is 1860.</td>
</tr>
<tr>
<td>Increment</td>
<td>1–999</td>
<td>Number of Oracle Internet Directory connections to be added to the pool when the existing connections in the pool are exhausted, to the limit of the <strong>Maximum</strong> parameter value. The default value is 1.</td>
</tr>
<tr>
<td>Minimum</td>
<td>Enter a nonnegative number</td>
<td>Number of Oracle Internet Directory connections in the pool at startup. The default value is 1.</td>
</tr>
<tr>
<td>Maximum</td>
<td>Enter a nonnegative number</td>
<td>Maximum number of Oracle Internet Directory connections in the pool not to be exceeded. The default value is 20.</td>
</tr>
</tbody>
</table>

Table F–28 lists descriptions of parameters in the **DSN Parameters** section.

### Table F–28  SMTP Inbound DSN Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Postmaster DSNs</td>
<td>All, None, Failures, or Undeliverables</td>
<td>Type of delivery status notifications (DSNs) the postmaster wants to receive. The default value is Failures.</td>
</tr>
<tr>
<td>Postmaster E-mail Address</td>
<td>Valid e-mail address</td>
<td>Enter the e-mail address of the postmaster.</td>
</tr>
<tr>
<td>Temporary DSN Interval (hours)</td>
<td>Enter a nonnegative number</td>
<td>If a message cannot be delivered in the specified interval, a delay DSN is sent. The default value is 24.</td>
</tr>
</tbody>
</table>
### DSN Language

Determines whether DSNs are sent in the default or user-preferred language.

- **Default**: DSNs are sent in the language selected from the [Default DSN Language list](#).
- **User Preferred**: DSNs appear in the user-preferred language according to the language header in the original message.

The default value is **User Preferred**.

### Default DSN Language

NA

The following languages are available for DSNs:

- American
- Arabic
- Czech
- German
- Danish
- Spanish
- Greek
- Latin American Spanish
- French
- Canadian French
- Hungarian
- Italian
- Hebrew
- Japanese
- Korean
- Norwegian
- Dutch
- Polish
- Portuguese
- Brazilian Portuguese
- Romanian
- Russian
- Swedish
- Finnish
- Slovak
- Thai
- Turkish
- Simplified Chinese_China
- Traditional Chinese

### Include Complete Error Message in DSN

True or False

If True, the reason for delivery failure is included with the DSN. The default value is True.

### Success DSN Preamble

String

Enter text to be displayed upon successful delivery of a message into a user’s inbox. This text will display to a user if they choose to receive delivery receipts. The text of this parameter must be encoded in UTF-8.

### Failure DSN Preamble

String

Enter text to be displayed upon failure of delivery of a message into a user’s inbox. This text will display to a user in a return message announcing delivery failure. The text of this parameter must be encoded in UTF-8.

### Delay DSN Preamble

String

Enter text to be displayed upon delay of delivery of a message into a user’s inbox. This text will display to a user in a return message announcing a delay in the delivery of the message. The text of this parameter must be encoded in UTF-8.
Table F–29 lists description of parameters in the Rules and Routing Control Parameters section.

<table>
<thead>
<tr>
<th>Table F–29  SMTP Inbound Rules and Routing Control Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Routing Control</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Spam Flood Interval (Minutes)</td>
</tr>
<tr>
<td>Spam Maximum Flood Count</td>
</tr>
<tr>
<td>Maximum Number of Recipients Allowed in an Envelope</td>
</tr>
<tr>
<td>Envelope and Message Header Checking</td>
</tr>
<tr>
<td>Reject Messages with Different Auth Id and Envelope Sender</td>
</tr>
<tr>
<td>Enforce Reverse DNS Lookup on Client IP</td>
</tr>
<tr>
<td>DNS Check on HELO/EHLO Domains</td>
</tr>
<tr>
<td>DNS Check on Sender Domain</td>
</tr>
<tr>
<td>Relay Allowed</td>
</tr>
<tr>
<td>Trusted Relay Domains</td>
</tr>
<tr>
<td>Address Rewriting Rule Separators</td>
</tr>
<tr>
<td>Recipient Rewriting Rules</td>
</tr>
</tbody>
</table>

See Also: “SMTP Address Rewriting Rules” on page 3-17 for information about rewriting rules.
Table F–29  (Cont.) SMTP Inbound Rules and Routing Control Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scanner Interfaces</strong></td>
<td></td>
<td><strong>Note:</strong> Effective only if the <em>External Filter</em> parameter is set to ocsv2, and will be used for Oracle Collaboration Suite Release 9.0.4 filters only.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Specifies C callouts for virus scanning. The form is: name:shared_library_path, when_to_call:host_&amp;_port,(function_set), repairmsg scanner_flags, system_flags</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In this form, the parts are as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>name:</strong> The name of the external filter</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>shared_library_path:</strong> The full path of the C shared library loaded by the server at startup</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>when_to_call,</strong> such as the time to call the external filter: ENV, DATA, RELAY, or NEVER, as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ ENV: After receiving the message envelope</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ DATA: After receiving the complete message and before local delivery</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ RELAY: Just before relaying a message</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ NEVER: Essentially disables the callout</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>host_&amp;_port,</strong> as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ If the scanner needs a host and port, enter them as host:port_number, such as SMTP machine:3602</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ If host and port are not needed, use INTERNAL</td>
</tr>
<tr>
<td></td>
<td>init, register_callback, scan_msg, send_msg, receive_msg, close</td>
<td><strong>function_set</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(The functions each filter callout should implement, which are called by the server to pass data to the scanner and to receive back the status and repaired messages)</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>repairmsg</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>If set to 1, callout can send the repaired message back to the server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If set to 0, server does not read any repaired message back from the callout and rejects the mail if the scanner returns failure.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>system_flags</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Should be set to 0.</td>
</tr>
<tr>
<td><strong>External Filter</strong></td>
<td>ocsv2, True, or False</td>
<td>Enables or disables external filter processing. When set to ocsv2, only Oracle Collaboration Suite Release 9.0.4 filters are applied. The <strong>Scanner Interfaces</strong> and <strong>External Filter Process</strong> parameters are effective only when <strong>External Filter</strong> is set to ocsv2. The default value is False.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Filters are defined through Policy pages.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>See Also:</strong> “Managing Oracle Mail Filters” on page 8-2 for more information about defining filters</td>
</tr>
</tbody>
</table>
Table F–29 (Cont.) SMTP Inbound Rules and Routing Control Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Filter Process</td>
<td>Multivalue</td>
<td>Note: Effective only if the External Filter parameter is set to ocsv2, and will be used for Oracle Collaboration Suite Release 9.0.4 filters only.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Specifies the path for the executable of the external process in four parts:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>name:path_to_external_process, when_to_call, system_flags</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In this form, the parts are as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>name: The name of the external filter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>path_to_external_process: The complete path of the process to be called</td>
</tr>
<tr>
<td></td>
<td></td>
<td>when_to_call: The time to call the external filter: ENV, DATA, RELAY, or NEVER, as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ ENV: After receiving the message envelope</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ DATA: After receiving the complete message and before local delivery</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ RELAY: Just before relaying a message</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ NEVER: Essentially disables the callout</td>
</tr>
<tr>
<td></td>
<td></td>
<td>system_flags: No value should be entered unless Oracle Collaboration Suite Release 9.0.3 filters are being used,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>in which case set this option to version=ocsv1</td>
</tr>
<tr>
<td>Trusted IPs</td>
<td>Multivalue string of trusted IP addresses, wildcards allowed</td>
<td>List of IP addresses from which all messages are permitted, regardless of any routing control checks. These entries are assumed to have full access and do not require authentication for access.</td>
</tr>
<tr>
<td>Trusted Domains</td>
<td>Multivalue string of trusted domains, wildcards allowed</td>
<td>List of allowed domains or sub-domains from which mail is received, if Routing Control is Enabled, regardless of any further routing control checks. These entries are assumed to have full access and do not require authentication for access.</td>
</tr>
<tr>
<td>Trusted Sender Domains</td>
<td>Multivalue string of trusted sender domains</td>
<td>List of allowed domains against which the domain part of the sender’s e-mail address is checked, if Routing Control is Enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The format of the string is as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>domain authflag</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In the preceding example, domain is the name of the domain and authflag is either auth or no-auth.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When the no-auth option is set, authentication is required. The end user is not prompted to authenticate using a password before access is allowed. However, the auth option does require password authentication before access is allowed.</td>
</tr>
<tr>
<td>Trusted Senders</td>
<td>Multivalue string of trusted senders</td>
<td>List of sender addresses against which the sender address is checked, if Routing Control is Enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The format of the string is as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>domain authflag</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In the preceding example, domain is the name of the domain and authflag is either auth or no-auth.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When the no-auth option is set, authentication is required. The end user is not prompted to authenticate using a password before access is allowed. However, the auth option does require password authentication before access is allowed.</td>
</tr>
</tbody>
</table>
Table F–30  (Cont.) SMTP Inbound General Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archive Processing</td>
<td>Enabled or Disabled</td>
<td>When enabled, incoming messages are checked for archive eligibility. A message is eligible for archiving if any of the senders or recipients is a local user with an archive policy set. The default value is Enabled. <strong>Note:</strong> Whatever value is chosen for this parameter is also applied to the List Server and SMTP inbound processes.</td>
</tr>
<tr>
<td>Presentation Name</td>
<td>String</td>
<td>Display name for the SMTP server instances. When the default value for this parameter has been changed, you must change the listener configuration to the same value. The default value is ESSMI.</td>
</tr>
<tr>
<td>Custom Name</td>
<td>String</td>
<td>Applies only if the presentation name is set to custom.</td>
</tr>
<tr>
<td>Maximum Size of Shell (in Bytes)</td>
<td>Enter a nonnegative number</td>
<td>Maximum size of database shell, in bytes, for a message. IMAP uses this parameter to perform a spam check on messages during an APPEND operation. The shell comprises all the headers of the message plus the placeholders for mime body parts. The default value is 1000000.</td>
</tr>
<tr>
<td>Maximum Number of Headers Allowed in a Message</td>
<td>Enter a nonnegative number</td>
<td>The maximum number of RFC822 headers allowed in a single message. IMAP uses this parameter to perform a spam check on messages during an APPEND operation. The default value is 1000.</td>
</tr>
<tr>
<td>Maximum Number of Clients</td>
<td>0–1000</td>
<td>Maximum number of clients allowed to connect to the server instance. The default value is 1000.</td>
</tr>
</tbody>
</table>

In the **General Parameters** section, local domains to which local mail user addresses belong are listed in the **Available Domain(s)** list and can be moved to the **Selected Domain(s)** list.

Table F–30 lists descriptions of parameters in the **General Parameters** section.
Table F–30  (Cont.) SMTP Inbound General Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Port                             | Enter a nonnegative, non-zero number | The port on which the listener listens for the SMTP service. The default value is 25.  
Note: When the port value in the listener configuration for this server is changed, it is recommended that this parameter’s value be set to the same value. |
| Checkpoint Interval              | Enter a nonnegative, number | Number of recipients processed in a single relay delivery attempt. The default value is 20.                                                     |
| Maximum Hop Count                | Enter a nonnegative, number | Maximum number of hops a message can go through. The default value is 25.                                                                    |
| Maximum Message Size (KB)        | Enter a nonnegative number  | Maximum allowed incoming message size. The default value is 10.                                                                             |
| Message Timeout (minutes)        | Enter a nonnegative, number | Number of minutes after an SMTP server restart, after which messages that remain in the being processed state will be processed again. The default value is 30.  
(If an SMTP server is restarted after a shutdown, it looks for messages being processed. If they stay in the same state for this long, it reprocesses them.) |
| SMTP Queue Timeout (days)        | Enter a nonnegative, number | Maximum number of days a message can be in the queue. The default value is 5.                                                                |
| Use Errors-To Header to Specify the Mail Address for DSNs | True or False | The default value is False.                                                                                                                 |
| Authentication                   | Mandatory, Optional, or None | Determines if SMTP authentication is enabled.  
Mandatory: Users must authenticate themselves before sending any messages.                         
Optional: Users may authenticate themselves, but the SMTP server accepts the message even if authentication fails.                         
None: Authentication is not required  
The default value is None. |
| Submit Only                      | True or False | If TRUE, submits inbound messages without resolving recipient. The default value is FALSE.                                             |
| Process IMIP Messages            | True or False | If True, IMIP messages will be sent to the IMIP queue. The default value is False.                                                           |
| Wallet Location for TLS Support  | Directory path | Enter file: followed by the absolute path to the directory in which the SSL wallet is located. It is only relevant if the Support STARTTLS Command is True.  
For example, file:/directory_path |
| Add Custom Headers               |                            | List of standard or extended (user-defined) headers added to each message at the time of message reception.                                |
| SASL Protection                  | None, Integrity, or Confidentiality | Applicable only to server-to-server communication within local servers (using the XAUTH command).  
- None: Password authentication only is protected during communication  
- Integrity: Adds integrity checking (to detect tampering of the communication)  
- Confidentiality: The communication is encrypted (and also implies Integrity)  
The default value is None. |
### Table F–30  (Cont.) SMTP Inbound General Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SASL Authentication</td>
<td>Enabled or Disabled</td>
<td>If Enabled, SASL authentication is permitted. The default value is Disabled.</td>
</tr>
<tr>
<td>Support STARTTLS Command</td>
<td>True or False</td>
<td>For this parameter to be enabled, a wallet location must be specified in the Wallet Location for TLS Support parameter. The default value is True.</td>
</tr>
<tr>
<td>Allow Clear Text Login</td>
<td>True or False</td>
<td>If True, enables the LOGIN command and insecure SASL authentication mechanisms, PLAIN and LOGIN, that transmit the password in plain text. If False, the SASL Authentication parameter must be enabled or the Support STARTTLS Command parameter must be set to True in order to log in to the SMTP inbound server and prevent password snooping.</td>
</tr>
<tr>
<td>Default Domain</td>
<td>String</td>
<td>Default domain used as user login if the user logging in does not provide one.</td>
</tr>
<tr>
<td>Add Domain to EMail Addresses with Missing Domain in Envelope</td>
<td>True or False</td>
<td>If enabled, a default domain will be added to the envelope sender or recipient if the domain is missing from the address. The default value is False.</td>
</tr>
<tr>
<td>Disclaimer Message</td>
<td>String</td>
<td>Enter disclaimer text that will display in messages sent outside the domain, that is relayed to an external domain. The disclaimer message displays inline beneath the body of the message. The text of this parameter must be encoded in UTF-8.</td>
</tr>
</tbody>
</table>
| Protocol Banner                                 | String             | This parameter determines the message that the server sends when accepting new incoming client requests. The text of this parameter must be encoded in US-ASCII. The following macros are also permitted and will be to all SMTP inbound servers on the particular Applications tier:  
  ■  %s (server type)  
  ■  %h (host name)  
  ■  %v (version information)  
  The default value is Server Ready.  
  **Note:** Any value entered in this field is also entered in the Protocol Banner parameter of all protocol servers. |
Oracle Mail SMTP-Inbound Instance Debug Parameters

When debug parameters are enabled, more analysis data is included in the log file, depending upon the level set in the Process Log Level parameter of the General Parameters section. The SMTP inbound process log file is located in the $ORACLE_HOME/oes/log/um_system/smtp_in directory.

Table F–31 lists the descriptions of the SMTP inbound debug parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Process Log Level | Internal Error, Error, Warning, Notification, Trace, Dump | Determines the level of detail the server writes to the log file, as follows:  
  - Internal Error: internal errors only. Administrator should file a bug with Oracle Support  
  - Error: all information included in Internal Error plus regular errors. Error condition exists and must be corrected by administrator  
  - Warning: everything up to Error plus warnings. Conditions exist that may require attention  
  - Notification: everything up to Warning plus Notification. An informational message only, no additional action needed  
  Levels beyond Notification are intended for Oracle Support to analyze a defect situation.  
  - Trace: everything up to Notification plus trace logs. Program traces that aid support debugging  
  - Dump: everything up to Trace, in addition to printing information from the program to aid in analyzing a problem. Extended debugging information that can aid debugging  
  The default value is Error. |
| Maximum Log Size (MB) | Enter a nonnegative number | Determines how big a log file can grow before the server writes to a new log file. The default value is 5.  
  See Also: "Log Files" on page 3-3 for more information about log files |
| Maximum Number of Log Files | Enter a nonnegative number | If the number of log files for an IMAP server instance reaches this limit, no new log files will be generated. The existing log files will be written to in rotation. The default value is 10.  
  See Also: "Log Files" on page 3-3 for more information about log files |
| Process Flags | -l, -cp=value, or -rac=value | Sets the local mailer flag, check point value, and enables Oracle Real Application Clusters. Each flag must be on its own line.  
  -l (local mailer flag): Messages to unknown local users are relayed to the next node, instead of being rejected.  
  -cp=value (check point value): Messages are delivered to at most value local recipients in one transaction. 0 means delivering to all recipients in one transaction.  
  -rac=value (enable optimization for Oracle Real Application Clusters): Set -rac=1 to enable. Message insertion and local delivery uses the same OCI service handle. If no value is set, the process will be less efficient. |
Oracle Mail Server Parameter Definitions

Table 3–1 on page 3-2 lists descriptions of parameters for open connections to the Oracle Collaboration Suite Database.

Oracle Mail SMTP-Inbound Oracle Collaboration Suite Database Connection Parameters

Oracle Mail SMTP Outbound Server

This section lists the instance setting, debug parameter, and Oracle Collaboration Suite Database connection parameter definitions for the Oracle Mail SMTP Outbound server process. It contains the following topics:

- Oracle Mail SMTP Outbound Instance Settings
- Oracle Mail SMTP Outbound Instance Debug Parameters
- Oracle Mail SMTP Outbound Oracle Collaboration Suite Database Connection Parameters

Oracle Mail SMTP Outbound Instance Settings

In the Mail Collaboration Suite Database section, the Collaboration Suite Database list displays Oracle Collaboration Suite Databases.

In the Collaboration Suite Database for Direct Delivery section are two lists showing available Oracle Collaboration Suite Databases and Oracle Collaboration Suite Databases currently being serviced.

Oracle Mail SMTP Inbound Debug Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entire Inbound Module</td>
<td>Enabled or Disabled</td>
<td>If Enabled, writes an internal debug log for the entire SMTP inbound module. The default value is Disabled.</td>
</tr>
<tr>
<td>Server Response</td>
<td>Enabled or Disabled</td>
<td>If Enabled, performs debugging for the SMTP server responses. The default value is Disabled.</td>
</tr>
<tr>
<td>OCI Calls</td>
<td>Enabled or Disabled</td>
<td>If Enabled, writes an internal debug log for OCI calls. The default value is Disabled.</td>
</tr>
<tr>
<td>Address Rewriting Rules</td>
<td>Enabled or Disabled</td>
<td>If Enabled, writes an internal debug log for address rewriting rule processing. The default is Disabled.</td>
</tr>
<tr>
<td>Log Message Body</td>
<td>Enabled or Disabled</td>
<td>If Enabled, writes an internal debug log for the message body. The default is Disabled.</td>
</tr>
<tr>
<td>Local Delivery</td>
<td>Enabled or Disabled</td>
<td>If Enabled, writes an internal debug log for SMTP inbound. The default value is Disabled.</td>
</tr>
<tr>
<td>Routing Control</td>
<td>Enabled or Disabled</td>
<td>If Enabled, writes an internal debug log for routing control. The default value is Disabled.</td>
</tr>
<tr>
<td>LDAP Resolution</td>
<td>Enabled or Disabled</td>
<td>If Enabled, writes an internal debug log for LDAP resolution. The default value is Disabled.</td>
</tr>
<tr>
<td>Recovery Module</td>
<td>Enabled or Disabled</td>
<td>If Enabled, performs recovery module debugging. The default value is Disabled.</td>
</tr>
<tr>
<td>DSN Module</td>
<td>Enabled or Disabled</td>
<td>If Enabled, writes an internal debug log for the DSN module. The default value is Disabled.</td>
</tr>
<tr>
<td>External Filter</td>
<td>Enabled or Disabled</td>
<td>If Enabled, writes an internal debug log for the external filter process. The default value is Disabled.</td>
</tr>
<tr>
<td>LDAP (DS) Call Tracing/Logging</td>
<td>Enabled or Disabled</td>
<td>If Enabled, writes an internal debug log for any calls made to Oracle Internet Directory. The default value is Disabled.</td>
</tr>
</tbody>
</table>
Available Collaboration Suite Database(s) is the list of all the mail-enabled Oracle Collaboration Suite Databases in the system to which servers can potentially connect.

Selected Collaboration Suite Database(s) lists Oracle Collaboration Suite Databases to which the List Server will connect.

The LDAP connection pool is a pool of open connections to Oracle Internet Directory. Table F–1 lists descriptions of parameters in the LDAP Connection Pool section.

Table F–2 lists descriptions of parameters in the LDAP Connection Retry Parameters section.

Table F–3 lists descriptions of parameters in the Thread Parameters section.

Table F–22 lists descriptions of parameters in the SMTP Protocol Timeouts section.

Table F–23 lists descriptions of parameters in the DSN Parameters section.

Table F–24 lists descriptions of parameters in the Rules and Routing Control Parameters section.

In the General Parameters section, local domains to which local mail user addresses belong are listed in the Available Domain(s) list and can be moved to the Selected Domain(s) list.

Table F–33 lists descriptions of parameters in the General Parameters section.

### Table F–32 SMTP Outbound Thread Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeout (seconds)</td>
<td>0–65535</td>
<td>Number of seconds before an idle thread is cleaned up. The default is 1860.</td>
</tr>
<tr>
<td>Increment</td>
<td>1–999</td>
<td>Number of threads added to the client connection pool. The default is 1.</td>
</tr>
<tr>
<td>Minimum</td>
<td>1–1000</td>
<td>Minimum number of threads available for client connection handling. The default is 1.</td>
</tr>
<tr>
<td>Maximum</td>
<td>0–100</td>
<td>Maximum number of threads available for client connection handling. The default is 50.</td>
</tr>
</tbody>
</table>

Table F–22 lists descriptions of parameters in the SMTP Protocol Timeouts section.

Table F–23 lists descriptions of parameters in the DSN Parameters section.

Table F–24 lists descriptions of parameters in the Rules and Routing Control Parameters section.

In the General Parameters section, local domains to which local mail user addresses belong are listed in the Available Domain(s) list and can be moved to the Selected Domain(s) list.

Table F–33 lists descriptions of parameters in the General Parameters section.

### Table F–33 SMTP Outbound General Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archive Processing</td>
<td>Enabled or Disabled</td>
<td>When enabled, incoming messages are checked for archive eligibility. A message is eligible for archiving if any of the senders or recipients is a local user with an archive policy set. The default value is Enable.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> Whatever value is chosen for this parameter, is also applied to the List Server and SMTP inbound processes.</td>
</tr>
<tr>
<td>Archive Queue</td>
<td>Enabled, Archiving Only, or</td>
<td>When enabled, archived messages are sent to a specified e-mail address. The address is specified in the administration pages of the Oracle WebMail client. The default value is Disabled.</td>
</tr>
<tr>
<td>Processing</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Checkpoint Interval</td>
<td>Enter a nonnegative, number</td>
<td>Number of recipients processed in a single relay delivery attempt. The default value is 20.</td>
</tr>
<tr>
<td>Fallback MX Host</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td>Maximum Hop Count</td>
<td>Enter a nonnegative, number</td>
<td>Maximum number of hops a message can go through. The default value is 25.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Maximum Message Size (KB)</td>
<td>Enter a nonnegative</td>
<td>Maximum allowed incoming message size. The default value is 10.</td>
</tr>
<tr>
<td>SMTP Minimum Queue Age (minutes)</td>
<td>Enter a nonnegative</td>
<td>Number of minutes a message stays in the queue before being delivered. The default value is 30.</td>
</tr>
<tr>
<td>Message Timeout (minutes)</td>
<td>Enter a nonnegative,</td>
<td>Number of minutes after an SMTP server restart, after which messages that remain in the being processed state will be processed again. The default value is 30.</td>
</tr>
<tr>
<td></td>
<td>number</td>
<td>(If an SMTP server is restarted after a shutdown, it looks for messages being processed. If they stay in the same state for this long, it reprocesses them.)</td>
</tr>
<tr>
<td>SMTP Queue Timeout (days)</td>
<td>Enter a nonnegative,</td>
<td>Maximum number of days a message can be in the queue. The default value is 5.</td>
</tr>
<tr>
<td></td>
<td>number</td>
<td></td>
</tr>
<tr>
<td>SMTP Relay</td>
<td>String</td>
<td>Enter the name of the relay host.</td>
</tr>
<tr>
<td>Use Errors-To Header to Specify</td>
<td>True or False</td>
<td></td>
</tr>
<tr>
<td>the Mail Address for DSNs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum Number of Connections in</td>
<td>Enter a nonnegative,</td>
<td>The default value is 10.</td>
</tr>
<tr>
<td>the Connection Pool</td>
<td>number</td>
<td></td>
</tr>
<tr>
<td>IP Address of Network Interface</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td>to Use</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SASL Protection</td>
<td>None, Integrity, or</td>
<td>Applicable only to server-to-server communication within local servers (using the XAUTH command).</td>
</tr>
<tr>
<td></td>
<td>Confidentiality</td>
<td>- None: Password authentication only is protected during communication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Integrity: Adds integrity checking (to detect tampering of the communication)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Confidentiality: The communication is encrypted (and also implies Integrity)</td>
</tr>
<tr>
<td>Enable server to server</td>
<td>True or False</td>
<td>The default value is False.</td>
</tr>
<tr>
<td>authentication and security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disclaimer Message</td>
<td>String</td>
<td>Enter disclaimer text that will display in messages sent outside the domain, that is relayed to an external domain.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The disclaimer message displays inline beneath the body of the message.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The text of this parameter must be encoded in UTF-8.</td>
</tr>
</tbody>
</table>
Oracle Mail Server Parameter Definitions

Oracle Mail SMTP Outbound Instance Debug Parameters

When debug parameters are enabled, more analysis data is included in the log file, depending upon the level set in the Process Log Level parameter of the General Parameters section. The SMTP outbound process log file is located in the $ORACLE_HOME/oes/log/um_system/smtp_out directory.

Table F–34 lists the descriptions of the SMTP outbound debug parameters.

### Table F–34 (Cont.) SMTP Outbound General Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Process Log Level</strong></td>
<td>Internal Error, Error, Warning, Notification, Trace, Dump</td>
<td>Determines the level of detail the server writes to the log file, as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Internal Error: internal errors only: Administrator should file a bug with Oracle Support</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Error: all information included in Internal Error plus regular errors: Error condition exists and must be corrected by administrator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Warning: everything up to Error plus warnings: Conditions exist that may require attention</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Notification: everything up to Warning plus Notification: An informational message only, no additional action needed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Levels beyond Notification are intended for Oracle Support to analyze a defect situation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Trace: everything up to Notification plus trace logs: Program traces that aid support debugging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Dump: everything up to Trace, in addition to printing information from the program to aid in analyzing a problem. Extended debugging information that can aid debugging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default value is Error.</td>
</tr>
<tr>
<td><strong>Maximum Log Size (MB)</strong></td>
<td>Enter a nonnegative number</td>
<td>Determines how big a log file can grow before the server writes to a new log file. The default value is 5.</td>
</tr>
<tr>
<td><strong>Maximum Number of Log Files</strong></td>
<td>Enter a nonnegative number</td>
<td>If the number of log files for an IMAP server instance reaches this limit, no new log files will be generated. The existing log files will be written to in rotation. The default value is 10.</td>
</tr>
<tr>
<td><strong>Process Flags</strong></td>
<td>-l, -cp=value, or -rac=value</td>
<td>Sets the local mailer flag, check point value, and enables Oracle Real Application Clusters. Each flag must be on its own line.</td>
</tr>
<tr>
<td></td>
<td>-l (local mailer flag): Messages to unknown local users are relayed to the next node, instead of being rejected.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>-cp=value (check point value): Messages are delivered to at most value local recipients in one transaction. 0 means delivering to all recipients in one transaction.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>-rac=value (enable optimization for Oracle Real Application Clusters): Set -rac=1 to enable. Message insertion and local delivery uses the same OCI service handle. If no value is set, the process will be less efficient.</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>OCI Calls</td>
<td>Enabled or Disabled</td>
<td>If Enabled, writes an internal debug log for OCI calls. The default value is Disabled.</td>
</tr>
<tr>
<td>Address Rewriting Rules</td>
<td>Enabled or Disabled</td>
<td>If Enabled, writes an internal debug log for address rewriting rule processing. The default is Disabled.</td>
</tr>
<tr>
<td>Submit Module</td>
<td>Enabled or Disabled</td>
<td>The default value is Disabled.</td>
</tr>
<tr>
<td>Local Delivery</td>
<td>Enabled or Disabled</td>
<td>If Enabled, writes an internal debug log for SMTP outbound. The default value is Disabled.</td>
</tr>
<tr>
<td>Queue Processor</td>
<td>Enabled or Disabled</td>
<td>The default value is Disabled.</td>
</tr>
<tr>
<td>LDAP Resolution</td>
<td>Enabled or Disabled</td>
<td>If Enabled, writes an internal debug log for LDAP resolution. The default value is Disabled.</td>
</tr>
<tr>
<td>Outbound Main Module</td>
<td>Enabled or Disabled</td>
<td>The default value is Disabled.</td>
</tr>
<tr>
<td>Recovery Module</td>
<td>Enabled or Disabled</td>
<td>If Enabled, performs recovery module debugging. The default value is Disabled.</td>
</tr>
<tr>
<td>Relay Module</td>
<td>Enabled or Disabled</td>
<td>The default value is Disabled.</td>
</tr>
<tr>
<td>DNS Module</td>
<td>Enabled or Disabled</td>
<td>If Enabled, enables DNS module debugging. The default value is Disabled.</td>
</tr>
<tr>
<td>List Server Interface</td>
<td>Enabled or Disabled</td>
<td>The default value is Disabled.</td>
</tr>
<tr>
<td>DSN Module</td>
<td>Enabled or Disabled</td>
<td>If Enabled, writes an internal debug log for the DSN module. The default value is Disabled.</td>
</tr>
<tr>
<td>External Filter</td>
<td>Enabled or Disabled</td>
<td>If Enabled, writes an internal debug log for the external filter process. The default value is Disabled.</td>
</tr>
<tr>
<td>LDAP (DS) Call Tracing/Logging</td>
<td>Enabled or Disabled</td>
<td>If Enabled, writes an internal debug log for any calls made to Oracle Internet Directory. The default value is Disabled.</td>
</tr>
</tbody>
</table>

Oracle Mail SMTP Outbound Oracle Collaboration Suite Database Connection Parameters

Table 3–1 on page 3-2 lists descriptions of parameters for open connections to the Oracle Collaboration Suite Database.
Alias and Distribution List Lookup

This appendix discusses alias and distribution list look up.

This appendix includes the following topics:

- Enabling Alias Lookup from Standard Clients
- Enabling Distribution List Lookup from Standard Clients

Enabling Alias Lookup from Standard Clients

**Note:** Lookup is available through the Oracle WebMail client and does not require user configuration. The lookup feature is available when addressing an e-mail that an end user is composing, and when adding members to a distribution list in the address book, in addition to the basic Address Book search that is available on every page through the search bar.

Enable e-mail alias lookup from a standard client, such as Netscape Communicator, as follows:

1. Run the `$ORACLE_HOME/oes/bin/oesSearchUtil.sh` script to enable or disable alias lookups from standard clients:

   ```
   $ORACLE_HOME/oes/bin/oesSearchUtil.sh -type alias -option enable or disable -domain email_domain
   ```

   In this command, `email_domain` is the e-mail domain name for which this option must be enabled or disabled.

   For example:

   ```
   $ORACLE_HOME/oes/bin/oesSearchUtil.sh -type alias -option enable -domain foo.com
   ```

2. Look up e-mail aliases from standard clients with a search base as `root`, or the e-mail alias container, such as:

   ```
   cn=Alias,domain_dn,cn=um_system,cn=EmailServerContainer,cn=Products,cn=OracleContext
   ```

   In this command, `domain_dn` is the domain DN.

   For example, if the e-mail domain is `domain.com`, the value of `domain_dn` is the string `cn=domain,dc=com.`
Another configuration is to create a referral at the public namespace level. This is useful if you do not want to use root as the search base and want to retain the same search base for searching users, distribution lists, and aliases. This can be achieved through a referral.

The following sample LDIF file shows how to create a referral for aliases in the public namespace. For standard clients, the search base should be configured as the subscriber_dn.

```ldif
cn=emailsearchbase,subscriber_dn
dn: cn=emailsearchbase, subscriber_dn
cn: emailsearchbase
objectclass: top
objectclass: referral
objectclass: extensibleObject
ref:
ldap://oid_host:oid_port/cn=Alias,dn=domain_dn,dc=um_
```

In this example:

- `subscriber_dn` is the distinguished name of the subscriber in Oracle Internet Directory
- `oid_host` is the Oracle Internet Directory host name
- `oid_port` is the Oracle Internet Directory port
- `domain_dn` is the domain DN

For example, if the e-mail domain is `domain.com`, the value is the string `dc=domain,dc=com`.

---

**Note:**
To be able to perform alias lookup, users must first bind themselves to Oracle Internet Directory through their e-mail client by adding a string similar to the following into the client’s LDAP preferences:

```
cn=username,cn=user_realm,dc=domain,dc=com
```

---

**Enabling Distribution List Lookup from Standard Clients**

**Note:**
Lookup is available through the Oracle WebMail client and does not require user configuration. The lookup feature is available when addressing an e-mail that an end user is composing, and when adding members to a distribution list in the address book, in addition to the basic Address Book search that is available on every page through the search bar.

E-mail distribution lists and membership information are synchronized between the private e-mail namespace and the public namespace to enable distribution list lookup from standard clients.

For `dlsync` to work, a public distribution list container must be created and must have all permissions for the `EmailAdminsGroup`. This synchronization option can be enabled or disabled using the Oracle WebMail client administration pages.
Enabling Distribution List Lookup from Standard Clients

Example

1. Substitute the required values in the following sample LDIF file for creating the public container and definition and load it using `ldapmodify` command.

   ```ldif
   dn: cn=subschemasubentry
   changetype: modify
   add: objectclasses
   objectclasses: ( 2.16.840.1.113894.5.2.5000 NAME 'mailgroup' SUP groupofuniquenames AUXILIARY MAY ( mail ) )
   
   dn: cn=dlContainer, subscriber_dn
   changetype: add
   objectclass: top
   objectclass: orclContainer
   cn: dlContainer
   orclaci: access to entry by
   group="cn=EmailAdminsGroup,cn=EMailServerContainer,cn=Products,cn=OracleContext"
   (add,delete,browse)
   orclaci: access to attr=(*) by
   group="cn=EmailAdminsGroup,cn=EMailServerContainer,cn=Products,cn=OracleContext"
   (read,write,search,compare)
   
   where subscriber_dn is the distinguished name of the subscriber in Oracle Internet Directory.

2. Open the Oracle WebMail client.

   ```
   See Also: "Oracle Collaboration Suite 10g WebMail Client" on page 1-2 for information about how to access the Oracle WebMail client
   ```

3. Click the Administration tab.

4. Click Domain.

5. Select Domain Settings.

6. Change the following properties:
   - Location in Public Namespace to cn=dlContainer, subscriber_dn
   - Objectclasses for creation in Public Namespace to the two values groupofuniquenames and mailgroup (should be entered in two lines)
   - Naming Attribute for creation in Public Namespace to cn

7. Run the distribution list synchronization utility, if required.

8. Configure the search base to be root or the subscriber_dn in standard clients.

This section includes the following topics:

- Distribution List Synchronization Utility
- Synchronizing One or Multiple Distribution Lists
- Synchronizing All Distribution Lists from a Private E-mail Namespace
Enabling Distribution List Lookup from Standard Clients

Distribution List Synchronization Utility

The `esdssyncdl` utility synchronizes distribution lists from the e-mail private namespace under `cn=EMailserverContainer` to a public namespace. This allows standard clients, such as Netscape Communicator, to see the distribution lists through anonymous searches. You can run `esdssyncdl` occasionally to dump or redump all distribution lists from a private namespace to a public namespace.

Whenever any update or delete operation occurs on the members of the private distribution list, the changes are reflected in the public distribution list. When you add or delete a distribution list using the Oracle WebMail administration pages, it occurs in the public namespace.

Synchronizing One or Multiple Distribution Lists

Running `esdssyncdl` with an input file containing a list of distribution lists, with one distribution list name in each line, synchronizes the private e-mail namespace under `cn=EMailServerContainer,cn=Products,cn=OracleContext` to a public namespace. Use this option when you only have a few distribution lists to synchronize.

The syntax is as follows:

```
esdssyncdl ldaphost=ldap_host (mandatory)
port=ldap_port (mandatory)
username=superuser_DN (mandatory)
password=superuser_password (mandatory)
preferencelocation=DN_of_the_Dl_preferences (mandatory)
	detail: DN where Dl preferences are located. (See Note 1 & 3)
inputfile=file_path
	detail: full path of the file with dls to synchronize, one dl's mail ID per line. (See Note 2)
flags=More_options_with_which_sync_can_be_modified
	detail: flags=all
```

The following is a usage example:

```
esdssyncdl ldaphost=gmldap01 port=389 username=cn=orcladmin password=welcome
inputfile=/tmp/dlfile preferencelocation=dc=us,dc=foo,dc=com,cn=um_system, cn=EMailServerContainer,cn=Products,cn=OracleContext
```

Synchronizing All Distribution Lists from a Private E-mail Namespace

Synchronizing all private distribution lists under the `cn=EMailServerContainer` to a public namespace can be done as a one-time task. This is the default option.

Use this option when your deployment has distribution lists populated under the `cn=EmailServerContainer` (the e-mail private namespace), and you want to add the lists to a public namespace so that a standard client can see them.

The syntax is as follows:

```
esdssyncdl ldaphost=ldap_host (mandatory)
port=ldap_port (mandatory)
username=superuser_DN (mandatory)
password=superuser_password (mandatory)
preferencelocation=DN_of_the_Dl_preferences (mandatory)
```

The following is a usage example:

```
esdssyncdl ldaphost=gmldap01 port=389 username=cn=orcladmin password=welcome
```
flags=all preference=location=dc=us,dc=foo,dc=com,cn=um_
system, cn=EMailServerContainer, cn=Products, cn=OracleContext

The following preferences are set in the domain where the distribution lists are present:

- orclmaildlsynccontainerdn is the distinguished name of the container where all public distribution lists are created
- orclmaildlsyncnamingattr is the naming attribute used for public distribution lists
- orclmaildlsyncattrstosync is the list of attributes to be synchronized from private to public distribution lists
- orclmaildlsyncobjectclass is the list of objectclasses to be synchronized from private to public distribution lists

For the inputfile content, the mail IDs of the distribution lists should be added to each line that is to be synchronized to a public namespace. For example:

dlcorp_us@foo.com
dieng_app@foo.com
disupport_us@foo.com

The distinguished name of the LDAP location where distribution list preferences are located. This helps in running multiple esdssyncdl commands simultaneously for a different domain.

The DN of the domain should be the nearest domain under which all distribution lists are present.

For example, assume that the private distribution lists are present under

cn=List,dc=us,dc=foo,dc=com, cn=um_
system, cn=EMailServerContainer, cn=Products, cn=OracleContext

The distinguished name of the preference should be as follows:

dc=us,dc=foo,dc=com, cn=um_
system, cn=EMailServerContainer, cn=Products, cn=OracleContext

If the inputfile and flags=all options are both specified, synchronization occurs based on the inputfile data.

When the sync utility is run for a distribution list that exists in a public namespace, all existing members of the public distribution list are replaced with the members of the private distribution list.
The DBMS_STATS package generates metrics for all Oracle Mail servers. Statistics are transferred between the statistics table and data dictionary, and can be used only when they are stored in the data dictionary. The statistics table enables users to export or import statistics from one database to another. Oracle Mail includes statistics that are collected from a mature system, because there is not enough statistical data when the system is first installed. Users can choose to import these statistics into their systems prior to using their own statistics.

Oracle Mail generates statistical information for each of the various Oracle Mail servers. This information, called metrics, can be used to monitor the health of the Oracle Mail system, and can be viewed using either the Oracle Enterprise Manager 10g Grid Control Console or the oesmon command-line utility.

This appendix includes the following topics:

- Metrics Common to All Oracle Mail Servers
- POP Server Metrics
- IMAP Server Metrics
- SMTP Inbound Server Metrics
- SMTP Outbound Server Metrics
- Housekeeper Server Metrics
- List Server Metrics
- NNTP Inbound Server Metrics
- NNTP Outbound Server Metrics
- Virus Scrubber Server Metrics

### Metrics Common to All Oracle Mail Servers

Table H–1 lists metrics common to all Oracle Mail servers.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.DUMP.DBconnection.dump</td>
<td></td>
</tr>
<tr>
<td>.DUMP.OIDstatus.Connection</td>
<td></td>
</tr>
<tr>
<td>.DUMP.threads.dump</td>
<td></td>
</tr>
<tr>
<td>.esqdb.expand_count</td>
<td></td>
</tr>
</tbody>
</table>
Table H–1  (Cont.) Metrics Common to All Oracle Mail Servers

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.esqudb.pending_request</td>
<td>Operating system process ID</td>
</tr>
<tr>
<td>.esqudb.queue_size</td>
<td>Time since the server has been up</td>
</tr>
<tr>
<td>.esqudb.requests_OK</td>
<td>Number of discarded log messages</td>
</tr>
<tr>
<td>.esqudb.requests_timedout</td>
<td>Number of total log messages</td>
</tr>
<tr>
<td>.esquldap.expand_count</td>
<td></td>
</tr>
<tr>
<td>.esquldap.pending_request</td>
<td></td>
</tr>
<tr>
<td>.esquldap.queue_size</td>
<td></td>
</tr>
<tr>
<td>.esquldap.requests_OK</td>
<td></td>
</tr>
<tr>
<td>.esquldap.requests_timedout</td>
<td></td>
</tr>
<tr>
<td>.um.admin.os_pid</td>
<td></td>
</tr>
<tr>
<td>.um.admin.uptime</td>
<td></td>
</tr>
<tr>
<td>.um.admin.log.discard</td>
<td></td>
</tr>
<tr>
<td>.um.admin.log.total</td>
<td></td>
</tr>
</tbody>
</table>

Table H–2  POP Server Metrics

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.ES_SPS.socket.currload</td>
<td>Current number of client connections</td>
</tr>
<tr>
<td>.ES_SPS.socket.sockmax</td>
<td>Maximum number of client connections allowed</td>
</tr>
<tr>
<td>.ES_SPS.thread.curthreads</td>
<td>Number of threads the server is currently using</td>
</tr>
<tr>
<td>.ES_SPS.thread.thrmax</td>
<td>Maximum number of threads the server creates</td>
</tr>
<tr>
<td>.ESPROTO.uptime</td>
<td>Time since the server has been up</td>
</tr>
<tr>
<td>.ESPROTO.COMMAND.total</td>
<td>Total number of executed commands</td>
</tr>
<tr>
<td>.ESPROTO.COMMAND.P03_COMMAND.totalcalls</td>
<td>Total number of calls for that command</td>
</tr>
<tr>
<td>.ESPROTO.COMMAND.P03_COMMAND.success</td>
<td>Total number of successful calls for that command</td>
</tr>
<tr>
<td>.ESPROTO.COMMAND.P03_COMMAND.fail</td>
<td>Total number of failed calls for that command</td>
</tr>
<tr>
<td>.ESPROTO.USERS.LOGIN.userid</td>
<td>A value of 1 or more indicates that the user is still logged in. Otherwise, it is 0.</td>
</tr>
<tr>
<td>.ESPROTO.connections.lost</td>
<td>Total number of client connections that have disconnected</td>
</tr>
<tr>
<td>.ESPROTO.connections.timeout</td>
<td>Total number of client connections that have timed out</td>
</tr>
<tr>
<td>.ESPROTO.connections.total</td>
<td>Total number of client connections</td>
</tr>
<tr>
<td>.ESPROTO.receive.bytes</td>
<td>Total number of bytes received by the server</td>
</tr>
<tr>
<td>.ESPROTO.transmit.bytes</td>
<td>Total number of bytes sent by the server</td>
</tr>
</tbody>
</table>
### IMAP Server Metrics

Table H–3 lists IMAP server metrics.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.ESPROTO.uptime</td>
<td>Time since the server has been up</td>
</tr>
<tr>
<td>.ESPROTO.COMMAND.total</td>
<td>Total number of executed commands</td>
</tr>
<tr>
<td>.ESPROTO.COMMAND.PO3_COMMAND.totalcalls</td>
<td>Total number of calls for that command</td>
</tr>
<tr>
<td>.ESPROTO.COMMAND.PO3_COMMAND.success</td>
<td>Total number of successful calls for that command</td>
</tr>
<tr>
<td>.ESPROTO.COMMAND.PO3_COMMAND.fail</td>
<td>Total number of failed calls for that command</td>
</tr>
<tr>
<td>.ESPROTO.USERS.LOGIN.userid</td>
<td>A value of 1 or more indicates that the user is still logged in. Otherwise, it is 0.</td>
</tr>
<tr>
<td>.ESPROTO.connections.lost</td>
<td>Total number of client connections that have disconnected</td>
</tr>
<tr>
<td>.ESPROTO.connections.timeout</td>
<td>Total number of client connections that have timed out</td>
</tr>
<tr>
<td>.ESPROTO.connections.total</td>
<td>Total number of client connections</td>
</tr>
<tr>
<td>.ESPROTO.receive.bytes</td>
<td>Total number of bytes received by the server</td>
</tr>
<tr>
<td>.ESPROTO.transmit.bytes</td>
<td>Total number of bytes sent by the server</td>
</tr>
<tr>
<td>.ES_SPS.socket.currload</td>
<td>Current number of client connections</td>
</tr>
<tr>
<td>.ES_SPS.socket.sockmax</td>
<td>Maximum number of client connections allowed</td>
</tr>
<tr>
<td>.ES_SPS.thread.curthreads</td>
<td>Number of threads the server is currently using</td>
</tr>
<tr>
<td>.ES_SPS.thread.thrmax</td>
<td>Maximum number of threads the server creates</td>
</tr>
</tbody>
</table>

### SMTP Inbound Server Metrics

Table H–4 lists SMTP inbound server metrics.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.BS_SPS.socket.currload</td>
<td>Current number of client connections</td>
</tr>
<tr>
<td>.BS_SPS.socket.sockmax</td>
<td>Maximum number of client connections allowed</td>
</tr>
<tr>
<td>.BS_SPS.thread.curthreads</td>
<td>Number of threads the server is currently using</td>
</tr>
<tr>
<td>.BS_SPS.thread.thrmax</td>
<td>Maximum number of threads the server creates</td>
</tr>
<tr>
<td>.MTA.uptime</td>
<td>Time string describing when this MTA came up</td>
</tr>
<tr>
<td>.MTA.connections.in.current</td>
<td>Current number of inbound SMTP Connections</td>
</tr>
<tr>
<td>.MTA.connections.in.total</td>
<td>Total number of inbound SMTP connections</td>
</tr>
<tr>
<td>.MTA.msgs.deferred.current</td>
<td>Current number of messages deferred</td>
</tr>
<tr>
<td>.MTA.msgs.deferred.total</td>
<td>Total number of messages deferred</td>
</tr>
<tr>
<td>.MTA.receive.kbytes</td>
<td>Total number of kilobytes received</td>
</tr>
<tr>
<td>.MTA.receive.messages</td>
<td>Total number of messages received</td>
</tr>
</tbody>
</table>
Table H–5 lists SMTP outbound server metrics.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.MTA.uptime</td>
<td>Time string describing when this MTA came up</td>
</tr>
<tr>
<td>.MTA.connections.broken</td>
<td>Number of broken connections encountered by the MTA</td>
</tr>
<tr>
<td>.MTA.connections.failed</td>
<td>Number of failed connections from the MTA to another MTA</td>
</tr>
<tr>
<td>.MTA.connections.rejected</td>
<td>Number of rejected connections</td>
</tr>
<tr>
<td>.MTA.connections.rejected_reason</td>
<td>Description of the reason for the most recent rejection</td>
</tr>
<tr>
<td>.MTA.connections.out.current</td>
<td>Current number of outbound SMTP connections</td>
</tr>
<tr>
<td>.MTA.connections.out.current.foreign</td>
<td>Current number of outbound SMTP connections to message transfer agents in foreign domains</td>
</tr>
<tr>
<td>.MTA.connections.out.current.native</td>
<td>Current number of outbound SMTP connections to message transfer agents in native domains</td>
</tr>
<tr>
<td>.MTA.connections.out.total</td>
<td>Total number of outbound SMTP connections</td>
</tr>
<tr>
<td>.MTA.connections.out.total.foreign</td>
<td>Total number of outbound SMTP connections to foreign domains</td>
</tr>
<tr>
<td>.MTA.connections.out.total.native</td>
<td>Total number of outbound SMTP connections to message transfer agents in native domains</td>
</tr>
<tr>
<td>.MTA.dl.receive.count</td>
<td>Number of messages sent to distribution lists</td>
</tr>
<tr>
<td>.MTA.msgs.deferred.current</td>
<td>Current number of messages deferred</td>
</tr>
<tr>
<td>.MTA.msgs.deferred.total</td>
<td>Total number of messages deferred</td>
</tr>
</tbody>
</table>
Table H–6 lists Housekeeper server metrics.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.MTA.mgs.deferred.totaltime</td>
<td>Total time inserting data into the database</td>
</tr>
<tr>
<td>.MTA.ndr.inbound</td>
<td>Total number of nondelivery reports generated by inbound mail</td>
</tr>
<tr>
<td>.MTA.ndr.loop</td>
<td>Total number of messages not delivered due to mail loops</td>
</tr>
<tr>
<td>.MTA.ndr.outbound</td>
<td>Total number of nondelivery reports generated by outbound mail</td>
</tr>
<tr>
<td>.MTA.queued.out.kbytes</td>
<td>Kilobytes queued awaiting to be sent out to the Internet</td>
</tr>
<tr>
<td>.MTA.queued.out.messages</td>
<td>Messages queued awaiting to be sent out to the Internet</td>
</tr>
<tr>
<td>.MTA.transmit.bytes</td>
<td>Total number of bytes transmitted</td>
</tr>
<tr>
<td>.MTA.transmit.bytes_foreign</td>
<td>Total number of bytes transmitted to foreign domain MTAs</td>
</tr>
<tr>
<td>.MTA.transmit.bytes_local</td>
<td>Total number of bytes transmitted to local entities</td>
</tr>
<tr>
<td>.MTA.transmit.messages</td>
<td>Total number of messages transmitted</td>
</tr>
<tr>
<td>.MTA.transmit.messages_foreign</td>
<td>Total number of messages transmitted to foreign domain MTAs</td>
</tr>
<tr>
<td>.MTA.transmit.messages_local</td>
<td>Total number of messages transmitted to local entities</td>
</tr>
<tr>
<td>.MTA.transmit.messages_native</td>
<td>Total number of messages transmitted to native domain MTAs</td>
</tr>
<tr>
<td>.MTA.transmit.messages_relay</td>
<td>Total number of messages transmitted during relay operations</td>
</tr>
<tr>
<td>.MTA.transmit.recipients</td>
<td>Total number of recipients transmitted</td>
</tr>
<tr>
<td>.MTA.transmit.recipients_foreign</td>
<td>Total number of recipients transmitted to foreign domain</td>
</tr>
<tr>
<td>.MTA.transmit.recipients_local</td>
<td>Total number of recipients transmitted to local entities</td>
</tr>
<tr>
<td>.MTA.transmit.recipients_native</td>
<td>Total number of recipients transmitted to native domain MTAs</td>
</tr>
<tr>
<td>.MTA.transmit.time</td>
<td>Total time transmitting data</td>
</tr>
<tr>
<td>.MTA.transmit.time_foreign</td>
<td>Total time transmitting data to foreign domain MTAs</td>
</tr>
<tr>
<td>.MTA.transmit.time_native</td>
<td>Total time transmitting data to native domain MTAs</td>
</tr>
<tr>
<td>.MTA.transmit.time.local</td>
<td>Total time transmitting data to local entities</td>
</tr>
<tr>
<td>.MTA.transmit.time.relay</td>
<td>Total time transmitting data during relay operations</td>
</tr>
</tbody>
</table>

Housekeeper Server Metrics

Table H–5 (Cont.) SMTP Outbound Server Metrics

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.GC.processed.expirables</td>
<td>Number of message instances expired by a particular Housekeeper instance</td>
</tr>
<tr>
<td>.GC.processed.prunables</td>
<td>Number of message instances removed from the system trash folder by a particular Housekeeper instance</td>
</tr>
<tr>
<td>.GC.processed.queued_prunables</td>
<td>Number of message references removed from the system trash queue by a particular Housekeeper instance</td>
</tr>
<tr>
<td>.GC.processed.collectables</td>
<td>Number of unreferenced messages removed from the system by a particular Housekeeper instance</td>
</tr>
<tr>
<td>.GC.processed.tertiary_storables</td>
<td>Number of messages moved to tertiary storage by a particular Housekeeper instance</td>
</tr>
</tbody>
</table>
### List Server Metrics

Table H–7 lists List Server metrics.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.SLIST.connections.busy</td>
<td>Number of busy database connections</td>
</tr>
<tr>
<td>.SLIST.connections.total</td>
<td>Total number of database connections</td>
</tr>
<tr>
<td>.SLIST.process.current_mails</td>
<td>Number of mails being processed currently by the List Server</td>
</tr>
<tr>
<td>.SLIST.process.current_user_threads</td>
<td>Number of threads in the List Server that are delivering mails to users</td>
</tr>
<tr>
<td>.SLIST.process.total_mails</td>
<td>Total number of mails processed by the List Server since startup</td>
</tr>
<tr>
<td>.SLIST.queue.pending</td>
<td>Number of e-mails waiting to be processed by the List Server</td>
</tr>
</tbody>
</table>

### NNTP Inbound Server Metrics

Table H–8 lists NNTP inbound server metrics.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.ES_SPS.socket.currload</td>
<td>Current number of client connections</td>
</tr>
<tr>
<td>.ES_SPS.socket.sockmax</td>
<td>Maximum number of client connections allowed</td>
</tr>
<tr>
<td>.ES_SPS.thread.currthreads</td>
<td>Number of threads the server is currently using</td>
</tr>
<tr>
<td>.ES_SPS.thread.thrmax</td>
<td>Maximum number of threads the server creates</td>
</tr>
<tr>
<td>.es.nntp.in.clients.flood.conns</td>
<td>Number of times the server has detected connection floods from a single client</td>
</tr>
<tr>
<td>.es.nntp.in.art.cache.hit</td>
<td>Article cache hits</td>
</tr>
<tr>
<td>.es.nntp.in.art.cache.miss</td>
<td>Article cache misses</td>
</tr>
<tr>
<td>.es.nntp.in.clients.article</td>
<td>Number of ARTICLE commands from clients</td>
</tr>
<tr>
<td>.es.nntp.in.clients.current</td>
<td>Number of connected clients</td>
</tr>
<tr>
<td>.es.nntp.in.clients.group</td>
<td>Number of GROUP commands from clients</td>
</tr>
<tr>
<td>.es.nntp.in.clients.list</td>
<td>Number of LIST commands from clients</td>
</tr>
<tr>
<td>.es.nntp.in.clients.post</td>
<td>Number of POST commands from clients</td>
</tr>
<tr>
<td>.es.nntp.in.clients.total</td>
<td>Number of clients serviced so far</td>
</tr>
</tbody>
</table>
### NNTP Outbound Server Metrics

Table H–9 lists NNTP outbound server metrics.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.es.nntp.out.threads</td>
<td>Number of live feed threads, may be zero</td>
</tr>
<tr>
<td>.es.nntp.out.conn.cache.hit</td>
<td>Connection cache hits</td>
</tr>
<tr>
<td>.es.nntp.out.conn.cache.miss</td>
<td>Connection cache misses</td>
</tr>
<tr>
<td>.es.nntp.out.traffic.errors</td>
<td>Feed errors</td>
</tr>
<tr>
<td>.es.nntp.out.traffic.messages</td>
<td>Feed messages</td>
</tr>
<tr>
<td>.es.nntp.out.traffic.rejects</td>
<td>Feed rejects</td>
</tr>
</tbody>
</table>

### Virus Scrubber Server Metrics

Table H–10 lists Virus Scrubber server metrics.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.VSCRUB.processed.prescan</td>
<td>Number of messages prescanned by the server</td>
</tr>
<tr>
<td>.VSCRUB.processed.scan</td>
<td>Number of messages scanned by external virus scanning software using this server</td>
</tr>
<tr>
<td>.VSCRUB.processed.infected</td>
<td>Number of messages deemed infected by the virus scanning software</td>
</tr>
<tr>
<td>.VSCRUB.processed.repaired</td>
<td>Number of messages deemed infected by the virus scanning software but able to repair and restore</td>
</tr>
<tr>
<td>.VSCRUB.pending.scan</td>
<td>Number of messages isolated by prescanning but yet to be scanned by external virus scanning software</td>
</tr>
<tr>
<td>.VSCRUB.threads.count</td>
<td>Number of active virus scanner threads at the moment</td>
</tr>
</tbody>
</table>
This appendix contains information necessary for using a plug-in for Oracle Mail user provisioning. It contains examples of various provisioning operations, including:

- Generating a User ID Based on User’s First and Last Names
- Assigning an Oracle Collaboration Suite Database Based on Country
- Establish Mail Quota Dynamically Based on Title
- Selectively Provision Users for Oracle Mail

To make customizations during Oracle Mail user creation through a centralized provisioning framework, administrators must implement additional code. This code must be in a class called `EmailCustomPolicyPlugin` contained in the `oracle.mail.provisioning.policy` package. This class must implement the `oracle.mail.provisioning.plugin.EmailPolicyPluginInterface` present in the `$ORACLE_HOME/jlib/esprovisioning.jar` file.

Customizations similar to the following examples, according to customer requirements, can be done by implementing this policy interface.

```java
package oracle.mail.provisioning.policy;

import oracle.mail.provisioning.plugin.EmailPolicyPluginInterface;
import oracle.idm.user.IdmUser;
import oracle.idm.provisioning.plugin.ApplicationContext;
import oracle.idm.provisioning.plugin.PluginException;
import oracle.idm.provisioning.plugin.PluginStatus;
import oracle.ldap.util.LDIF;
import oracle.ldap.util.ModPropertySet;

Any changes made by administrator implementation will eventually be merged by the centralized provisioning framework and will go into effect when a user is created.

```java
public class EmailCustomPolicyPlugin implements EmailPolicyPluginInterface {

    The `processPolicy` method in the `EmailCustomPolicyPlugin` class is invoked by the Oracle Mail pre-data-entry plug-in. If customizations are required in a deployment, this method must be implemented.

    The centralized provisioning framework passes two `ModPropertySet` objects containing changes made to `baseuser` attributes and `mailuser` attributes so far in the pre-data-entry plug-in. The `baseuser` attributes and `mailuser` attributes are the attributes for the base user and Oracle Mail user, respectively. When the Oracle Mail provisioning plug-in invokes the implemented plug-in, it passes the original
ModPropertySet for the baseuser attribute containing base user attributes passed by the centralized provisioning framework to the Oracle Mail plug-ins, and two additional ModPropertySet instances for baseuser and mailuser attribute changes, respectively.

If changes must be made to any baseuser attribute, such as deriving a user ID based on first name and last name, those changes must be done in the ModPropertySet for the base user changes.

Similarly, make changes to the mailuser attribute, such as assigning an Oracle Collaboration Suite Database or changing quota, in the ModPropertySet for mail user changes.

The processPolicy method and its parameters are as follows:

```java
public void processPolicy(ApplicationContext appCtx,
        IdmUser idmUser,
        ModPropertySet originalBaseUserAttrs,
        ModPropertySet originalMailUserAttrs,
        ModPropertySet modifiedBaseUserAttrs,
        ModPropertySet modifiedMailUserAttrs,
        PluginStatus pluginStatus)
    throws PluginException {
```

- **appCtx**: This parameter contains the jndi DirContext, type of operation, locale, and logging.
- **idmUser**: This parameter contains base user attributes used in modify and delete operations. In a create operation, if any application needs the global user ID, it can be obtained here.
- **originalBaseUserAttrs**: This parameter contains the original base user attributes that Oracle Delegated Administration Services or Oracle Directory Integration and Provisioning passes to Oracle Mail plug-ins.
- **originalMailUserAttrs**: This parameter contains the original Oracle Mail user attributes that Oracle Delegated Administration Services or Oracle Directory Integration and Provisioning passes to Oracle Mail plug-ins.
- **modifiedBaseUserAttrs**: This parameter contains any changes made to current base user attributes in the e-mail pre-data-entry plug-in. As a part of customization, the baseuser attribute values that need to be modified can be set in this parameter.
- **modifiedMailUserAttrs**: This parameter contains any changes made to current Oracle Mail user attributes in the e-mail pre-data entry plug-in. As a part of customization, the mailuser attribute values that must be modified can be set in this parameter.
- **PluginStatus**: This is the plug-in status object, which can contain provisioning status, description, and an execution status. These values are consumed by the provisioning framework.
- **PluginException**: This exception generates PluginException in case of errors.

See Also: Oracle Internet Directory API Reference for more information
Generating a User ID Based on User’s First and Last Names

This example generates a user ID, assigns an Oracle Collaboration Suite Database, and establishes mail quota during user creation.

```java
String op_type = appCtx.getCallOp();
if (op_type.equals(ApplicationContext.OP_CREATE)) {
    // The preceding code checks if it is a create operation.
    String firstname = originalBaseUserAttrs.getModPropertyValue("givenname");
    String lastname = originalBaseUserAttrs.getModPropertyValue("sn");
    if ((firstname != null) && (lastname != null)) {
        String mailid = firstname + "." + lastname + "@foo.com";
        // The preceding code generates the user ID from the firstname and lastname of the base user.
        modifiedBaseUserAttrs.deleteProperty("mail");
        modifiedBaseUserAttrs.addProperty(LDIF.ATTRIBUTE_CHANGE_TYPE_ADD, "mail", mailid);
    }
}
```

Assigning an Oracle Collaboration Suite Database Based on Country

This example assigns an Oracle Collaboration Suite Database based on the country in which the user resides or works. This example assumes the following:

- Oracle Collaboration Suite Database assignment is according to the user country
- Country information is stored in the c attribute of the base user
- Oracle Collaboration Suite Database name for the USA is usdb.foo.com
- Oracle Collaboration Suite Database name for India is indb.foo.com
- Oracle Collaboration Suite Database for all other users is ocsms.foo.com

```java
String country = originalBaseUserAttrs.getModPropertyValue("c");
if (country != null) {
    String mailstore = "ocsms.foo.com";
    if (country.equalsIgnoreCase("usa"))
        mailstore = "usdb.foo.com";
    if (country.equalsIgnoreCase("india"))
        mailstore = "indb.foo.com";
    // Assigning mailstore based on country.
}
```

Establish Mail Quota Dynamically Based on Title

This example assigns higher mail quota to managers, while for all other users, the default mail quota that is set at the domain level applies. This example assumes the following:

- The title attribute of the base user is Manager for managers
- Assign 200 MB of mail quota to managers

```java
String title = originalBaseUserAttrs.getModPropertyValue("title");
if ((title != null) && (title.equalsIgnoreCase("manager"))) {
    modifiedMailUserAttrs.deleteProperty("orclmailquota");
    modifiedMailUserAttrs.addProperty(LDIF.ATTRIBUTE_CHANGE_TYPE_ADD, "orclmailquota", "200MB");
}
```
Selectively Provision Users for Oracle Mail

This example provisions users selectively. This example assumes the following:

If the `title` attribute of the base user is `temporary`, do not provision.

```java
if ((title != null) && (title.equalsIgnoreCase("temporary"))) {
    pluginStatus.setProvStatus(IdmUser.PROVISION_NOT_REQUIRED);
}
```

Setting the provisioning status to `PROVISION_NOT_REQUIRED` causes Oracle Delegated Administration Services to show no provisioning for Oracle Mail, and Oracle Directory Integration and Provisioning does not create an Oracle Mail user.

If the custom plug-in requires any base user attributes other than `mail`, run the `oidprovtool` utility in the Applications tier or Oracle Collaboration Suite Infrastructure (Infrastructure) `$ORACLE_HOME` to add the additional attributes, as in the following example, where `cn` and `sn` attributes are added:

```bash
oidprovtool operation=modify ldap_host=OID_HOST ldap_port=OID_PORT
ldap_user_dn='cn=orcladmin' ldap_user_password=ORCLADMIN_PASSWORD
application_type=EMAIL
application_dn='cn=EmailServerContainer,cn=Products,cn=OracleContext'
application_name=EMAIL
event_subscription='USER:ANY:MODIFY(mail,dn,orcluserApplnProvStatus;email)'
event_subscription='USER:ANY:ADD (mail,dn,orclguid,cn,sn)'
event_subscription='USER:ANY:DELETE' interface_version=3.0
```

This example assumes the following:

- `OID_HOST` is the Infrastructure Oracle Internet Directory host name
- `OID_PORT` is the Infrastructure Oracle Internet Directory port number
- `ORCLADMIN_PASSWORD` is the password for `cn=orcladmin`

**Note:** Ensure that `mail`, `dn`, `orclguid` attributes are always included in the list of subscribed attributes. Otherwise, e-mail provisioning will not work as expected.

To compile and load the policy jar file, follow these instructions on an Applications tier `$ORACLE_HOME`. In multiple Applications tiers, these steps must be performed on the Applications tier that contains the latest Oracle Mail provisioning patches.

1. To compile `EmailCustomPolicyPlugin.java`, the CLASSPATH must include the following jar files:

   ```bash
   $ORACLE_HOME/jlib/esprovisioning.jar
   $ORACLE_HOME/jlib/ldapjclnt10.jar
   ```

2. Compile the policy plug-in.

   ```bash
   $ORACLE_HOME/jdk/bin/javac
   oracle/mail/provisioning/policy/EmailCustomPolicyPlugin.java
   ```
3. Create the policy plug-in jar file.

   
   $ORACLE_HOME/jdk/bin/jar cvf $ORACLE_HOME/oes/provisioning_policyplugin/policyplugin.jar oracle/mail/provisioning/policy/*.class

4. Load the policy jar file into the provisioning framework.

   Substitute $ORACLE_HOME with the full path of the Applications tier $ORACLE_HOME and create an ldif file with following lines:

   ```
   dn: cn=Plugins, cn=EMAIL, cn=Applications, cn=Provisioning,cn=Directory Integration Platform,cn=Products,cn=OracleContext
   changetype: modify
   replace: orclODIPPluginExecData
   orclODIPPluginExecData: $ORACLE_HOME/jlib/esprovisioning.jar
   
   dn: cn=Plugins, cn=EMAIL, cn=Applications, cn=Provisioning,cn=Directory Integration Platform,cn=Products,cn=OracleContext
   changetype: modify
   add: orclODIPPluginExecData
   orclODIPPluginExecData: $ORACLE_HOME/oes/provisioning_policyplugin/policyplugin.jar
   ```

   Assuming the ldif file is $ORACLE_HOME/oes/provisioning_policyplugin/loadpolicy.ldif, run the following command to upload the policy jar file into the provisioning framework:

   ```
   $ORACLE_HOME/bin/ldapmodify -b -v -Dcn=orcladmin -w orcladmin_password -h oid_host -p oid_port -f $ORACLE_HOME/oes/provisioning_policyplugin/loadpolicy.ldif
   ```
absent transaction support
The inability to perform both the Oracle Collaboration Suite Database and Oracle Internet Directory operations for an e-mail schema entry at one time.

address resolution
Address resolution resolves a contact name into its corresponding e-mail address.

alias
Alternate e-mail address for a recipient.

antispam
See routing control

archive policy
An archive policy is a set of conditions applied to user e-mail that stores all user e-mail in a third-party storage facility.

auto-complete
Quickly searches for and completes an e-mail address as soon as one or a few letters of a contact name is entered. A list of contacts is displayed if more than one possible match exists.

back end
A term used to describe where the Oracle Collaboration Suite Database runs.

beacon transaction
A utility or a script that reaches out, like a beacon, to check on a given metric, source, or anything that concerns the administrator.

delivery status notification (DSN)
A notification sent back to the sender of an e-mail message regarding the status of the message. DSNs can be sent out to notify the sender of failed, delayed, or successful delivery of a message.

demilitarized zone (DMZ)
A computer or small subnetwork that exists between a trusted internal network, such as a corporate private LAN, and an untrusted external network, such as the public Internet.
Directory Cache
A component of Oracle Mail that builds an in-memory, cached copy of the corporate directory, enabling faster lookup of user information when using the Oracle WebMail client.

distribution list
An alias or e-mail ID that represents a group of recipients.

DMZ
See demilitarized zone (DMZ)

DNS
See domain name server (DNS)

domain
Most commonly refers to a group of computers whose host names share a common suffix, the domain name.

domain name server (DNS)
An Internet service that translates domain names into IP addresses.

DSN
See delivery status notification (DSN)

filter
A set of specific conditions that is applied to a message in various stages of the delivery cycle to prevent viruses and other harmful agents from accessing the Oracle Mail system.

firewall
Software installed on a special piece of hardware, such as a router, that acts as an intermediary to protect a set of computers or networks from outside attack. It regulates access to computers on a local area network from outside, and regulates access to outside computers from within the local area network. A firewall can work either by acting as a proxy server that forwards requests so that the requests behave as though they were issued by the firewall computer, or by examining requests and attempting to eliminate suspect calls.

flashback mail recovery
Process of using Oracle Flashback Query to recover e-mail from the Oracle Collaboration Suite Database.

Housekeeper
A background process that works inside the Oracle Collaboration Suite Database and performs periodic tasks, such as garbage collection, which cleans up deleted message bodies. Additional tasks include performing Oracle Text index synchronization and optimization for enabling message body search, and moving message bodies to tertiary storage tablespaces.

identity management
The creation, management, and use of online, or digital, entities. Identity management involves securely managing the full life cycle of a digital identity from creation
(provisioning of digital identities) to maintenance (enforcing organizational policies regarding access to electronic resources), and, finally, to termination.


**IMAP**

*See Internet Message Access Protocol (IMAP)*

**init.ora**

A file containing database parameters present in `ORACLE_HOME`. But the file that the database uses, by default, is `initSID.ora` where `SID` is the database SID. The administrator can also edit the name of the file.

**instance**

An individual process of an Oracle Mail server.

**Internet Message Access Protocol (IMAP)**

A protocol for retrieving e-mail messages.

**LDAP**

*See Lightweight Directory Access Protocol (LDAP)*

**Lightweight Directory Access Protocol (LDAP)**

A set of protocols for accessing information directories. LDAP is based on the standards contained within the X.500 standard, but is significantly simpler.

**List Server**

Mail server that processes messages addressed to *distribution lists*.

**message transfer agent (MTA)**

The program responsible for receiving incoming e-mail and delivering the messages to individual users.

**middle tier**

*See Oracle Collaboration Suite Applications tier*

**MTA**

*See message transfer agent (MTA)*

**MX record**

A mail exchange (MX) record is an entry in a domain name database that identifies the mail server that is responsible for handling e-mails for that domain name.

**Network News Transport Protocol (NNTP)**

The protocol used to post, distribute, and retrieve USENET messages. The official specification is RFC977.

**news site**

One or more news servers used by the same community of users.
**newsgroup**
A repository usually within the Usenet system, for messages posted from many users at different locations.

**NNTP**
Network News Transport Protocol (NNTP)

**oidadmin**
The administration tool for Oracle Internet Directory. It provides LDAP access to all of the attributes and objects within Oracle Internet Directory relating to application using Oracle Internet Directory as its directory store, such as Oracle Mail.

**Oracle Application Server Portal**
Oracle Application Server Portal (OracleAS Portal) is a complete solution for building, deploying and monitoring Web database applications and content-driven Web sites. OracleAS Portal enables you to create and view database objects through an easy-to-use HTML-based interface, and provides tools for creating HTML-based interfaces. It also enables you to resolve performance problems using performance tracking facilities, and enables you to manage database security through its interface.

**Oracle Collaboration Suite 10g Database**
See Oracle Collaboration Suite Database

**Oracle Collaboration Suite Applications tier**
The second tier in a typical three-tier architecture, in which the first tier is the host where the client is running; the second tier is the host running the Oracle Collaboration Suite processes; and the third tier is where the Oracle Collaboration Suite Database runs.

**Oracle Collaboration Suite Database**
The database upon which Oracle Mail user data is stored.

**Oracle Mail**
The e-mail component of Oracle Collaboration Suite.

**Oracle Internet Directory**
Oracle Internet Directory is a general purpose directory service that enables retrieval of information about dispersed users and network resources. Oracle Internet Directory combines LDAP version 3 with the high performance, scalability, robustness, and availability of Oracle Database 10g.

**Oracle Text**
A feature of Oracle Database 10g that provides advanced search and retrieval services on content stored in an Oracle repository. It is fully integrated into OracleAS Portal to provide users with the ability to perform a full text search and retrieval of content managed within the OracleAS Portal schema of the Oracle Application Server Metadata Repository. It also provides automatic grouping and classification of results by gist and theme.

**Oracle WebMail**
Browser-based client for accessing e-mail.
**parameter**
In general, parameters are characteristics used to customize a program. For example, file names, page lengths, and font specifications could all be considered parameters.

**peer**
A news server that exchanges news articles.

**POP**
*See* Post Office Protocol (POP)

**Post Office Protocol (POP)**
A protocol used to retrieve e-mail from a mail server.

**process**
An executing program.

**quota**
Quota refers to the amount of predetermined space each user is allotted to store messages in the Oracle Collaboration Suite Database.

**redo logs**
A set of files that protect altered database data in memory that has not been written to the data files. The redo log can consist of two parts: the online redo log and the archived redo log.

**routing control**
Accept or reject messages based on the policies defined for the SMTP server.

**SASL**
*See* Simple Authentication and Security Layer (SASL)

**Secure/Multipurpose Internet Mail Extensions (S/MIME)**
Standard for signing and encrypting mail messages.

**Secure Sockets Layer (SSL)**
An industry standard protocol designed by Netscape Communications Corporation for securing network connections. SSL provides authentication, encryption, and data integrity using public key infrastructure (PKI).

**server**
A computer program that stays up all the time and serves a task.

**server-side rule**
A rule that is processed (applied) by the server.

**Simple Authentication and Security Layer (SASL)**
A method for adding authentication support to connection-based protocols. To use this specification, a protocol includes a command for identifying and authenticating a user to a server and for optionally negotiating a security layer for subsequent protocol interactions. The command has a required argument identifying a SASL mechanism.

**Simple Mail Transfer Protocol (SMTP)**
A protocol for sending e-mail messages between servers.
S/MIME
See Secure/Multipurpose Internet Mail Extensions (S/MIME)

SMTP
See Simple Mail Transfer Protocol (SMTP)

spam
Unsolicited bulk e-mail.

SSL
See Secure Sockets Layer (SSL)

tertiary storage
Tertiary storage is a separate tablespace used to hold old messages. Using a separate tablespace allows administrators to use a possibly larger (and cheaper) storage medium, different from the active storage area for new messages.

thin client
An application that executes the user interface within a Web browser and the business logic on a remote server. In the context of this document, thin client refers to Oracle WebMail.

TLS
See Transport Layer Security (TLS)

Transport Layer Security (TLS)
A cryptographic protocol that provides secure communication over the Internet.

user ID
A user’s e-mail address or a truncated version of it, such as user.name or uname.

Virus Scrubber
Name of the mail server process that can fetch messages from the Oracle Collaboration Suite Database and pass them through a virus scanner.
A

actions
server-side rules, 9-5

address rewriting rules
  components, 3-18, 3-19
defined, 3-17
designing, 3-21
host, 3-17
mailer, 3-17
operators
defined, 3-20
tokens, 3-19
user, 3-17

administrative privileges
domain, 1-1
system, 1-1

alias attributes, 2-23
aliases, 2-22, 2-23
antispm, 6-5
antispm checks
  for NNTP server, 6-9
  for SMTP server, 6-6
antispm protection
  third-party filter, 6-5
antispm protection
  applying SAVSE filters, 6-10
archive policies, 8-26
  creating, 8-27
  editing, 8-28
attributes
  alias, 2-23
distribution list, 2-13, 2-16
domain, 2-12
E-Mail Collaboration Suite Database target, 7-6
E-Mail IMAP Service target, 7-4
E-Mail SMTP Inbound Service target, 7-5
newsgroup, 2-27
Oracle Internet Directory Client target, 7-7
peer server, 2-25
See Also
parameters
server-side rules, 9-5
user, 2-2
auto-complete, 5-1
automatic reply
e-mail feature, 2-5

automatically complete
See auto-complete

B

backup
  about oesbp utility, 10-2
  Oracle Collaboration Suite Database, 10-1
  Oracle Mail, 10-1
beacon transactions, A-1
blocking messages, D-25
bounce processing
  about, 3-38

C

capturing outbound messages, D-26
cold backup
database backup utility, 10-2
collection
  enabling, 3-25
  Housekeeper server tasks
deleted message collection, 3-24
command-line utilities
oeschart, 7-11
oeschk, D-30
oesctl
  about, D-16
  examples, D-18
oesdl, D-2
  examples, D-4
oesmon, 7-9
oesng, D-6
  examples, D-8
oespr
  about, D-9
  examples, D-10
oesrl
  about, D-24
  creating server-side rules, 9-9
  displaying server-side rules, 9-8
  editing server-side rules, 9-9
oesucr
  about, D-11
  examples, D-12
oesutil, D-45
oidadmin, 3-33
omnctl
   about, D-16
conditions
   server-side rules, 9-3
copying messages to a folder, D-27
copying outgoing messages, D-26
corporate directory
   See Oracle Internet Directory
creating aliases, 2-22
creating graphs
   oeschart, 7-14
cctxsys
database user, 3-27

D

DBMS_STATS package, H-1
deleting aliases, 2-23
deleting server-side rules, D-25
deprovisioning
   users
   Oracle WebMail, 2-8
Directory Cache, 5-1
   pass-through mode, 5-1
Directory Provider
   defined, 5-1
discarding all messages, D-26
distribution lists
   adding users, 2-21
   adding users to a new command line, D-5
   adding users to an existing command line, D-5
archiving posts
   defined, 3-34
   attributes, 2-13, 2-16
   bounce processing, 3-38
   creating, 2-19
   deleting, 2-21
   command line, D-6
external
   defined, 3-35
group types, 2-15
lookup
   dlsync, G-2
   enabling, G-2
managing, 2-12
managing users, 2-21
modifying, 2-20
   modifying default parameter values, 2-20
   parameters, 2-16
posting types, 2-15
removing members, 2-21
   command line, D-6
   removing users, 2-21
   showing all to which a user subscribes, 2-22
subscription types, 2-15
dlsync
distribution list lookup utility, G-2
DNS, 3-12
domain administrator
   defined, 1-1
domain attributes, 2-12
   flashback mail recovery, 2-12
   location in public namespace, 2-12
   naming attribute for creation in public namespace, 2-12
   objectclasses for creation in public namespace, 2-12
domain name server
   See DNS
domains
   about, 2-10
   creating, 2-11
deleting
   using oesutil utility, D-45
   managing
      modifying default distribution list parameter values, 2-20
      setting default user attributes, 2-6
      modifying settings, 2-11
E

editing alias attributes, 2-23
e-mail
domains, 2-10
group target, 7-8
messages
   life cycle of, 9-1
   quota, 2-3
   recovering deleted, 2-9
   user attributes
      e-mail user account name, 2-2
      users
         adding, 2-2
         modifying attributes, 2-4
         removing, 2-8
         setting default attributes, 2-6
e-mail alias lookup
   enabling, G-1
e-mail server directory service
   See ESDS
error messages
   Housekeeper server, B-6
   IMAP server, B-1
   List Server, B-7
   NNTP server, B-8
   Oracle Webmail, B-11
   overview, B-1
   POP server, B-1
   SMTP server, B-4
   Virus Scrubber server, B-11
es_perf_data view, 7-14
es_perf_metric table, 7-13
es_perf_process table, 7-12
es_perf_sample table, 7-13
es_perf_timestamp table, 7-13
esd_check_quota_usage.pl script, D-48
esd_copy_messages.sql script, D-53
esd_find_message.sql script, D-49
esd_list_folder_messages.sql script, D-54
esd_list_unopened_inbox.sql script, D-54
esd_list_user_folders.sql script, D-54
esd_logsCan.pl script, D-46
esd_queue_queue.sql script, D-53
esd_queue_examine.sql script, D-49
esd_show_message.sql script, D-50
esd_show_session_usage.sql script, D-56
esd_show_sessions.sql script, D-55
ESDS, 3-11
esdssyncdl
distribution list synchronization utility, G-4
synchronizing distribution lists, G-4
esperftbl tablespace, 7-12
ESTERSTORE tablespace
defined, 3-31
moving, 3-31
events
server-side rules, 9-2
export backup
database backup utility, 10-1
expressions
server-side rules, 9-4

F
filters, 8-2
applying, 8-4
applying to Collaboration Suite Database, 8-5
creating, 8-2
editing, 8-3
editing applied, 8-7
reordering, 8-3
firewalls, 6-4
flashback mail recovery, 2-12
See Also Oracle Flashback Query

G
garbage collection
See collection
graphs
displaying in Oracle Enterprise Manager, 7-16
Grid Control Console
See Oracle Enterprise Manager 10g Grid Control Console

H
hot backup
database backup utility, 10-2
Housekeeper server, 3-23
creating a text indexing process, 3-29
dynamically starting and stopping tasks
command line, D-23
enabling process control message cleanup, 3-25
error messages, B-6
message recovery
configuring to record deleted messages, 3-26
metrics, H-5
parameters
debug, F-5
general, F-3
Housekeeping Operations, F-3
tasks, 3-23
collection, 3-24
index synchronization, 3-24
tertiary storage, 3-24
tertiary storage, 3-32
troubleshooting, A-18
housekeeping
see Housekeeper server

I
identity management
e-mail system component, 6-3
IMAP
defined, 3-9
troubleshooting, A-14
IMAP server, 3-9
error messages, B-1
metrics, H-3
parameters
debug, F-11
general, F-8
rules and routing control, F-7
shared message flags, F-7
thread, F-6
process architecture, 3-10
IMAP4
See IMAP
index synchronization, 3-24
indexes
defined, 3-27
information storage database
e-mail system component, 6-2
See Also Oracle Collaboration Suite Database
Internet Message Access Protocol
See IMAP

L
LDAP objectclasses
for creation in public namespace, 2-12
groupofnames, 2-12
groupofuniquenames, 2-12
Lightweight Directory Access Protocol
See LDAP
list
See distribution lists
List Server, 3-33
distribution list attributes, 2-13
error messages, B-7
mail interface, 3-34
mail merge
defined, 3-38
types, 3-38
metrics, H-6
parameters
  debug, F-33
  DSN, F-26
  general, F-30
  rules and routing control, F-27
  SMTP protocol timeouts, F-25
  target-level settings, F-25
log files
  about, 3-3
  location
    Directory Cache, 5-2
    oesbkp utility, 10-3
    Oracle WebMail, 4-9
    Virus Scrubber, 6-15
LogMiner
  about, 10-4
  configuring Housekeeper server process, 3-26
  enabling supplemental logging, 3-26
  recovering deleted e-mail, 2-9
  setting up, 3-26
lookup
  creating a referral, G-2
  enabling distribution list, G-2
  enabling e-mail alias, G-1
M
  mail clients
    e-mail system component, 6-3
    troubleshooting, A-3
  mail delivery
    troubleshooting, A-7
  mail merge
    defined, 3-38
    PL/SQL mail merge, 3-39
    scheduled mail delivery
      defined, 3-41
      standard mail merge, 3-39
      types, 3-38
  MAIL_RECOVERY_FQ package
    recovering messages, 10-8
  message archiving, 8-26, 8-27, 8-28
  enabling, 8-29
  message cleanup, 3-25
  message recovery
    Housekeeper server process
      configuring to record deleted messages, 3-26
    LogMiner, 10-4
      enabling supplemental logging, 3-26
      setting up Oracle Collaboration Suite Database, 3-26
      recovering deleted e-mail, 2-9
  message transfer agent
    See MTA
metrics
  about, H-1
  common to all servers, H-1
  Housekeeper server, H-5
  IMAP server, H-3
  List Server, H-6
  NNTP inbound server, H-6
  NNTP outbound server, H-7
  POP server, H-2
  SMTP inbound server, H-3
  SMTP outbound server, H-4
  Virus Scrubber server, H-7
middle tier
  See Oracle Collaboration Suite Applications tier
  MTA, 3-13
  MX record, 3-13

N
  Network News Transport Protocol
    See NNTP
  news peers
    adding
      command line, D-9
    deleting
      command line, D-9
  news servers, 3-42
  newsgroups
    adding private, 2-27
    adding public, 2-29
    attributes, 2-27
    creating public
      command line, D-8
    creating public moderated
      command line, D-8
    creating simple public
      command line, D-8
    defined, 2-26
    deleting private, 2-28
    deleting public, 2-30
      command line, D-9
    editing private, 2-28
    editing public, 2-29
    private, 2-26
    public, 2-26
  NNTP
    defined, 3-41
    news servers, 3-42
    news site, 3-42
    newsgroups, 3-42
    peer, 3-42
  NNTP inbound server metrics, H-6
    parameters
      access and routing control, F-13
      debug, F-15
      general, F-14
      thread, F-12
  NNTP outbound server metrics, H-7
    parameters
      debug, F-17
      general, F-16
      thread, F-16
  NNTP server
    antispam checks, 6-9
caching articles  
defined, 3-43
error messages, B-8
inbound  
defined, 3-43
outbound  
defined, 3-43
routing control, 6-9

oc4j.properties
- Oracle WebMail, 4-3
oesbkp utility
- about, 10-2
  backup files, 10-4
  logging information, 10-3
  parameters and definitions, 10-3
  syntax, 10-2
oeschart utility
- about, 7-11
  creating graphs, 7-14
oeschk utility
- about, D-30
oesctl utility
- about, D-16
  creating server instances, D-18
  deleting server instances, D-19
  disabling server instances, D-20
  enabling servers, D-19
  examples, D-18
  listing server instances, D-19
  listing servers, D-18
  showing server instance status, D-23
  showing server process status, D-23
  synchronizing configuration to opmn.xml, D-20
oesdl utility
- about, D-2
  adding users to a new distribution list, D-5
  adding users to an existing distribution list, D-5
  deleting a distribution list, D-6
  examples, D-4
  removing members from a distribution list, D-6
oesmon utility, 7-9
  syntax options, 7-9
oesng utility, D-6
  examples, D-8
oespr utility, D-9
  examples, D-10
oesrl utility, D-24
  blocking messages, D-25
  capturing outbound messages, D-26
  copying messages to a folder, D-27
  copying outgoing messages, D-26
  creating server-side rules, 9-9
  deleting server-side rules, 9-9, D-25
  discarding all messages, D-26
  displaying server-side rules, 9-8
  editing server-side rules, 9-9
  rejecting messages
based on text strings, D-25
with too many recipients, D-27
server-side rule examples, D-27
oesucr utility, D-11
  examples, D-12
oesutil utility, D-45
oidadmin utility, 3-33
opmnctl utility, D-16
  creating server instances, D-18
  deleting server instances, D-19
  disabling server instances, D-20
  dynamically starting and stopping Housekeeper server tasks, D-23
  enabling servers, D-19
  listing server, D-18
  listing server instances, D-19
  refreshing server instances, D-22
  restarting server instances, D-21
  showing server instance status, D-23
  showing server process status, D-23
  starting a single server instance, D-21
  starting all server instances, D-21
  stopping a single server instance, D-22
  stopping all server instances, D-22
Oracle Collaboration Suite 10g Database
  See Oracle Collaboration Suite Database
Oracle Collaboration Suite 10g Mail
  See Oracle Mail
Oracle Collaboration Suite Applications tier
e-mail system component, 6-2
Oracle Collaboration Suite Database
  backup, 10-1, 10-2
  backup and recovery, 10-1
  defined, 3-1
  enabling supplemental logging
  LogMiner, 3-26
  modifying connection parameters, 3-2
  purging monitoring data from, 7-9
  setting up for LogMiner, 3-26
  target
  about, 7-6
  creating, 7-6
  troubleshooting, A-19
Oracle Enterprise Manager 10g Application Server Control
  server process
  refreshing, 3-5
  restarting, 3-5
Oracle Enterprise Manager 10g Application Server Control Console for Collaboration Suite
  parameters
  modifying default settings, 3-8
  modifying instance settings, 3-8
server instance
  creating, 3-6
  creating like, 3-6
  deleting, 3-7
  starting, 3-5
  stopping, 3-5
server process
disabling, 3-5
enabling, 3-5
Oracle Enterprise Manager 10g Grid Control Console, 7-1
about, 1-4
Oracle Flashback Query
MAIL_RECOVERY_FQ package, 10-7
recovery utility, 10-5
recovering messages, 10-8
Oracle Internet Directory
client target, 7-7
client target properties, 7-7
configuring SSL from Oracle WebMail, 4-9
Directory Cache, 5-1
Oracle Mail
backup and recovery, 10-1
about oesbkp utility, 10-2
LogMiner, 10-4
oesbkp backup files, 10-4
oesbkp logging information, 10-3
oesbkp parameters and definitions, 10-3
oesbkp syntax, 10-2
Oracle Flashback Query, 10-5
recovering messages, 10-8
error messages
Housekeeper server, B-6
IMAP server, B-1
List Server, B-7
NNTP server, B-8
overview, B-1
POP server, B-1
SMTP server, B-4
Virus Scrubber server, B-11
filters
about, 8-2
applying, 8-4
creating, 8-2
editing, 8-3
editing applied, 8-7
reordering, 8-3
filters to Collaboration Suite Database
applying, 8-5
message archiving, 8-26
creating an archiving policy, 8-27
editing an archiving policy, 8-28
enabling, 8-29
metrics
Housekeeper server, H-5
IMAP server, H-3
List Server, H-6
NNTP inbound server, H-6
NNTP outbound server, H-7
POP server, H-2
SMTP inbound server, H-3
SMTP outbound server, H-4
Virus Scrubber server, H-7
policies, 8-1 to 8-30
routing control, 8-8
incoming mail, 8-8
incoming news, 8-21
outgoing mail, 8-19
SAVSE filters
applying, 6-13
editing, 6-10
security
about, 6-1
server instances
creating, D-18
deleting, D-19
listing, D-19
refreshing, D-22
restarting, D-21
starting a single, D-21
starting all, D-21
stopping all, D-22
server log files, 3-3
server metrics
common to all servers, H-1
server parameters
Housekeeper debug, F-5
Housekeeper general, F-3
Housekeeping Operations, F-3
IMAP debug, F-11
IMAP general, F-8
IMAP rules and routing control, F-7
IMAP shared message flags, F-7
IMAP thread, F-6
LDAP connection pool, F-1
LDAP connection retry, F-1
List Server debug, F-33
List Server DSN, F-26
List Server general, F-30
List Server rules and routing control, F-27
List Server SMTP protocol timeouts, F-25
NNTP inbound access and routing control, F-13
NNTP inbound debug, F-15
NNTP inbound general, F-14
NNTP inbound thread, F-12
NNTP outbound debug, F-17
NNTP outbound general, F-16
NNTP outbound thread, F-16
POP debug, F-20
POP general, F-18
SMTP inbound debug, F-43
SMTP inbound DSN, F-35
SMTP inbound general, F-40
SMTP inbound rules and routing control, F-37
SMTP inbound thread, F-35
SMTP outbound debug, F-47
SMTP outbound general, F-45
SMTP outbound thread, F-45
Virus Scrubber debug, F-24
Virus Scrubber general, F-21
servers
disabling, D-20
enabling, D-19
Housekeeper, 3-23
IMAP, 3-9
List Server, 3-33
Index-7

listing, D-18
NNTP, 3-41
POP, 3-9
showing instance status, D-23
SMTP, 3-12
Virus Scrubber, 6-14
target
types, 7-1
tertiary storage, 3-31
troubleshooting
being alerted to problems, A-1
users
adding, 2-2
managing, 2-1
modifying attributes, 2-4
removing, 2-8
setting default attributes, 2-6
Oracle Mail Portlet API
overview, 4-9
Oracle Management Agent, 7-1
Oracle Text
creating a Housekeeper server instance to index text, 3-29
improving performance, 3-29
installing, 3-27
searching e-mail, 3-27
verifying installation, 3-29
Oracle WebMail
accessing, 1-2
aliases
creating, 2-22
deleting, 2-23
editing attributes, 2-23
configuring SSL to Oracle Internet Directory, 4-9
distribution lists
adding users, 2-21
attributes, 2-13
creating, 2-19
deleting, 2-21
group types, 2-15
modifying, 2-20
modifying default parameter values, 2-20
parameters, 2-16
posting types, 2-15
removing members, 2-21
showing all to which a user subscribes, 2-22
subscription types, 2-15
domains
creating, 2-11
modifying settings, 2-11
error messages, B-11
filters
about, 8-2
applying, 8-4
applying to Collaboration Suite Database, 8-5
creating, 8-2
editing, 8-3
editing applied, 8-7
reordering, 8-3
location of log files, 4-9
managing distribution lists, 2-12
message archiving, 8-26
creating an archiving policy, 8-27
default an archiving policy, 8-28
newsgroups
adding private, 2-27
adding public, 2-29
attributes, 2-27
defined, 2-26
deleting private, 2-28
deleting public, 2-30
editing private, 2-28
editing public, 2-29
private, 2-26
public, 2-26
overview, 4-1
peer servers
adding, 2-24
deleting, 2-26
editing, 2-25
managing, 2-24
properties, 4-3
oc4j.properties, 4-3
recovering deleted e-mail, 2-9
routing control, 8-8
incoming mail, 8-8
incoming news, 8-21
outgoing mail, 8-19
See Also
routing control
SAVSE filters
applying, 6-13
editing, 6-10
setting log levels, 4-9
tool kit
state file, 4-2
users
adding, 2-2
managing, 2-1
modifying attributes, 2-4
removing, 2-8
setting default attributes, 2-6
orclMailAdminCollectionInterval, 7-11
orclMailAdminStoreDN, 7-12

P

parameters
minqueueage, 3-17
modifying default server settings, 3-8
modifying server instance settings, 3-8
Oracle Collaboration Suite Database
connection, 3-2
orclMailAdminCollectionInterval, 7-11
orclMailAdminStoreDN, 7-12
queuetimeout, 3-17
See Also
server parameters
send_schedule delivery tag, 3-41
pass-through mode, 5-1
Pattern (LHS), 3-19
peer server attributes, 2-25
peer servers
   adding, 2-24
   attributes
      accepted newsgroups, 2-25
      feed newsgroups, 2-25
      host name, 2-25
      installation, 2-25
      port, 2-25
      rejected newsgroups, 2-25
   deleting, 2-26
   editing, 2-25
   managing, 2-24
PL/SQL mail merge, 3-39
policies, 8-1 to 8-30
   archiving, 8-26
POP
   defined, 3-9
POP server
   debug parameters, F-20
   error messages, B-1
   general parameters, F-18
   metrics, H-2
   process architecture, 3-10
POP3
   See POP
post office protocol
   See POP
process control message cleanup
   enabling, 3-25
provisioning users
   command line, D-11
   Oracle WebMail, 2-2
pruning
   enabling, 3-25

Q
   quota
      checking percentage used
         using oesutil utility, D-45
      e-mail, 2-3
         voice mail, 2-3

R
   recovering deleted e-mail, 2-9
   recovering messages, 10-8
   recovery
      about oesbkp utility, 10-2
      Oracle Collaboration Suite Database, 10-1
      Oracle Mail, 10-1
   rejecting messages
      based on text strings, D-25
      with too many recipients, D-27
   request for comments
      See RFCs
Result (RHS), 3-19
RFCs
   supported, E-1
   routing control, 8-8
for NNTP server, 6-9
for SMTP server, 6-6
incoming mail, 8-8
   advanced settings, 8-16
   copying settings, 8-18
   general settings, 8-9
   reject settings, 8-10
   saving settings, 8-18
   trust settings, 8-13
incoming news, 8-21
   copying settings, 8-26
   general settings, 8-21
   reject settings, 8-22
   saving settings, 8-26
   trust settings, 8-24
outgoing mail, 8-19
   copying settings, 8-21
   saving settings, 8-20
   process defined, 6-6
rules
   See filters
      See server-side rules
S
   SASL, 6-3
   SAVSE
      filters
         applying, 6-13
         editing, 6-10
   SAVSE filters
      ICAP configuration, 6-11
      string parameters, 6-12
   scheduled mail delivery, 3-41
scripts
   esd_check_quota_usage.pl, D-48
   esd_copy_messages.sql, D-53
   esd_find_message.sql, D-49
   esd_list_folder_messages.sql, D-54
   esd_list_unopened_inbox.sql, D-54
   esd_list_user_folders.sql, D-54
   esd_logsan.pl, D-46
   esd_mail_queue.sql, D-53
   esd_queue_examine.sql, D-49
   esd_show_message.sql, D-50
   esd_show_session_usage.sql, D-56
   esd_show_sessions.sql, D-55
   utllockt.sql, D-57
searches
   of e-mail, 3-27
   of e-mail bodies in various languages, 3-28
Secure Sockets Layer
   See SSL
security
firewalls, 6-4
   Oracle Mail, 6-1
SMTP server, 6-2
send_schedule delivery tag parameters, 3-41
server instance
   creating
using Oracle Enterprise Manager, 3-6
using the command line, D-18
creating like
using Oracle Enterprise Manager, 3-6
deleting
using Oracle Enterprise Manager, 3-7
using the command line, D-19
disabling
using Oracle Enterprise Manager, 3-5
using the command line, D-20
enabling
using Oracle Enterprise Manager, 3-5
using the command line, D-19
listing
using the command line, D-19
refreshing
using Oracle Enterprise Manager, 3-5
using the command line, D-22
restarting
using Oracle Enterprise Manager, 3-5
using the command line, D-21
show status of
using the command line, D-23
starting
using Oracle Enterprise Manager, 3-5
starting a single
using the command line, D-21
starting all
using the command line, D-21
stopping
using Oracle Enterprise Manager, 3-5
stopping a single
using the command line, D-22
stopping all
using the command line, D-22
server parameters
Housekeeper debug, F-5
Housekeeper general, F-3
Housekeeping Operations, F-3
IMAP debug, F-11
IMAP general, F-8
IMAP rules and routing control, F-7
IMAP shared message flags, F-7
IMAP thread, F-6
LDAP connection pool, F-1
LDAP connection retry, F-1
List Server debug, F-33
List Server DSN, F-26
List Server general, F-30
List Server rules and routing control, F-27
List Server SMTP protocol timeouts, F-25
modifying default settings, 3-8
modifying instance settings, 3-8
NNTP inbound access and routing control, F-13
NNTP inbound debug, F-15
NNTP inbound general, F-14
NNTP inbound thread, F-12
NNTP outbound debug, F-17
NNTP outbound general, F-16
NNTP outbound thread, F-16
POP debug, F-20
POP general, F-18
SMTP inbound debug, F-43
SMTP inbound DSN, F-35
SMTP inbound general, F-40
SMTP inbound rules and routing control, F-37
SMTP inbound thread, F-35
SMTP outbound debug, F-47
SMTP outbound general, F-45
SMTP outbound thread, F-45
Virus Scrubber debug, F-24
Virus Scrubber general, 6-15, F-21
servers
Housekeeper, 3-23
IMAP, 3-9
List Server, 3-33
NNTP, 3-41
Oracle Mail
defined, 7-2
POP, 3-9
SMTP, 3-12
server-side rules
about, 9-1
blocking messages, D-25
capturing outbound messages, D-26
display, 9-3
domain-wide, 9-3
system-wide, 9-3
user, 9-3
copying messages to a folder, D-27
copying outgoing messages, D-26
creating, 9-8
with oesrl utility, 9-9
deleting, D-25
with oesrl utility, 9-9
discarding all messages, D-26
displaying
with oesrl utility, 9-8
display, 9-9
events, 9-2
examples
using oesrl utility, D-24
parts of
actions, 9-5
attributes, 9-5
conditions, 9-3
expressions, 9-4
rejecting messages
based on text strings, D-25
with too many recipients, D-27
tips, D-29
service
Oracle Mail
defined, 7-2
service target
creating, 7-4
service targets
about, 7-3
service types, 7-10
Simple Authentication and Security Layer
See SASL
simple mail transfer protocol
See SMTP

SMTP
address rewriting rules, 3-17
configuring, 3-13
defined, 3-12
message flow, 3-13
multiple Collaboration Suite Database setup, 3-13
single Collaboration Suite Database setup, 3-13
single node setup, 3-13
thread pool
database connection, 3-15
Oracle Internet Directory server, 3-15
worker, 3-15
troubleshooting, A-14

SMTP inbound server
architecture, 3-15
defined, 3-15
DSN parameters, F-35
general parameters, F-40
metrics, H-3
rules and routing control parameters, F-37
thread parameters, F-35

SMTP outbound server
architecture, 3-16
creating for message archiving, 8-29
definition, 3-16
general parameters, F-45
metrics, H-4
thread parameters, F-45
thread pool
database connection, 3-16
Oracle Internet Directory server, 3-16

SMTP server
antispm checks, 6-6
error messages, B-4
routing control, 6-6
security, 6-2
spam, 6-5
spam control
See routing control

SSL
about, 6-5
configuring between Oracle WebMail and Oracle Internet Directory, 4-9
standard mail merge, 3-39
statistics
See metrics

Symantec AntiVirus Scan Engine
See SAVSE

syncrhonizing distribution lists rom a private e-mail namespace, G-4

T

tablespace
esperftbl, 7-12
ESTERSTORE, 3-31
target
e-mail group, 7-8
Oracle Collaboration Suite Database
creating, 7-6
Oracle Internet Directory client
creating, 7-7
service
about, 7-3
creating, 7-4
type, 7-10
types, 7-1
Web application
creating, 7-5
tertiary storage, 3-31
configuring Housekeeper for, 3-32
Housekeeper server tasks, 3-24

text indexing
See index synchronization, 2-5
TLS, 6-5

Transport Layer Security
See TLS

troubleshooting, A-1 to A-24
being alerted to problems, A-1
Housekeeper server, A-18
mail queues, A-15
Oracle Collaboration Suite Database, A-19
problems with a single message, A-12
problems with mail clients, A-3
problems with mail delivery, A-7
problems with mail protocols, A-14

U

user
administrative privileges, 1-1
user attributes, 2-2
e-mail user account name, 2-2
users
adding
Oracle WebMail, 2-2
modifying attributes
Oracle WebMail, 2-4
provisioning
command line, D-11
removing
Oracle WebMail, 2-8
setting default attributes
Oracle WebMail, 2-6
utllockt.sql script, D-57

V

Virus Scrubber server
about, 6-14
configuring, 6-15
error messages, B-11
log files, 6-15
metrics, H-7
parameters
dev, F-24
general, F-21
PL/SQL script, 6-19
examples, 6-19
quarantine, 6-19, 6-20
restore, 6-20
voice mail
quota, 2-3