SCO*office* Mail Server

Administrator's Guide

The SCO Group

Administrator's Guide

by The SCO Group

Table of Contents

Preface

This book introduces the SCO SCOoffice™ Mail Server (hereafter "SCO*office* Mail Server"), a highly reliable, scalable messaging server that runs on Linux® platforms. This book is intended primarily for SCO*office* Mail Server administrators, as well others who install and maintain SCO*office* Mail Server software.

Portions of this book are also intended to be read from SCO*office* Mail Server **Server Manager** Help screens. That is, when you click on **Help** in the **Server Manager**, you will see one of the chapters or sections of this book, which are intended to provide background information necessary to manage your SCO*office* Mail Server preferences. You can follow the links within each section to see the Table of Contents and other topics.

This *Administrator's Guide* is available online after the product is installed, and in HTML and PDF formats on the SCO*office* Mail Server distribution media.

We recommend that you consult the Preface of the *Getting Started Guide* for important information about:

• SCO*office* Mail Server documentation

• viewing SCO*office* Mail Server online documentation

• SCO Technical Support, including:

  • product registration

  • Late News about product features and enhancements

  • SCO Self-Help Services

How Can We Improve This Book?

What did you find particularly helpful in this book? Are there mistakes in this book? Could it be organized more usefully? Did we leave out information you need or include unnecessary material? If so, please tell us.

To help us implement your suggestions, include relevant details, such as book title, section name, page number, and system component. We would appreciate information on how to contact you in case we need additional explanation.

> **Note:** Technical Publications cannot provide technical support. For answers to technical questions, please contact your software vendor or your support representative, or refer to the "Technical Support" section in the *Getting Started Guide.*

To contact us with documentation-related questions or comments, email us at `<techpubs@caldera.com>`.

Thank you.

Chapter 1. About the SCO*office* Mail Server

SCO*office* Mail Server is a messaging server product built around directory services and industry-standard open source components. The design goals of the SCO*office* Mail Server required:

- ease of use.
- ease of management.
- stability.
- security.
- ability to integrate with popular email clients.
- superior performance in all these areas than competing solutions for small and medium businesses.
- platform neutrality.

The principle components of the SCO*office* Mail Server are:

OpenLDAP (directory services)

> The SCO*office* Mail Server uses a Lightweight Directory Access Protocol (LDAP) directory to store information concerning mail accounts, mail aliases, and the mail domains configured on your server. OpenLDAP is the directory server for the SCO*office* Mail Server. Both personal and corporate user information and mail authentication are all stored in the directory and now easily managed using the **Server Manager**.

Postfix (MTA)

> The heart of any messaging server is the Mail Transfer Agent (MTA), which is responsible for queuing and routing of email messages, handling mailing lists and aliases, and forwarding email. Postfix is the Mail Transport Agent for the SCO*office* Mail Server. Unlike other MTA systems before it, Postfix (originally known as IBM Secure Mailer) was designed explicitly with security in mind. Postfix has been configured to query the LDAP directory for information needed to deliver mail to the correct Cyrus inbox and to resolve mail aliases.

Cyrus (message store)

> The message store is used to store mail folders. The Cyrus message store provides access to personal mail through the Internet Message Access Protocol (IMAP4) and Post Office Protocol (POP) via its IMAP and POP server. IMAP and POP servers are key components that allow email clients to connect to the server and fetch mail. The Cyrus server differs from other message store and IMAP server implementations in that it is run on "sealed" servers, where users are not normally

permitted to log in. The Cyrus server queries the LDAP directory for authentication of users using the **pam_ldap** interface.

The Cyrus message store is stored in parts of the filesystem that are private to the Cyrus system and all user access to mail is only through clients using the IMAP and POP3 protocols. This means that SCO*office* Mail Server mailboxes are not compatible with traditional UNIX or Linux flat file mailbox format and you will not be able to access them using **mailx** or any other client that does not support IMAP or POP. However, the Cyrus database mailbox format provides a message store which is much more scalable than the traditional flat file format. Also, users are able to access their mail from command line utilities, but they will have to use the **fetchmail** utility to do so.

The SCO*office* Mail Server also provides:

PAM LDAP module

    The LDAP Pluggable Authentication Module provides the ability for IMAP and POP services to authenticate against passwords stored in the LDAP directory.

OpenSSL

    OpenSSL is a Secure Sockets Layer communications library that provides cryptographic security for the Cyrus IMAP and POP servers and the **Server Manager** interface.

Apache – webserver

    The SCO*office* Mail Server configures the standard Apache webserver (installed by default on Linux platforms) to serve the **Server Manager** mail administration and mail client preferences interfaces.

MUA support

    An email client is called a Mail User Agent (MUA). MUA functionality is often included with Internet browsers together with calendar clients capability. The SCO*office* Mail Server supports standard mail clients, and it provides a user management interface to enable server-based functionality on Outlook clients.

local delivery agent

    MTA's do not communicate directly with the message store, rather they call a local delivery agent, which is a simple program that knows how to place a mail message in a given user's inbox. The local delivery agent for the SCO*office* Mail Server is the Cyrus **deliver** program.

Chapter 2. Configuration and Administration

Administrative Interfaces

The SCO*office* Mail Server includes these administrative interfaces:

- **Server Manager**
- **Preferences Manager**
- Command line utilities and scripts

We also recommend that you familiarize yourself with platform-specific graphical administrative tools.

Server Manager

The principle graphical interface for SCO*office* Mail Server administration. It provides mail server administrative screens accessible only by administrators with the login name "*admin*".

By default, the **Server Manager** is served by the Apache webserver at:

*https://**hostname**/msg*

where ***hostname*** is the value returned by the **hostname**(1) on the SCO*office* Mail Server system.

> **Note:** SSL (Secure Socket Layer) connections are enabled by default in the SCO*office* Mail Server, allowing you to log in to the **Server Manager** immediately using an *https* URL. We strongly recommend that you use secure SSL connections provided by the *https* URL whenever possible.

Preferences Manager

The SCO*office* Mail Server mail client user interface. It provides client mail preference screens accessible to all users with an active SCO*office* Mail Server mail account and an Internet browser. Like

the **Server Manager** screens, it is served by the Apache webserver at:

*https://**hostname**/msg*

although logging in with a user mail account displays a different set of screens. For more information about client preference screens, see "Managing Client Preferences".

Command line utilities and scripts

Although most administrative functions can be managed with the **Server Manager**, the following command lines utilities are also available:

imapcp(8)

>   migrate existing IMAP mailboxes to SCO*office* Mail Server

msgaclget(8)

>   get current state of LDAP access controls

msgaclset(8)

>   modify the state of LDAP access controls

msgaliasadd(8)

>   add a member to a SCO*office* Mail Server alias

msgaliascreate(8)

>   create a new SCO*office* Mail Server alias

msgaliasdelete(8)

>   delete a SCO*office* Mail Server alias

msgaliaslist(8)

>   list attributes of a SCO*office* Mail Server alias

msgaliaslistall(8)

>   list attributes of all SCO*office* Mail Server aliases

msgaliasmigrate(8)

    migrate mail alias file members to SCO*office* Mail Server LDAP datastore

msgaliasremove(8)

    delete a member from a SCO*office* Mail Server alias

msgaliasreplace(8)

    modify the restricted setting or the description of a SCO*office* Mail Server alias

msgcalendarlistnodes(8)

    query SCO*office* Mail Server calendar node information

msgdomaincount(8)

    list the names and descriptions of all SCO*office* Mail Server mail domains

msgdomaincreate(8)

    create a new SCO*office* Mail Server mail domain

msgdomaindelete(8)

    delete a SCO*office* Mail Server mail domain

msgdomainlist(8)

    list the description of a SCO*office* Mail Server mail domain

msgdomainlistall(8)

    list the descriptions of all SCO*office* Mail Server mail domains

msgdomainmodify(8)

    modify the description of a SCO*office* Mail Server mail domain

msgdomainmove(8)

    rename a SCO*office* Mail Server mail domain

msgimpsetup(8)

    configure IMP mail client to work with the SCO*office* Mail Server Cyrus server

msgldaphost(8)

    configure the SCO*office* Mail Server LDAP host

msgservicelist(8)

    list the status of a SCO*office* Mail Server system service

msgservicelistall(8)

    list the status of all SCO*office* Mail Server system services

msgsievebuild(8)

    rebuild SCO*office* Mail Server user mail filters

msguninstall(8)

    remove the SCO*office* Mail Server from a host system

msgusercreate(8)

    create a new SCO*office* Mail Server user

msguserdelete(8)

    delete a SCO*office* Mail Server user

msgusergetaliases(8)

    list SCO*office* Mail Server alias membership for a specified user

msguserisadmin(8)

    determine admin privileges of a specified SCO*office* Mail Server user

msguserlist(8)

    list SCO*office* Mail Server user attributes

msguserlistall(8)

    list all SCO*office* Mail Server users' attributes

msgusermigrate(8)

    migrate */etc/passwd* members to SCO*office* Mail Server LDAP datastore

msgusermod(8)

    modify SCO*office* Mail Server user attributes

msguserpw(8)

    change a SCO*office* Mail Server user's password

These utilities are called from the */opt/lsb-sco.com/msg/bin* directory. If you use them frequently, you might want to add `/opt/lsb-sco.com/msg/bin` to your `PATH` environment variable. For more information, see their respective manual pages.

Warning

Many of these utilities form the back end for the administrative interface. This listing does not include those utilities in */opt/lsb-sco.com/msg/bin* that should only be run by the administrative interface. Do not run the following utilities from the command line:

- **msgencrypt**
- **msgexec**
- **msggenclientconfig**
- **msginboxcreate**
- **msgroot**
- **msgvscan**

See also Running SCO*office* Mail Server Utilities From Scripts.

Graphical utilities

Webmin

Webmin™ is the browser-based system administration interface for SCO Linux and Caldera OpenLinux. It is the prefered utility for managing system functions used by the SCO*office* Mail Server, such as:

- network configuration, including DNS/BIND
- SSL certificate and key management
- MySQL management for Webmail components

For more information, see "Introduction to Webmin" in the *Caldera OpenLinux System Administration Guide*.

The admin Administrative Account

The SCO*office* Mail Server has a single administrative account named *admin*. This is the name you use to log into the **Server Manager** for administering your messaging server. It is a valid mail account and can receive mail.

Note: Do not configure a local system account named *admin*; doing so will prevent the SCO*office* Mail Server administrator from receiving mail.

The *admin* account is managed like other user accounts as described in "Managing Mail Users". You can also change the *admin* password by clicking on **Admin Password** under the **System** menu in the **Server Manager**.

Before proceeding with SCO*office* Mail Server configuration, we recommend that you change the initial *admin* password, set by default to "admin." Neither the *admin* password nor any user password can be a null string. You must enter a string of at least one character; we recommend that you follow conventional password precautions as described in Chapter 8 "Changing Your SCOoffice Mail Server Password" in the *Client User's Guide*.

Caution

You must select and maintain passwords carefully to ensure the security of your SCO*office* Mail Server. Insufficient password protection is a security risk.

Aliasing root Mail to SCO*office* Mail Server admin Mailbox

The *root* mail account is used by several OpenLinux programs to log various activities. This mail is

normally sent to the *root* mailbox in */var/spool/mail/root*. However, because *root*'s mail is not kept in a SCO*office* Mail Server mailbox, this mail is not accessible using either POP or IMAP protocols.

If you wish to have *root*'s mail accessible using IMAP or POP, we recommend that you create an alias called *root* in the primary mail domain and add *admin* as its only member. This will cause all mail addressed to *root* to go to the SCO*office* Mail Server mailbox for the *admin* user. Since the *admin* account is privileged, we recommend accessing that account from SSL sessions only.

Importing User Data

The SCO*office* Mail Server enables you to migrate user data from existing UNIX system mail configurations by converting existing data files into LDAP datastores. You can import:

- mailboxes
- users
- aliases

> **Note:** In this SCO*office* Mail Server release, user data can only be imported from UNIX and Linux systems. Future SCO*office* Mail Server releases will include the capability of importing data from Microsoft® Windows and Exchange systems.

Importing Mailboxes

Existing mailboxes can be imported to the SCO*office* Mail Server using any IMAP-capable mail client.

For existing IMAP mailboxes:

- Administrators can migrate existing IMAP mailboxes from the command line using the imapcp(8) utility.
- Mail client users can drag their IMAP mailbox from the previous server to the IMAP mailbox on the SCO*office* Mail Server.

For existing POP mailboxes:

Once mail client users have downloaded their POP mail, they can upload it from their client to their SCO*office* Mail Server IMAP mailbox.

Importing Users

Use the **msgusermigrate** migration utility to convert UNIX system */etc/passwd* entries to an LDAP datastore. To do so, copy the existing */etc/passwd* and */etc/shadow* files to a *tmp* directory on the SCO*office* Mail Server system and run **msgusermigrate**. For more information, see the msgusermigrate(8) manual page.

Warning

Make sure that none of the UIDs in the imported */etc/passwd* file exist as system users on the SCO*office* Mail Server system. Do not use the **msgusermigrate** utility in an attempt to create SCO*office* Mail Server mailboxes for existing system users; doing so will result in failed mail delivery to the SCO*office* Mail Server accounts. If you must have system users on your SCO*office* Mail Server system, make sure that their SCO*office* Mail Server UserID is different from their system uids.

Also, be sure that the imported */etc/passwd* does not contain an *admin* account. If you attempt to import a duplicate *admin* account, you might disable the SCO*office* Mail Server.

We recommend that you carefully review the contents of the imported */etc/passwd* file before running the **msgusermigrate** utility.

Importing Aliases

Use the **msgaliasmigrate** migration utility to convert UNIX system mail alias file entries to an LDAP datastore. To do so, run it on an imported *aliases* file or the local */etc/mail/aliases* file. For more information, see the msgaliasmigrate(8) manual page.

System Settings

Licensing and Registering SCO products

You must License and Register the SCOoffice Mail Server. You license the SCOoffice Mail Server when you install it. Other SCO products will prompt you for license information during their installation process. Registration is done through the SCO registration application available on the web at http://www.sco.com/registration Registration activates your one year subscription to SCO Update, a repository for SCOoffice software fixes and updates, for a period of one year.

Warning

If you defer licensing during installation, your software product is in 60 day evaluation mode and will expire unless a license is provided within that timeframe. The number of user licenses provided in 60 day evaluation mode is not limited. After the expiration period, you must supply both user and server licenses or the SCOoffice Mail Server management tools will cease to function.

Use the Licenses screen to license the SCOoffice Mail Server software and manage user licenses. The following three items on the Certificate of License and Authenticity are your "license" and are always used in conjunction with one and another:

Serial Number

A unique number identifying each SCO product.

Activation Key

A license code which activates the product.

License Data

Additional license information needed to activate some products. This field is not always present on the Certificate of License and Authenticity, and is not required for licensing in those cases.

Should the 60 Day evaluation period expire, before a license is applied, the web-based management interface will cease to function. It is still possible to enable licensing from the command line using:

```
brand -g serial_number activation_key [optional_license_data]
```

Changing the admin Password

You can use the **Server Manager** to change the password for the *admin* administrator account:

1. In the **System** menu, click on **Admin Password**.

2. Enter and confirm the new password value in the **Change Password** screen

3. Click on **Apply** to complete the change.

You can also change the *admin* password in the **View Users** but it is more direct to use this method in the **System** menu.

Managing Global User Access Privileges

You can use the **Server Manager** to set global access privileges for users in all mail domains controlled by the SCO*office* Mail Server.

In the **System** menu, click on **User Access**. You can grant or deny these privileges globally:

Users can change their own password

Controls whether users can change the value of their mail account password via the SCO*office* Mail Server admin user configuration interface.

Users can change their own profile

Controls whether users can change their profile parameters as described in "Managing Mail Users".

Users can create mail aliases

Controls whether users can create mail aliases within the SCO*office* Mail Server directory using the **Server Manager** user configuration interface.

Note: When you change these settings, **Preferences Manager** screens for users currently logged in are not changed dynamically. We recommend that you alert SCO*office* Mail Server users when global or individual changes are made to their privileges.

Managing Mail Services

The **Server Manager** allows you to view the status and perform certain actions on the SCO*office* Mail Server component servers. In the **System** menu, click on **Mail Services** to view the list of configured services. Click on the service name to display its status, the PID of the active process, and the command that launched it. You can also take the following **Service Actions**:

- **cyrus** IMAP/POP Server

  Start/Stop

    Start or stop the server

- **docview** - OpenLinux Documentation Server

  Start/Stop

    Start or stop the server

  Restart

    Stop and restart the server

  Reload

    Reload DocView configuration files

- **ldap** - OpenLDAP Directory Server

  Restart

    Stop and restart the server

  Note: Stopping the LDAP server disables the **Server Manager**; this can only be done manually.

- **postfix** - Mail Transport Agent (MTA)

    Start/Stop

    Start or stop the MTA

    Restart

    Stop and restart the MTA

    Reload

    Reload MTA configuration files

Mail services can also be controlled from the command line using standard **init** scripts:

`/etc/rc.d/init.d/`*`service`* `[ start|stop|restart|reload ]`

Managing Junk Mail

The **Server Manager** allows you to control access to the Realtime Blackhole List (RBL) mail filtering service. Click on:

Reject messages

to enable RBL service

Don't use RBL

to disable RBL service

Then click on **Apply** to complete the change.

> **Note:** RBL is a subsciption service that must be contracted before mail is filtered. For more information, see "Junk Mail Filtering".

You can also make the simple BCC filter available by granting individual **User Access** privileges for junk mail filtering or by setting a default for user creation; see "Junk Mail Filtering" for more information.

at Command Output to root Mailbox

Several **Server Manager** backend utilities schedule jobs with the **at**(1) command, which sends output to the *root* user's system mailbox. The following actions will generate spurious warning mail to *root*:

• creating or deleting a domain

• changing any of the **User Access** values in the **Server Manager System** menu

The warning message varies on the supported platforms, but in all cases it will be output captured by the **at** command. These messages can be safely ignored.

The *root* user's mailbox is */var/spool/mail/root*; you should examine and clear this file regularly. You might also want to alias *root*'s mail to the SCO*office* Mail Server mailbox for the *admin* user, as described in "Aliasing root Mail to SCOoffice Mail Server admin Mailbox".

Running SCO*office* Mail Server Utilities From Scripts

All SCO*office* Mail Server utilities require some form of authentication, but it is not practical to enter the administrator's password every time a SCO*office* Mail Server utilities is invoked, especially if many executions are desired.

The preferred method is to pipe the *admin* user's fully qualified LDAP name (distinguished name) and password to the utility. This is because it is a security risk to store a password in a file or to pass it as a command line argument, which would be visible to a **ps**(1) listing. The administrator's LDAP distinguished name is contained in the */etc/opt/lsb-sco.com/msg/msg.conf* file in the `ADMINDN` variable. A script can prompt for the *admin* password once and pipe it to as many SCO*office* Mail Server utilities as needed after that.

Here is an example using a SCO*office* Mail Server utility in an OpenLinux **bash**(1) shell script:

```
# Get the password in a safe way.
# If you need to run the script non-interactively, you can enter
# the password directly in the script and bypass this section.
echo -n "Enter administrators password : "
stty -echo
read password
stty echo

# Need to echo a newline after getting the password.
echo

# Get the admin distinguished name from msg.conf.
admindn=`grep ADMINDN /etc/opt/lsb-sco.com/msg/msg.conf | sed s/ADMINDN://`

# Issue a command; use ADMINDN from msg.conf,
# although you can specify any user's DN there if desired.
cat « DONE | /opt/lsb-sco.com/msg/bin/msgusercreate -uid=user0 -
domain=`hostname -f`
$admindn
$password
DONE
```

Enabling Webmail Service

The SCO*office* Mail Server provides Webmail service with the IMP (Internet Messaging Program) webmail client and Horde framework, which are enabled by default. At installation, the SCO*office* Mail Server:

- configures the **mysql** database engine to work with the horde database, which is used to store user information.

- sets the horde database password to the value of the *PW* attribute, which is stored in the *msg.conf* (5) file. The system administrator can change this password using the utility:

  /usr/libexec/horde/database/dbpasswd.sh

    Note: Later versions of the horde package might store this utility in
      /usr/lib/horde/database/dbpasswd.sh

You will need this password if you want to make changes to your Horde or IMP configuration files.

• starts the **mysql** daemon and sets it to run by default.

SCO*office* Mail Server users can access the IMP webmail client immediately by pointing their browsers at *https://**hostname**/horde/imp*, as described in "Enabling IMP Webmail Client Users".

To disable Webmail service:

1. Disable default **mysql** daemon startup by editing the */etc/sysconfig/daemons/mysql* file and changing the *ONBOOT* parameter to `"no"`.

2. Stop the **mysql** daemon using either:

   Webmin (SCO Linux and Caldera OpenLinux only)

   In the **Servers** screen, click on **MySQL Database Server**, then click on **Stop MySQL Server**.

   command line

   Enter **`/etc/rc.d/init.d/mysql stop`**.

For more information, see the Horde and IMP documentation, available from the SCO*office* Mail Server webpage in DocView.

Using Volution System Management Services

The Caldera Volution platform includes two system management and administration products that are compatible with the SCO*office* Mail Server:

Volution Manager (VM)

   This Web-based management system enables administrators to manage the network with profiles and policies, without having to individually manage each system. Based on LDAP directory

services, it can be configured to provide hardware and software inventory, software distribution, health monitoring of systems, printer configuration and scripted scheduled actions. It consists of:

Volution Manager Server

> A server system running VM Server software. This includes the computer creation daemon (**volutionccd**) which adds VM Client computers to the directory structure, the DENS daemon (**densd**) which acts as an event scheduler, and the software repository daemon (**volutionsrd**) which adds distributable package objects to the software repository.

Volution Manager Client

> A Linux or UNIX system that can be managed by the VM Server. Each installed client runs the VM Client daemon (**volutiond**) which includes support for OpenSLP, the protocol the client uses to locate the VM Server.

Volution Manager Console

> A browser-based interface used to perform management tasks. Once the VM Server and VM Clients are installed and configured, the VM Management Console is where Volution system management takes place.

Volution Online

> A proactive, subscription package management system. It tracks thousands of RPM packages, tracks alerts against these packages, and facilitates updates to your systems.

Working With Volution Manager

Volution Manager and the SCO*office* Mail Server can reside:

on the same machine

> Both the Manager Server and SCO*office* Mail Server Volution services can coexist on the same Caldera OpenLinux server, sharing the same OpenLDAP directory server. No special installation or configuration is required, simply run the installations for both products on the same system.

> The Manager Client and SCO*office* Mail Server can also coexist together on the same machine, facilitating simple remote management of the SCO*office* Mail Server platform.

on different machines

> The Manager Server and SCO*office* Mail Server can also share the same OpenLDAP server but reside on different systems. In this configuration, the SCO*office* Mail Server has to be configured to recognize a remote LDAP server as described in "Configuring a Remote OpenLDAP Server".

The Volution Manager and Messaging Server can work together to provide:

software distribution and maintenance

> Volution Manager can be used to supply updates, patches, fixes, or advanced configuration changes to a SCO*office* Mail Server system when the VM Client is installed on the same system.

system monitoring

> Volution Manager can detect system problems on a SCO*office* Mail Server system with the VM Client installed. Volution Manager can be configured to notify staff or take corrective action for a range of problems, such as poor network performance and approaching disk space limits. Many standard alerts are pre-configured with the Volution Manager product.

email alerts

> Volution Manager can also be configured to notify administrators of problems using email messages. In this case, the SCO*office* Mail Server can be used as the email server that delivers these notifications to designated recipients. The SCO*office* Mail Server can also redirect messages to Linux applications (such as a helpdesk application).

For more information, see the Volution Manager *Administration Guide*.

Chapter 3. Mail Administration

Managing Mail Domains

About Mail Domains

A *mail domain* is a name used for mail delivery that describes the site where a computer is located and generally includes the machine (host) name, a department (optionally), and the site's organization or country. In its default configuration, a system has exactly one IP address associated with each network interface and it has exactly one system and domain name.

The default configuration for the SCO*office* Mail Server assumes there is only one mail domain, with the same name as the system domain name, and one set of mail users who are addressed to that system name. This is sufficient for most simple mail systems.

The SCO*office* Mail Server also enables *virtual domains*. You can create virtual domains if you want multiple mail domains presented from a single mail server. SCO*office* Mail Server mail domains can be either attached to actual physical network interfaces or they can be virtual. There is no difference in how you configure them using the **Server Manager**. The only requirement is that all mail users and mail aliases under that domain must have addresses which are qualified by the domain's name. For example, if you create a virtual domain "***abc.com***" and create a mail account under that mail domain, the corresponding user must have an address of the form "***username@abc.com***".

> **Note:** Creating a mail domain in the SCO*office* Mail Server does not configure a new network address nor does it configure DNS for the domain names. It only configures the mail system to accept mail addressed to that mail domain. Network interfaces and name resolution can be managed efficiently with the **Webmin** interface; see the *Caldera OpenLinux System Administration Guide* for more information.
>
> A *postmaster* alias is created automatically in new domains with the "*admin*" administrator account as its sole member. This alias should not be deleted from the domain.

Configuring Mail Domains

In the **Server Manager**, click on these buttons in the **Domains** menu to:

View Domains

Lists the mail domains controlled by the SCO*office* Mail Server.

Create Domain

Enter a mail domain name and description.

Delete Domain

Deletes the domain names you select.

The SCO*office* Mail Server supports multiple mail domains, with user and alias lists displayed in per-domain views. To switch to a different domain, select it from the **Domain** box in the upper right of the screen.

To change domain names, including the primary domain, use the **msgdomainmove**(8) utility. For more information, see the msgdomainmove(8) manual page.

Configuring Virtual Domains

Before configuring the SCO*office* Mail Server for virtual domains, you must create mail exchanger (MX) records in DNS to resolve virtual domain names to the SCO*office* Mail Server host machine. To update DNS, use the **Webmin** DNS/Bind Server Module as described in "Creating a Mail Exchanger Record" in the *Caldera OpenLinux System Administration Guide*.

You can then create mail domains with the **Server Manager** using the new virtual domain names.

The msgdomainmove(8) utility can also be used to change virtual domain names.

Managing Mail Users

You can create and modify mail accounts for users who receive mail on the SCO*office* Mail Server. The email account includes:

- general information for the user, such as the user's name, password, and telephone number.

- email addressing information, including the primary email address for the user and the option of forwarding their email to another user.

- a Cyrus inbox for the user.

- automatic reply information for extended absences.

- default filtering for unsolicited email (spam); this can be configured with the msgusermod(8) utility.

> **Note:** If you have large numbers of users or aliases on your SCO*office* Mail Server, it may take some time to load the **View** displays, and these displays may occupy many screens.
>
> Postfix requires (as do most MTAs under requirement by RFC822) that an account for "*postmaster*" exists so that messages to the address "postmaster@*host.domain*" can be delivered successfully. Typically, the postmaster receives any error messages generated by Postfix. The postmaster mail alias is created automatically during installation with the "*admin*" administrator account as its sole member. A *postmaster* alias is also created automatically in new domains when they are added. This alias should not be deleted from the server.

See also "Managing Global User Access Privileges".

Use the **Server Manager** to enter and modify mail account information. In the **Users** menu, click on:

- **View Users**
- **Find User**
- **Create User**
- **Delete User**

View Users

List all users in the selected mail domain, sorted by `User ID`. Clicking on the `User ID` link displays the user's complete account information. From this display you can take these **User Actions**:

- **Modify** the listed settings
- change the admin or user's **Password**. You can also change the *admin* password by clicking on **Admin Password** under the **System** menu in the **Server Manager**.
- view and modify the user's mail **Quota**
- view **Aliases** to which the user is subscribed
- **Delete** this user

Clicking on **Quota** lists mail quota usage for all users, sorted by `email address`. Click on `email address` to set or modify the quota.

Setting Mail Quotas

To set or modify the user's mail quota limit, click on **View Users** and

- select a `User ID` and click on **Quota**, or
- select the **Quota** view and click on an `email address`.

Quota limits apply to the user's entire mailstore, including inbox and folders. Enter a value in megabytes of disk space; enter `NONE` to remove the quota.

Once over the quota, no new messages will be delivered to a user's inbox and mail will bounce. Users will recieve a warning from their mail client when the **% Used** value is over 90% of their quota limit. If the user's quota is near the limit when a large message is delivered, it is possible for the **MB used** value to exceed the quota. See the msguserlist(8) for more information

> **Note:** 0 is a legal value for mail quotas, but it will disable mail delivery for that user.
>
> The **Server Manager** quota controls affect individual users; there are no global quota controls. To assign default quotas for new users as they are created, set the **–DefaultQuotaLimit** ACL (Access Control List) attribute as described in the msgaclset(8) manual page.

It is possible to manipulate mail quotas directly as described in "Quotas" in *Cyrus IMAP Server: Overview and Concepts* and the **cyradm**(1) manual page. However, we recommend using the **Server Manager** to manage mail quotas because it is easier and less error prone than manually editing files.

Find User

Search for a user in the selected mail domain. You can enter a full or partial word to be found in the `User ID` or any of the `Name` fields. Click on the `User ID` links in the search results to display user information and take **User Actions**.

Create User

Create a new user. Required entries are marked with asterisks "*"; on some browsers, optional entries are displayed when you click on **More**.

*User ID

An identification name for the user which is unique for the entire messaging server (unique across all mail domains). This is the name with which the user will authenticate for IMAP or POP access. It must consist of alphanumeric characters and digits; hyphens (-) and underbars (_) may also be used. Dots (.) and other special characters are not allowed. Example: *joes*.

> **Note:** This name cannot be the the same as any system user name.

First Name

The first name of the user (example: "Joe").

Last Name

The last name of the user (example: "Smith").

> **Note:** A **Display Name** is created by default in the **View Users** menu from the first and last names.

***Mail address**

The primary Internet email address for the user. The mail domain is automatically set to the domain listed in the **Server Manager** toolbar. The name used here does not have to be the same as the **User ID**.

> **Note:** The **Mail address**does not have to be the same as the **User ID**. For example, you might want to create **User ID** `joes` with the **Mail address** `joe.smith@my_company.com`. If you set **User IDs** and **Mail addresses** to be different on your system, make sure your mail client users understand the difference; they cannot log in to the Messaging Server with a **Mail address** that differs from their **User ID**.

***Password**

The user's password used to authenticate for IMAP/POP/LDAP access. You must confirm the password you entered.

Work Phone

The business phone number of the user.

Mobile Phone

The mobile phone number of the user.

Home Phone

The home phone number of the user.

Pager

The pager number of the user.

FAX

The facsimile telephone number of the user.

Title

> The job title for the user.

Office Location

> The physical delivery office name for the user.

Alternate Mail

> An alternate email address for the user. The email address must be qualified with the name of the mail domain under which the user resides, which is automatically set to the domain listed in the **Server Manager** toolbar.

> **Note:** This field can only be modified using the **Server Manager**; users cannot do so.

Forward Mail To:

> An email address to which to forward all the user's email.

When you have entered all required and optional information, click on **Create** to enter the new user account information.

Delete User

Select a *User ID* to delete. When you click on **Select**, all the associated user information is erased from the LDAP database. You can also delete users from the **View Users** display.

Caution

If you delete a user who is the last owner or member of an alias, the alias will be silently deleted. Before removing a user, we recommend that you see check their aliases; to do so, click on **Aliases** in their **View User** display. For this reason, we also recommend that every alias have at least two owners, and that important aliases also include the *admin* user as an owner or member.

You cannot delete the *admin* user.

Managing Mail Aliases

You can create and modify mail aliases on the SCO*office* Mail Server. Mail aliases allow you to:

- use a single mail address to deliver mail to a group of users.
- deliver mail to a single user under a variety of user names.
- map one email address to another for purposes of mail routing.
- append mail to files for archival purposes.
- filter or process mail through programs.

> **Note:** If you have large numbers of users or aliases on your SCO*office* Mail Server, it may take some time to load the **View** displays, and these displays may occupy many screens.

Use the **Server Manager** to enter and modify mail alias information. In the **Aliases** menu, click on:

- **View Aliases**
- **Find Aliases**
- **Create Aliases**
- **Delete Aliases**

View Aliases

Lists all aliases in the selected mail domain, sorted by *Alias*. Clicking on the *Alias* link displays the complete alias information. From this display you can take these **Alias Actions**:

- **Modify** the **Description** and **Membership** settings
- add or remove alias **Members**; enter names or **Browse** user and alias lists
- add or remove alias **Owners**
- specify **Programs/Files** for the alias
- **Delete** this alias

<div style="border:1px solid black; padding:1em;">

Caution

If you delete a user who is the last owner or member of an alias, the alias will be silently deleted. Before removing a user, we recommend that you see check their aliases; to do so, click on **Aliases** in their **View User** display. For this reason, we also recommend that every alias have at least two owners, and that important aliases also include the *admin* user as an owner or member.

</div>

Find Aliases

Search for an alias in the selected mail domain. You can enter a full or partial word to be found in the *Alias* or *Name* fields. Click on the *Alias* links in the search results to display alias information and take **Alias Actions**.

Create Aliases

Create a new alias. Required entries are marked with asterisks "*"; on some browsers, optional entries are displayed when you click on **More**.

When you create an alias, you must specify an owner and members. In addition to manually entering individual names, you can also click on **Browse** to view lists of owners, users, and aliases in the current domain. To add a owner, user or alias to the new alias, click on the plus sign (+) in **Add** column, and the user name will be added in the **Create Aliases** screen. Close the **Browse** window when you have finished selecting new owners or members.

*Alias

An identification name for the alias which is unique for the entire messaging server (unique across all mail domains), appended with the name of the mail domain under which the alias resides. This mail domain is automatically set to the domain listed in the **Server Manager** toolbar.

Description

The description of the mail alias. Example: "The Company Glee Club".

*Owner

The email address(es) of owner(s) of the alias; there must always be at least one owner. By default, the user that creates an alias is automatically listed as an owner and a member, but this default does not apply to *admin* users, who must explicity add themselves as owners or members if desired. Multiple owners are permitted, each of whom have the ability to modify alias attributes, add and remove owners, and delete the alias. Only existing owners can add or remove other owners; if an alias is restricted, only owners can add or remove members.

> **Note:** We recommend that every alias have at least two owners, and that important aliases also include the *admin* user as an owner or member.

Membership

Radio buttons indicating whether the alias is **Open** or **Restricted**; the default is **Open**. Users can add or remove themselves to or from an **Open** alias, but a user cannot add or remove others from an **Open** alias unless that user is also an owner. To add or remove themselves to or from **Restricted** aliases, users must ask an owner.

*Alias Member(s)

The email address(es) of members of the alias. At least one member must be added, in a comma-separated list. Members can be entered as:

- **User ID**s (if in the current mail domain).

- aliases (if in the current mail domain). A mail alias can contain the names of other aliases.

- complete email addresses (if in a different mail domain).

Append File

The path of a file on the system to which mail to this alias will be appended. This file must conform to Postfix specifications for the `/file/name` value in alias database input files; see the Postfix *aliases*(5) manual page for further information. Mail cannot be appended to files owned by *root*. Only the *admin* user can set this attribute.

Pipe Program

A program through which to pipe a message sent to the alias. This command must conform to Postfix specifications for the `|command` value in alias database input files; see the Postfix *aliases*(5) manual page for more information. Only the *admin* user can set this attribute.

<div style="border:1px solid black; padding:1em;">

Caution

If used improperly, setting the **Append File** and **Pipe Program** options can cause serious system problems, such as filesystem overruns and security breaches.

</div>

When you have entered all required and optional information, click on **Create** to enter the new alias information.

Delete Aliases

Select an `Alias` to delete. You can also delete users from the **View Aliases** display.

Backup and Restore

Backing Up the SCO*office* Mail Server

To protect users against accidental file deletion and catastrophic system failures, backups of the SCO*office* Mail Server should be performed regularly. Particular care should be taken to make regular (and multiple) backups of the file */var/imap/mailboxes.db*. See the discussion under "Mail Directory Recovery " below for more information.

Linux backup utilities such as **tar**(1), **cpio**(1L), and **afio**(1) may be used to backup and restore the SCO*office* Mail Server. Commercial backup products are also available, which offer many additional features including faster restore. The current list of supported backup products can be found in the *Late News* document on the SCO*office* Mail Server documentation website:

http://www.sco.com/support/docs/SCOoffice/mail

```
                        Caution

We recommend that you stop the ldap service using the command line with the
/etc/rc.d/init.d/ldap script before performing any SCOoffice Mail Server backup
```

Restoring Accidently Deleted Email

To restore a specific user's email, simply restore the contents of the
directory */var/spool/imap/user/UserID*, where *UserID* is the SCO*office* Mail Server unique identifier for
that user. After restoring the directory, you must run the command:

```
su cyrus -c /usr/cyrus/bin/reconstruct
```

This will inform the SCO*office* Mail Server that old email has been restored and should now made
visible to users.

See also the **reconstruct**(8) manual pages.

Configuring Failover Scripts for the SCO*office* Mail Server in a Cluster Environment

ReliantHA Update 1.1.2 contains sample failover scripts for configuring the SCO*office* Mail Server into a
cluster environment. This update can be downloaded for free from http://www.sco.com/downloads.

Mail Directory Recovery

This section describes how to perform disaster recovery on the various databases used by the Cyrus
IMAP component of the SCO*office* Mail Server. Inconsistencies can occur in these databases in the event

of an unforseen event such as a system crash.

Should a mail system failure occur, first view the log files and try to determine what went wrong. Of particular interest are the files:

- */var/log/imapd*
- */var/log/messages*
- */var/log/mail*

The SCO*office* Mail Server provides special tools needed to recover the IMAP databases. All of the tools described below can be found in the */usr/cyrus/bin/*.

Reconstructing Mailbox Directories

The largest databases in the SCO*office* Mail Server are stored in mailbox directories. By default the SCO*office* Mail Server mailbox directories are found under */var/spool/imap/user/**user_name***.

Each mailbox directory contains message files. There is one message file for each message stored on the IMAP server. The name of each message consists of the message's unique identifier number, followed by a dot (.).

In addition to the message files, each mailbox directory also may contain the files *cyrus.header*, *cyrus.index*, *cyrus.cache*, and *cyrus.seen*. Each of these files contains additional information about the mailbox which is used by the Cyrus IMAP server.

The **reconstruct** utility is used to recover from mailbox directory corruption. An administrator can recover from a damaged disk by restoring message files from a backup and running the **reconstruct** command to regenerate what it can of the other files. By default, **reconstruct** acts on all of the mailbox directories on the system. After running **reconstruct**, you should also run **quota -f** as described below.

See also the **reconstruct**(8) and **quota**(8) manual pages.

Restoring the Mailbox List Database

The mailboxes file, */var/imap/mailboxes.db*, is the most critical file in the Cyrus IMAP system. It contains a sorted list of each mailbox on the server, along with the mailboxes *quota root* and *ACL*. The command **ctl_cyrusdb -r** can be used to restore Cyrus database files if they become corrupt. Should that fail, a copy of the *mailboxes.db* file is saved in the */var/opt/lsb-sco.com/msg/* directory every time a cyrus mailbox is created, deleted, or modified by any of the SCO*office* Mail Server tools. Should all else fail, you may restore this copy to the */var/imap* directory and run **ctl_cyrusdb -r**. The **ctl_cyrusdb** utlity is automatically run every time the Cyrus IMAP server is started

See also the **ctl_cyrusdb**(8) manual page.

Restoring Subscription Files

The subdirectory */var/imap/user* of the configuration directory contains user subscriptions. There is one file per user, with a filename of the userid followed by the suffix *.sub*. Each file contains a sorted list of subscribed mailboxes.

There is no program to recover from damaged subscription files. You may recover from lost files simply by restoring from backups.

Chapter 4. Managing Clients

Client Administration

Mail client software must be configured to authenticate with and receive messages from the SCO*office* Mail Server. Configuration procedures are explained in "Enabling Outlook Client Users", with instructions for mail client users to run client configuration tools on their personal systems.

Once mail client software is configured and mail accounts created as described in "Managing Mail Users". See also the *Client User's Guide*.

Most mail client software allows multiple mailboxes. That is, a mail client user could access several mail accounts from the same mail client and manage the mailboxes separately. The guidelines in SCO*office* Mail Server documentation for configuring mail clients assume that only SCO*office* Mail Server accounts will be configured on the client. Although other mail accounts can be created or might already exist, you might want to set a policy regarding your support of multiple accounts.

Enabling Mail Client Users

To enable a mail client user to access their mail from a SCO*office* Mail Server server:

1. Create a SCO*office* Mail Server email account as described in "Managing mail users".

2. In some cases, you must inform users whether to select **IMAP** or **POP** in the server configuration selection screens.

3. Provide this account information to the user so they can access the **Preferences Manager** and configure their mail client software.

4. If you are migrating existing mail users to a SCO*office* Mail Server installation, you might need to inform them of potential changes to the appearance and behavior of their mail client software.

Follow the instructions in this section to enable these mail clients:

• Outlook and Outlook Express

- Netscape Messenger

- Eudora Mail

- KMail

- IMP webmail

> **Note:** Online Help screens in the **Preferences Manager** provide detailed configuration instructions from the *Client User's Guide*. These instructions are derived from information presented in the following sections.

Enabling Outlook Client Users

Both Outlook and Outlook Express can be configured to use the mail and LDAP directory services of the SCO*office* Mail Server. Outlook Express is mainly a mail client and is distributed as a component of Internet Explorer, which is included with Microsoft Windows operating systems. Outlook is a full-featured messaging and collaboration client application that is included with Microsoft Office. Under normal circumstances, only one of these clients is used at a time, although they can be run simultaneously.

A SCO*office* Mail Server **Outlook Configuration Tool** is available to automatically configure these clients.

General Outlook Client Requirements

Before running the **Outlook Configuration Tool**, the client MS Windows system must have:

- networking installed and configured.

- Internet Explorer 5 or greater.

- no running copies of Outlook.

No special configuration is required for Outlook Express.

Outlook 2000 and Outlook 98 Requirements

Outlook 2000 and Outlook 98 can be installed in three configurations:

Corporate/Workgroup

> required configuration if SCO*office* Mail Connector for Microsoft Outlook is in use.

Internet Email Only

> required configuration if SCO*office* Mail Connector for Microsoft Outlook is not in use.

no email

> not supported for SCO*office* Mail Server use.

For more information regarding use of Outlook 2000 features, refer to your Microsoft documentation. In addition, the Microsoft Knowledge Base article Q197636 describes using Outlook 2000 with an IMAP4 server. See also the Microsoft document *Microsoft Outlook 2000 Features and Configuration Guide* available on the Microsoft website at http://www.microsoft.com/office/outlook/

Outlook Client Configuration Tool

The **Outlook Configuration Tool** can detect and configure both Outlook and Outlook Express clients. When a user downloads the **Outlook Configuration Tool** from the **Preferences Manager**, a custom configuration data file for that user is generated and downloaded with the configuration program. This data file contains email address, directory binding, and calendar information specific to the user who downloads it.

The **Outlook Configuration Tool** configures two Internet Accounts for Outlook Express clients:

* *Internet email - SCOoffice Mail Server*
* *LDAP - SCOoffice Mail Server*

The **Outlook Configuration Tool** prepares Outlook clients depending on their mode:

Internet Email Only mode

> Configures two Internet Accounts:

> • *Internet email - SCOoffice Mail Server*

> • *LDAP - SCOoffice Mail Server*

Corporate/Workgroup mode

> Installs and creates the "SCOoffice Mail Server" MAPI profile, which contains the following
> accounts and services:

> • IMAP mailbox

> • Outlook Address book (includes LDAP information)

> • calendar information

> • Personal Folders

> When the user starts Outlook 2000 in Corporate/Workgroup mode, the "SCOoffice Mail Server"
> profile should be selected. Refer to your Microsoft Outlook 2000 documentation for further
> information regarding the usage of Profiles and setting a default Profile.

> **Note:** The **Outlook Configuration Tool** does not alter existing mail accounts. If any existing
> accounts need to be modified or removed, this must be done manually.

The **Outlook Configuration Tool** creates a shortcut on the Desktop and a shortcut in the Outlook
shortcut bar, which when selected bring up a browser window that displays the main screen of the
SCO*office* Mail Server user interface. It also adds a **Volution** menu with a button that launches the
SCO*office* Mail Server user interface.

When the Outlook configuration program completes, it removes itself from the system.

Managing Outlook Client Configuration

If the user's mail client has not already been configured for the SCO*office* Mail Server, instruct them to
do so:

  1. Close Outlook or Outlook Express if you are currently using it.

> **Note:** If you are running an Outlook 2000 or Outlook 98 mail client, your mail administrator might direct you to configure your mail client in either *Corporate/Workgroup* mode or *Internet Email Only* mode. If this is the case, you must configure your mail client before running the **Preferences Manager**.

2. Log into **Preferences Manager** by pointing your browser at:

   *https://**hostname**/msg*

   where **hostname** is the system name supplied by the mail administrator for **Preferences Manager** access.

3. Enter your mail account name and password when the **Preferences Manager** screen appears.

4. Click on the **Client Setup** in the **Preferences** menu. This displays configuration information used by your mail client software to communicate with the SCO*office* Mail Server.

5. Run the client configuration program by clicking the **Configure** button. The client configuration screen includes instructions on how to respond to further prompts.

6. In the **File Download** dialogue window, select **Run this program from its current location**.

   > **Note:** If you are using the Netscape browser, you may see a dialogue window indicating "Unknown File Type". If you see this message:
   >
   >   a. Click on **Pick App** in the dialogue window. A new dialogue window displays.
   >
   >   b. Type "wscript" in the box and click on **OK**. A new dialogue window displays.
   >
   >   c. Select the **Open It** checkbox and click on **OK**.
   >
   > You can now proceed to the next step.

7. When prompted to configure your system with the SCO*office* Mail Server, click on **Yes**.

   During the installation, you might be informed that Outlook is being started. If this is the first time Outlook has been run on your system, you will be prompted to select a networking mode; select `Corporate/Workgroup` or `Internet Email Only` depending on your Mail Administrator's instructions. If you are prompted to create an email account, click on **Cancel** or **Close** to exit the account creation dialog; it is not necessary to configure an account at this time.

You might see a dialog box informing you that your Outlook client is configured in Internet Email Only mode. If this is correct, click on **Yes** to continue. If not, click on **No** to cancel the installation, configure your Outlook client in Corporate/Workgroup mode, and restart the **Client Setup** procedure.

8. The **InstallShield Wizard** informs you that it is preparing to install the Volution SCO*office* Mail Server Com-Addin if it is not already present on your system. Click on **Next** to continue.

   After a short time, you are informed that Volution SCO*office* Mail Server Com-Addin files are being copied to your system. Click on **Finish** when prompted by the **InstallShield Wizard**, and click on **OK** when Volution SCO*office* Mail Server configuration is complete.

This completes mail client configuration. When you start your Outlook client, you will be able to receive email with your new account. If the SCO*office* Mail Connector for Microsoft Outlook is installed, you must log in with your SCO*office* Mail Server UserID.

> **Note:** The **Outlook Configuration Tool** indirectly configures Outlook XP by setting up Internet Email Accounts. When Outlook XP is started after running the **Outlook Configuration Tool**, it will prompt the user to import the new Internet Email Accounts that it has found. The user *must* click on **Yes** to have these new accounts configured within Outlook XP. Note that the LDAP address book for the SCO*office* Mail Server will be configured but will not appear in the list of address books until Outlook XP is restarted after importing the accounts.

You must also instruct mail users to set mail preferences with **Preferences Manager** as described in "Managing Client Preferences".

Outlook Sent Items Folder

When you configure your SCO*office* Mail Server mailbox as a POP3 mailbox, the *Sent Items* folder functions as expected because the messages are physically stored and managed on the client. However, with IMAP mailboxes (the SCO*office* Mail Server default), the messages physically reside on the server. You can still configure Outlook to save copies of outgoing messages to the *Sent Items* folder in the

Outlook *Personal Folders* collection (Outlook Today). You do not need a separate *Sent Items* folder under your IMAP SCO*office* Mail Server *Inbox*.

If you want to store the contents of your *Sent Items* folder on the SCO*office* Mail Server, use the **Rules Wizard** to create a rule that selects all outgoing messages and specifies that they be copied to a folder of your choice, including a folder on the SCO*office* Mail Server.

You can also create a new folder under your IMAP Inbox by right-clicking on your IMAP *Inbox* and selecting **New Folder**. Periodically drag the contents of the *Sent Items* folder to this new folder under your IMAP *Inbox*.

Outlook Deleted Items Folder

Outlook does not does not copy messages deleted from an *IMAP* folder (that is, the SCO*office* Mail Server mailbox) to the *Deleted Items* folder as it does for POP3 mailboxes. If you want this functionality, you must do one of the following:

- When you want to delete a message from your *IMAP* folder, drag it to the *Deleted Items* folder. This action will make a copy of the message in the *Deleted Items* folder and will mark it as deleted in your *IMAP* inbox.
- If you want to have your deleted messages stored on the server, create a folder for these messages under your *IMAP* inbox. Drag any messages that you want to delete from your *IMAP* inbox to this new folder. Again, this action will mark the message as deleted in your *IMAP* inbox.

Enabling Netscape Messenger Client Users

Netscape Messenger can be configured to use the mail and LDAP directory services of the SCO*office* Mail Server. The SCO*office* Mail Server also supports Netscape Address Book; for more information, see Netscape Help.

If the user's mail client has not already been configured for the SCO*office* Mail Server, instruct them to do so:

1. Close Netscape Messenger if you are currently using it.
2. Log into **Preferences Manager** by pointing your browser at:

*https://**hostname**/msg*

where ***hostname*** is the system name supplied by the mail administrator for **Preferences Manager** access.

3. Enter your mail account name and password when the **Preferences Manager** screen appears.

4. Click on the **Client Setup** in the **Preferences** menu. This displays configuration information used by your mail client software to communicate with the SCO*office* Mail Server. Keep this screen available or print its contents.

5. Start Netscape Messenger.

6. In the **Edit** menu, select **Preferences**, then open **Mail & Newsgroups**.

7. In the **Identity** preferences panel of **Mail & Newsgroups**, enter your user information in the boxes. The `Your name` and `Email address` fields are required, and the `Your name` field in Netscape Messenger must have the same contents as the `Name` field in the **Client Setup** display.

8. In the **Mail Servers** preferences panel of **Mail & Newsgroups**, click on **Add** under **Incoming Mail Servers** to add the SCO*office* Mail Server machine.

    a. Under the **Mail Server Properties General** panel:

    `Server Name`

       enter the machine name on which the SCO*office* Mail Server resides.

    `Server Type`

       select `IMAP Server` or `POP3 Server`.

    `User Name`

       enter the `Account name` from the **Preferences Manager** client configuration display.

    b. If you selected `IMAP Server`, under the **Mail Server Properties Advanced** panel:

    `IMAP service directory`

       enter **user.name**, where ***name*** is the value you entered for `User Name`.

9. In the **Mail Servers** preferences panel of **Mail & Newsgroups** under **Outgoing Mail Server**:

`Outgoing mail (SMTP) server`

    enter the machine name on which the SCO*office* Mail Server resides.

```
Outgoing mail server user name
```
> enter value you entered for `User Name`.

This completes mail client configuration. When you restart Netscape Messenger, you will be able to receive email with your new account.

> **Note:** For Netscape Messenger Release 4.7, there is no SCO*office* Mail Server support for using the SCO*office* Mail Server LDAP directory for roaming access.

You must also instruct mail users to set mail preferences with **Preferences Manager** as described in "Managing Client Preferences".

To set up the Netscape Messenger LDAP address book to use the SCO*office* Mail Server:

1. Start Communicator.

2. Select **Communicator→Address Book**.

3. In the Address Book screen, select **File→New Directory**.

4. Enter:
    ```
    Description : SCOoffice Mail Server
    LDAP Server : server_name
    Server Root : server_root
    ```

    You can obtain the `Server Root` value from the **Client Setup** screen as the `Searchbase` parameter.

Enabling Eudora Mail Client Users

If the user's mail client has not already been configured for the SCO*office* Mail Server, instruct them to do so:

1. Close Eudora Mail if you are currently using it.

2. Log into **Preferences Manager** by pointing your browser at:

   *https://**hostname**/msg*

   where ***hostname*** is the system name supplied by the mail administrator for **Preferences Manager** access.

3. Enter your mail account name and password when the **Preferences Manager** screen appears.

4. Click on the **Client Setup** in the **Preferences** menu. This displays configuration information used by your mail client software to communicate with the SCO*office* Mail Server. Keep this screen available or print its contents.

Further configuration depends upon whether they are:

• configuring their Eudora client for the first time.

• configuring your Eudora client with SSL security.

• reconfiguring their Eudora client for the SCO*office* Mail Server.

Initial Configuration With the Eudora Setup Wizard

The first time Eudora is launched, the **Eudora New Account Setup Wizard** will appear. Proceed through the setup screens, entering information as requested and clicking on **Next** to continue.

1. In the **Account Settings** screen, select **Create a brand new email account**.

2. In the **Personal Information** screen, enter **Your Name** from the **Name** field in the **Preferences Manager Client Setup** display.

3. In the **Email Address** screen, enter the **Email Address** from the **Preferences Manager Client Setup** display.

4. In the **Login Name** screen, enter **Login Name** from the **Name** field in the **Preferences Manager Client Setup** display.

5. In the **Incoming Email Screen** screen:

   • enter **Incoming Server** from the **Server Name** field in the **Preferences Manager Client Setup** display.

   • select **POP** or **IMAP** according to administrator guidelines.

If **IMAP** is selected, an **IMAP Location Prefix** screen will be displayed. Leave the **Location Prefix** box blank.

- select **Never** from the **Secure Sockets when Receiving** list.

6. In the **Outgoing Email Screen** screen:

- enter **Outgoing Server** from the **Server Name** field in the **Preferences Manager Client Setup** display.

- select **Never** from the **Secure Sockets when Receiving** list.

7. Click on **Finish** to complete configuration and exit the **Setup Wizard**. When you restart Eudora, you will be able to receive email with your new account.

SSL Configuration for Eudora Mail

Eudora Mail and the SCO*office* Mail Server both provide SSL (Secure Socket Layer) security by default. Eudora provides a commercial Certificate Authority (CA) key, and the SCO*office* Mail Server provides a demonstration key with the option of enabling a commercial key.

However, the Eudora default security configuration does not work correctly with the SCO*office* Mail Server. Eudora tries to determine if TLS (Transport Layer Security) is supported by mail servers it connects with, and if not, to configure mail service without SSL. This check fails with this version of SCO*office* Mail Server and Eudora 5.1; Eudora does not find the SSL alternate port and does not transfer mail.

To work around this problem, you must manually enable or disable SSL on your Eudora client. To do so:

1. Start Eudora and select **Tools→Options**.

2. Click on **Checking Mail**.

The default value for the **Secure Sockets when Sending** field is **Use TLS if Available**. You must change it to one of the following entries:

Never

to receive mail without SSL security.

Required, Alternate Port

> to receive mail with SSL security.

Other selections will disable mail transfer.

3. Click on **Sending Mail**.

The default value for the **Secure Sockets when Receiving** field is **Use TLS if Available**. You must change it to one of the following entries:

Never

> to send mail without SSL security.

Required, Alternate Port

> to send mail with SSL security.

Other selections will disable mail transfer.

4. Restart Eudora.

If you elected to disable SSL, this completes Eudora client configuration. Mail users can now use Eudora to send and receive email without SSL security.

If you elected to enable SSL, you must have a server key and certificate of authority. If you have not already done so, you must use **Webmin** to generate a Certificate Signing Request (CSR) from a commercial Certificate Authority (CA) provider, or generate a self-signed certificate and key. For more information, see "Enabling SSL" in the *Administrator's Guide*.

If you obtained a server key and certificate from a company for which Eurora already provides trusted client certificates (such as Verisign®), this completes Eudora client configuration. Verify that Eudora has accepted the server certificate:

a. Select **Tools→Options**

b. Click on **Checking Mail**.

c. In the **Last SSL Info**, confirm that the server certificate is in the trusted list.

5. If you did not obtain a server key and certificate from a company for which Eurora already provides trusted certificates or you generated your own key and certificate, you must manually configure Eudora to authenticate with the SCO*office* Mail Server.

   Start Eudora and select **Tools→Options** You will be prompted to provide the password for your account, after which the download of the mail will fail.

   Attempt to download mail a second time; this will also fail, but the error message will indicate that Eudora does not trust the certificate supplied by the server.

6. From the Eudora menu bar, select **Tools→Options**. Then click on **Checking Mail** and select **Last SSL Info**.

7. In the **Certificate Not Trusted** dialog box, click on **Certificate Information Manager**. Select the server certificate for your mail server from the list of known untrusted server certificates, then click on **Add to Trusted**.

8. Restart Eudora.

   This completes Eudora client configuration. Mail users can now use Eudora to send and receive email with SSL security.

Modifying Eudora Configuration

1. In the Eudora **Tools** menu, select **Options**.

2. Click on **Getting Started**, then enter:

   Real Name

   > from the **Name** field in the **Preferences Manager Client Setup** display.

   Return Address

   > from the **Email Address** field in the **Preferences Manager Client Setup** display.

   Mail Server

   > from the **Server Name** field in the **Preferences Manager Client Setup** display.

   Login Name

   > from the **Account Name** field in the **Preferences Manager Client Setup** display.

SMTP Server

> from the **Server Name** field in the **Preferences Manager Client Setup** display.

Allow Authentication

> check the box (this should be the default).

3. Click on **Checking Mail**, then enter:

Mail Server

> from the **Server Name** field in the **Preferences Manager Client Setup** display.

Login Name

> from the **Account Name** field in the **Preferences Manager Client Setup** display.

Secure Sockets when Receiving

> select **Never**.

other fields

> use defaults.

4. Click on **Incoming Mail**, then enter:

Server Configuration

> select **POP** or **IMAP** according to administrator guidelines.

Authentication Style

> select **Passwords**.

other fields

> use defaults.

5. Click on **Sending Mail**, then enter:

Return Address

> from the **Email Address** field in the **Preferences Manager Client Setup** display.

SMTP Server

> from the **Server Name** field in the **Preferences Manager Client Setup** display.

Secure Sockets when Receiving

> select **Never**.

other fields

> use defaults.

6. Click on **OK** to complete configuration and exit. When you restart Eudora, you will be able to receive email with your new account.

Enabling KMail Client Users

If the user's KMail client has not already been configured for the SCO*office* Mail Server, instruct them to do so.

1. Close KMail if you are currently using it.

2. Log into **Preferences Manager** by pointing your browser at:

   *https://**hostname**/msg*

   where ***hostname*** is the system name supplied by the mail administrator for **Preferences Manager** access.

3. Enter your mail account name and password when the **Preferences Manager** screen appears.

4. Click on the **Client Setup** in the **Preferences** menu. This displays configuration information used by your mail client software to communicate with the SCO*office* Mail Server. Keep this screen available or print its contents.

5. Log into your system and start KMail. If this is the first time KMail has been run, click on **OK** to create a *Mail* subdirectory in your home directory.

6. In the KMail **Settings** menu, select **Configuration** .

7. Click on **Identity**, then click on **New Identity**. Enter **New Identity** from the **Account Name** field in the **Preferences Manager Client Setup** display, and select "**With empty fields**".

8. When your **New Identity** is displayed, enter:

   Name

   > from the **Name** field in the **Preferences Manager Client Setup** display.

Email Address

> from the **Email Address** field in the **Preferences Manager Client Setup** display.

Reply To Address

> from the **Email Address** field in the **Preferences Manager Client Setup** display.

Signature

> specify a file or enter a signature message in the box.

Click on **Apply** to save your selections in the **Identity** screens.

9. Click on **Network** and **Sending Mail**, then select:

SMTP

> Enter **Server** from the **Server Name** field in the **Preferences Manager Client Setup** display, and use the default port number (unless instructed otherwise by your mail administrator).

Incoming Mail

> Select **Pop3**, then enter:

> **Name**

>> from the **Name** field in the **Preferences Manager Client Setup** display.

> **Login**

>> from the **Account Name** field in the **Preferences Manager Client Setup** display.

> **Password**

>> of your choice; you can elect to have KMail remember this password.

> **Host**

>> from the **Server Name** field in the **Preferences Manager Client Setup** display.

> **Port**

>> use the default.

other fields

Enter additional information as desired.

Click on **Apply** to save your selections in the **Network** screens.

10. Set **Network Properties** as desired and click on **Apply** to save your selections in the **Network** screens.

11. Click on **OK** to complete configuration and exit. When you restart KMail, you will be able to receive email with your new account.

Enabling IMP Webmail Client Users

IMP client users do not need to enter configuration information from the **Preferences Manager Client Setup** display. To log into the IMP webmail client, they need only know:

· their SCO*office* Mail Server account name and initial password.

· their SCO*office* Mail Server email address.

· the IMP client URL, usually:

*https://**hostname**/horde/imp*

If the user's IMP account has not already been configured for the SCO*office* Mail Server, instruct them to do so:

1. Log into IMP by pointing your browser at:

*https://**hostname**/horde/imp*

2. Enter your account name and password.

3. Click on **Preferences** and enter your SCO*office* Mail Server account name and email address.

This completes IMP client configuration. To view and modify your SCO*office* Mail Server user preferences, log into **Preferences Manager** by pointing your browser at:

*https://**hostname**/msg*

where ***hostname*** is the system name supplied by the mail administrator for **Preferences Manager**
access. When you enter your mail account name and password, you will see the **Preferences Manager**
screen.

> **Note:** The IMP webmail client does not work consistently on Netscape 6.0 and 6.1 browsers; you
> must upgrade to Netscape 6.2. You can also connect to the SCO*office* Mail Server from an IMP
> client on Netscape 4.7.
>
> If you attempt to use the IMP webmail client to send a large attachment (greater than 1Mb), you
> might get an error message such as the following:
>
> ```
> Warning: Undefined variable: attachments_size in
> /home/httpd/html/horde/imp/compose.php3 on line 930
> ```
>
> To resolve this problem, you must increase the value of `upload_max_filesize` in the
> */etc/httpd/php.ini* to an appropriate value, as described in the Technical Article "I get an 'Undefined
> variable' warning when trying to attach a large attachment within SCOoffice Mail Server WebMail"
> (Ref.#116659) (Ref.#116659), available from the SCO Support Knowledge Base site:
>
> ```
> http://support.caldera.com/caldera/
> ```

Managing Client Preferences

Mail client users can set their own mail preferences with **Preferences Manager**. When they log in with a
valid mail account name and password, they are presented the same user preferences as displayed on the
administrative screens, although no other configuration options are presented:

- **Preferences**
- **Users**
- **Aliases**

You must instruct users on using **Preferences Manager** to set mail preferences:

1. Close your email client software.

2. Log into **Preferences Manager** by pointing your browser at:

   *https://**hostname**/msg*

   where ***hostname*** is the system name supplied by the mail administrator for **Preferences Manager** access.

3. Enter your mail account name and password when the **Preferences Manager** screen appears.

4. Enter, modify or display your email options.

5. When you have completed email configuration, click the **Logout** button to exit **Preferences Manager**. Your new or modified preferences will be in effect the next time you start your email client.

Help screens are also available from the user preferences page.

Preferences

Your Profile

Displays your personal information. To modify it, enter or edit the desired fields, and click the **Apply** button to enter your changes.

Forward email

When set, forwards your email to the address you enter in the box.

- To forward your mail, enter an email address and click on **Apply**.
- To disable forwarding, erase the contents of the box and click on **Apply**.

Vacation email

When set, sends a vacation message; that is, an automatic reply for all email you receive during a vacation or extended absence. A list of messages sent is also maintained.

- To enable vacation email, click on **Vacation email on**. You can also customize the subject heading and content of your vacation message. If you do not enter a subject or content, the

following defaults are set:

Subject

```
Absence notification
```

Message

```
This is an automated reply: This person is temporarily out of the
office
```

- To disable forwarding, click on **Vacation email off**. You may also want to clear your list of messages sent.

> **Note:** The postfix virtual maps feature can be used to remap multiple domain names to a single name by using the **@domain altdomain** directive. Similarly, you may use MX records to deliver all email for multiple domains to a single server and alter the postfix **mydestination** to include the additional domains. In cases such as this, users belong to not one, but multiple simultaneous domains. To ensure proper vacation handling, the administrator will want to make use of the *domains.conf* feature. The file */etc/opt/lsb-sco.com/msg/domains.conf* should be edited to include a list of all of the alternate domains, one per line, supported by the system. This file is used by the vacations feature to help determine whether a vacation message should be sent to the sender. By default, vacation replies are only sent in reply to mail messages explicitly sent to (To: or cc:) the sender and not to mail messages sent out as blind copies (bcc:) or to aliases. Without a domains.conf entry, only messages sent to the primary address of users can be treated as a valid case for a vaction reply.

Change Password

To change your password, enter your old password, enter a new password, retype the new password, and click on **Apply**.

Client Setup

Displays information required by clients to communicate with the SCO*office* Mail Server. Clicking the **Configure** downloads this information to your email client.

> **Note:** Downloading Outlook configuration information is usually performed only once per user. Outlook client users should not repeat this step unless instructed to do so.

Users

Find Users

Allows you to search for users based on `UserId`, `Name`, and `Email Address` fields, and you can enter partial strings. You can also browse the complete list of email users by clicking the **Show All**. For each account listed, you can view their profile and aliases to which they subscribe.

Aliases

Your Aliases

Displays aliases for which you are the Owner or a Member.

Find Aliases

Allows you to search for aliases or browse a list of available aliases. You can also browse the complete list of email aliases by clicking the **Show All**.

Create Alias

Allows you to create aliases.

Chapter 5. Security

Preventing Open Mail Relay

The SCO*office* Mail Server supports POP-Before-SMTP by default using the the Dynamic Relay Authentication Control (DRAC) server. This feature prevents people from using the site as a relay unless they previously have authenticated with the server via POP or IMAP.

The **rpc.dracd** program uses the Berkeley DB package to maintain a relay authorization map for Postfix. The Cyrus server has been modified to make an RPC call to notify the **rpc.dracd** daemon to add new host entries to the authorization map for each user after they have logged in using POP or IMAP. The **rpc.dracd** daemon is then responsible for adding or updating entries in the authorization map and for periodically expiring old entries (by default, every 30 minutes).

For more information, see:

- the **dracauth**(3) and **rpc.dracd**(1m) manual pages
- The DRAC home page (http://mail.cc.umanitoba.ca/drac/index.html)

Avoiding Viruses

Integrating Anti-Virus Software

The SCO*office* Mail Server provides integration with anti-virus software. To enable supported anti-virus software:

1. Install the anti-virus software.

2. Tell Postfix to enable virus scanning on the system by uncommenting the content_filter parameter in the */etc/postfix/main.cf* file and running **postfix reload**.

3. Edit the */etc/opt/lsb-sco.com/msg/vscan.conf* file and remove the comments appropriate to your anti-virus software.

For more information, see:

- the vscan.conf(5) manual page

- the current list of supported anti-virus software packages in the *Late News* document on the SCO*office* Mail Server documentation website:

  http://www.sco.com/support/docs/SCOoffice/mail

- your anti-virus software product documentation

Filtering Incoming Email

Postfix provides support for filtering the headers of incoming mail messages. In addition to routine message sorting, this can be useful in the early stages of a virus' distribution when the subject heading is known but anti-virus checking software has not been updated to protect against it.

Postfix MTA can protect against such attacks using a "header_checks" file. For example, to block all messages with the subject header ILOVEYOU from being received or propagated:

1. Create the file */etc/postfix/header_checks* with the contents:

   ```
   /^Subject: ILOVEYOU/ REJECT
   ```

2. Change the file ownership to the *postfix* account:

   chown postfix /etc/postfix/header_checks

3. Then modify the file /etc/postfix/main.cf to include:

   ```
   header_checks = regexp:/etc/postfix/header_checks
   ```

4. Restart Postfix using either:

   Server Manager

   In the **System** menu, click on **Mail Services**, then click on **Reload** in the **postfix** display.

command line

Enter:

/etc/rc.d/init.d/postfix reload

Using Sophos MailMonitor With the SCO*office* Mail Server

To configure Sophos MailMonitor for SMTP anti-virus software with the SCO*office* Mail Server, follow this procedure:

1. Familiarize yourself with "Sophos MailMonitor for SMTP (Unix) Release Notes", which are available at:

   http://www.sophos.com/sophos/products/full/readmes/readmsu.txt

2. Install Sophos Anti-Virus for Unix on your SCO*office* Mail Server system before installing MailMonitor. MailMonitor requires SAVI, which is provided by Sophos Anti-Virus for Unix. It is available for download from the Sophos website at:

   http://www.sophos.com/downloads/products/unix.html

   Make sure you get the version labelled "Linux on Intel using libc6" (*linux.intel.libc6.tar*).

3. Install Sophos MailMonitor. It is also available for download from the Sophos website at:

   http://www.sophos.com/downloads/products/smtp.html

   Make sure you get the version labelled "MailMonitor for SMTP on Unix (Linux/Intel)" (*mmsmtp.linux.intel.tar*).

4. Run **install.sh** from the *mmsmtp-install* directory as directed. Make sure that you set the following values:

interface on which **mmsmtp** listens:

```
127.0.0.1:10025
```

smtp_server_address

```
127.0.0.1
```

smtp_server_port

```
10026
```

5. Tell Postfix to enable virus scanning on the system by uncommenting the content_filter parameter in the */etc/postfix/main.cf* file and running **postfix reload**.

   Edit the */etc/postfix/master.cf* file and comment out the first line, which begins with 127.0.0.1:10025. Normally this line runs the **msgvscan**(8) which is not used by Sophos MailMonitor. The edited line should read:

   ```
   # 127.0.0.1:10025
   ```

6. Restart Postfix:

   ```
   /etc/rc.d/init.d/postfix stop
   /etc/rc.d/init.d/postfix start
   ```

7. Start the **mmsmtpd** daemon by entering:

   ```
   /usr/local/sophos/mmsmtp/bin/mmsmtpd -start
   ```

   There should be several **mmsmtp-1.0** processes up and running. They can be monitored by checking the */var/log/mmsmtp/mmsmtp.log* files.

8. Verify that the two ports (10025, 10026) are working by entering:

   ```
   telnet localhost 10025
   EHLO localhost
   MAIL FROM: root@your_domain
   RCPT TO: admin@your_domain
   DATA
   From: root@your_domain
   ```

```
To: admin@your_domain
Subject: Test

This is a test
 .
QUIT
```

Repeat this process with port 10026.

The results of the **telnet** commands to these ports should be similar to:

```
trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 127.0.0.1 ESMTP Postfix
```

A test virus called "Eicar" is available from Sophos. Attach it to an email message and you (and the *admin* and *postmaster* accounts as well) should receive email that a virus has been detected. The email with the virus will be placed by default in the */var/spool/mmsmtp/quarantine directory*.

It is not neccessary to edit the *vscan.conf* (5) file (uncommenting lines, as you would when configuring other anti-virus software) because that file is not used by Sophos MailMonitor.

Enabling SSL

The SCO*office* Mail Server provides SSL (Secure Socket Layer) configuration by default. That is, **https** can be used immediately using demonstration keys, and should be used to provide secure web connections.

However, many SSL benefits are not available without a signed certificate and key. These can be obtained:

- from commercial Certificate Authority (CA) providers, using **Webmin** to generate a Certificate Signing Request (CSR) .

- using **Webmin** to generate a self-signed certificate and key.

We recommend using commercial products, because they guarantee unique certificates, and they provide legal protection. Nonetheless, self-signed certificates are adequate for many installations.

Both self-signed certificates and CSRs can be managed with **Webmin**. In the **Webmin** interface, select **System** and **Certificate and Key Management**. Then select either:

Generate Key and Certificate Signing Request (CSR)

> Use the defaults provided and fill out other forms as desired. The Common Name field must match the SCO*office* Mail Server address. When you receive the signed certificate and key from the Certificate Authority, you must import it using the **Webmin Import Key or Signed Certificate** facility.

Generate Self Signed Certificate and Key

> Use the defaults provided and fill out other forms as desired. The Common Name field must match the SCO*office* Mail Server address. When you generate the key, you will be prompted to overwrite the demonstration keys in the *text/ssl/private* directory; you can safely do so.

Once you have acquired or generated a key, you must provide the Cyrus and Postfix services with read/write access to the key. Assuming that the new key is *text/ssl/private/hostkey.pem*, enter:

```
cd /etc/ssl

cp private/hostkey.pem cyrus-key.pem

chown cyrus cyrus-key.pem

chmod 600 cyrus-key.pem

cp private/hostkey.pem postfix-key.pem

chown postfix postfix-key.pem

chmod 600 postfix-key.pem
```

For more information about SSL configuration, see "Section 4.8. Using Certificate and Key Management" in the *Caldera OpenLinux System Administration Guide*.

Chapter 6. Managing SCO*office* Mail Server Components

The SCO*office* Mail Server installation sets initial configuration parameters for SCO*office* Mail Server components. For most simple mail configurations, it is not necessary to alter these initial values or to configure SCO*office* Mail Server components directly. The **Server Manager** enables you to manage most of the basic SCO*office* Mail Server functionality, including mail administration of mail domains, mail accounts, mail aliases, and other general SCO*office* Mail Server system settings as discussed in "System Settings". In addition to its ease of use, we recommend using the **Server Manager** whenever possible because it is less error-prone than editing files directly.

Nonetheless, the SCO*office* Mail Server supports advanced component configuration for customized installations. To configure the many features available for OpenLDAP, Postfix, and Cyrus, consult the individual documentation available for each configurable component. The following sections cover only those features directly managed by the SCO*office* Mail Server and any integration issues which affect the operation of the SCO*office* Mail Server:

- OpenLDAP
- Postfix
- Cyrus

For more information, see their respective documentation, available from the SCO*office* Mail Server webpage in DocView.

Advanced OpenLDAP Configuration

This section discusses:

- OpenLDAP configuration parameters
- relocating the OpenLDAP database
- configuring a remote OpenLDAP server
- configuring an alternative LDAP server

<div style="border:1px solid black;">

Caution

These are advanced configuration procedures that require extensive LDAP knowledge and experience.

</div>

OpenLDAP Configuration Parameters

The configuration file for OpenLDAP is */etc/ldap/slapd.conf*. It is configured for operation with the SCO*office* Mail Server upon installation. We recommend that you *do not* alter this configuration. In particular, changing the access directives defined for the SCO*office* Mail Server database might disable the SCO*office* Mail Server and the **Server Manager**. For more information, see the *slapd.conf* (5) manual page.

> **Note:** The */etc/ldap.conf* file is the configuration file for the LDAP PAM module and is configured for use with the SCO*office* Mail Server. Do not change the settings in this file.

Relocating the OpenLDAP Database

By default, OpenLDAP is installed with its database in the directory */var/ldap/openldap-ldbm*. You can relocate the queue to a different filesystem, although we recommend that you do so before configuring the SCO*office* Mail Server and enabling mail delivery.

To relocate the OpenLDAP database before the SCO*office* Mail Server is enabled:

1. Shut down the LDAP directory server:

   /etc/rc.d/init.d/ldap stop

2. Copy the existing database to the new location. Use the **cp -p** flag to maintain the proper permissions and ownership of files and directories. For example:

   mkdir -p */new/location*
   cp -pR /var/ldap/openldap-ldbm */new/location*

3. Set the *directory* parameter in */etc/ldap/slapd.conf* to the new path for the database and comment out the old path. For example:

```
# relocated OpenLDAP database for SCOoffice Mail Server use
# directory        /var/ldap/openldap-ldbm
directory         /new/location
```

4. Start OpenLDAP:

   /etc/rc.d/init.d/ldap start

Configuring a Remote OpenLDAP Server

To configure a remote LDAP server:

1. Install the SCO*office* Mail Server on the remote server.

2. On the remote server, run the command:

   /opt/lsb-sco.com/msg/bin/msgldaphost

   This will provide information about server passwords and user entities specific to the remote server.

3. On the local system, run the same **msgldaphost** command to set the system to point to the remote host, and to specify passwords and user entities.

For more information, see the msgldaphost(8) manual page.

> **Note:** If you have configured the SCO*office* Mail Server to use a remote LDAP server, you must provide the LDAP **Server Name** to users when they set up their mail clients. The **Preferences Manager** does not correctly list the remote LDAP server in **Client Setup** screens of the **Preferences** menu. This only affects Netscape, Eudora, and KMail clients; the **Outlook Configuration Tool** correctly adds the remote LDAP server for Outlook clients, and IMP webmail clients do not need to provide this information.

Configuring an Alternative LDAP Server

The SCO*office* Mail Server can be configured to use a directory server other than OpenLDAP; for example, the Sun® iPlanet and Novell® eDirectory directory servers. To do so, you will need information contained in:

schema files

> Schema files for the Sun iPlanet and Novell eDirectory directory servers are installed in the */etc/ldap/schema/netscape* and */etc/ldap/schema/nds* subdirectories.

LDIF files

> An LDIF (LDAP Data Interchange Format) file containing additional information about the required directory content and structure is stored on installed systems as */etc/opt/lsb-sco.com/msg/ldif.base*. See also the *ldif* (5) manual page.

slapd.conf

> The */etc/ldap/slapd.conf* file contains useful information on the ACL's (Access Control Lists) enforced by the SCO*office* Mail Server. See also the *slapd.conf* (5) manual page.

When you have assembled the required information, run the **msgldaphost** command as described in "Configuring a Remote OpenLDAP Server". For more information, see the msgldaphost(8) manual page.

Advanced Postfix Configuration

This section discusses:

• Postfix configuration parameters

• relocating the Postfix message queue

• managing large messages and attachments

Postfix Configuration Parameters

Postfix configuration is controlled by parameters in the*/etc/postfix/main.cf* file. Although there are around 100 parameters, they are set to reasonable defaults (by default or by the SCO*office* Mail Server installation) and do not require modification. The SCO*office* Mail Server supports advanced Postscript configuration, but note the constraints on the following parameters:

`alias_maps`

> Specifies the list of alias databases used by the local delivery agent. For the SCO*office* Mail Server, this is defined to look up aliases stored in the LDAP directory. Normal Postfix alias files cannot be used with the SCO*office* Mail Server, because Postfix has been altered for the SCO*office* Mail Server to look up the entire address instead of just the local part. For example, if mail were to be sent to "*alias@foo.com*", the entire address "*aliasname@foo.com*" would be looked up in the aliases databases instead of just "*aliasname*". This is controlled by the postfix `domain_in_alias` parameter, which must be set to the value "yes" for correct operation of the SCO*office* Mail Server.

`bounce_notice_recipient`
`2bounce_notice_recipient`
`delay_notice_recipient`
`error_notice_recipient`

> Specify the recipient for *postmaster* notices for the various errors that Postfix can report, based upon the `notify_classes` parameter configuration. Although Postfix assigns a default value of "`postmaster`" to these parameters if they are not configured, these parameters must be explicitly set for the operation of the SCO*office* Mail Server. The **Server Manager** configures these parameters.

> > **Note:** We recommend that you not edit these parameters directly.

`fallback_transport`

> Specifies the optional transport agent to use for recipients that are not found in the Linux **passwd** database. The SCO*office* Mail Server sets this parameter to the Cyrus delivery agent, so that the local delivery agent first attempts to deliver mail to a Linux system account mailbox; if this fails, then it attempts to deliver mail via the Cyrus delivery agent to a SCO*office* Mail Server mail account. This also means that if a Linux account user and SCO*office* Mail Server mail account user are created with the same uid, then mail will always go to the Linux account user. See `mailbox_transport` parameter below for more information.

<div style="border:1px solid black">

Warning

Do not change the `fallback_transport` parameter; doing so might disable the mail server, and mail may fail to be delivered to SCO*office* Mail Server mail accounts.

</div>

`local_recipient_maps`

Specifies optional lookup tables that define all addresses for which the machine will accept mail with respect to the values of the `mydestination` and `inet_interfaces` parameters. If this parameter is defined, then the SMTP server will reject mail for any addresses not found in the databases specified in `local_recipient_maps`. The SCO*office* Mail Server sets this parameter to $alias_maps. To turn off this facility, comment out the `local_recipient_maps` parameter in the */etc/postfix/main.cf* configuration file.

`mailbox_transport`

This Postfix parameter specifies the optional transport in the *master.cf* file to use for local delivery after processing *aliases* and *.forward* files. Because this parameter has precedence over the `fallback_transport` parameter, it is not used by the SCO*office* Mail Server and should not be set manually.

<div style="border:1px solid black">

Warning

If you set this to the Cyrus delivery agent, mail will not be delivered to any Linux system accounts. If you set this to anything else, mail will fail to be delivered to SCO*office* Mail Server mail accounts.

</div>

`mydestination`

Specifies what domains the machine will accept mail for and deliver locally, instead of forwarding to another machine. The **Server Manager** updates this parameter automatically when you create a new mail domain.

Note: We recommend that you not edit this parameter directly.

For more information about the*/etc/postfix/main.cf* file, see "Postfix Configuration - Basics" in the *Wietse's Postfix Project* documentation.

Relocating the Postfix Message Queue

By default, Postfix is installed with its message queue in the directory */var/spool/postfix*. You can relocate the queue to a different filesystem, although we recommend that you do so before configuring the SCO*office* Mail Server and enabling mail delivery.

To relocate the Postfix message queue before the SCO*office* Mail Server is enabled:

1. Stop Postfix:

   /etc/rc.d/init.d/postfix stop

2. Set the `queue_directory` parameter in */etc/postfix/main.cf* to the new path for the queue and comment out the old path. For example:

   ```
   # relocated Postfix message queue for SCOoffice Mail Server use
   # queue_directory = /var/spool/postfix
   queue_directory = /new/location/postfix
   ```

3. Create the new directory for the Postfix message queue using the same directory name. For example:

   mkdir /new/location/postfix
   chown postfix:postfix /new/location/postfix
   chmod 755 /new/location/postfix

4. Start Postfix:

   /etc/rc.d/init.d/postfix start

Managing Large Messages and Attachments

Postfix includes built-in limits to the size of email messages and mailboxes. If either of these limits is exceeded, mail will not be delivered to the intended destination.

To control the size of email messages and mailboxes, you must set the parameters `message_size_limit` and `mailbox_size_limit` in the Postfix *main.cf* file to higher values. These parameters must be adjusted together; the value of `mailbox_size_limit` must be greater than or equal to the value of `message_size_limit`. When you have completed these adjustments, you must reload Postfix using the **Server Manager Mail Services** menu or using the **/etc/rc.d/init.d/postfix reload** command.

For more information about the */etc/postfix/main.cf* file, see "Postfix Configuration - Basics" in the *Wietse's Postfix Project* documentation.

Advanced Cyrus Configuration

This section discusses:

• Cyrus configuration parameters

• relocating the Cyrus message store

Cyrus Configuration Parameters

Cyrus configuration is controlled by parameters in the */etc/imapd.conf* file. Although there are around 100 parameters, they are set to reasonable defaults (by default or by SCO*office* Mail Server installation) and do not require modification. The SCO*office* Mail Server supports advanced Cyrus configuration, but note the constraints on the following parameters:

`admins`

Configures the list of user ids with administrative rights for Cyrus inboxes. For the SCO*office* Mail Server this is configured to include the administrative user "*admin*". This user is necessary for

proper operation of the SCO*office* Mail Server Manager; *do not* delete "*admin*" from the the
`admins` parameter.

`sasl_pwcheck_method`

Defines the mechanism used by the Cyrus IMAP and POP servers to verify plain text passwords.
For the SCO*office* Mail Server, this parameter is set to the value "`PAM`" to allow Cyrus servers to
authenticate via PAM (Pluggable Authentication Modules), which in turn is configured for these
servers to use LDAP authentication. *Do not change this parameter.*

For more information, see the *imapd.conf* (5) manual page.

Relocating the Cyrus Message Store

By default, Cyrus is installed with its message store in the directory */var/spool/imap*. You can relocate
the queue to a different filesystem, although we recommend that you do so before configuring the
SCO*office* Mail Server and enabling mail delivery.

To relocate the Cyrus message queue before the SCO*office* Mail Server is enabled:

1. Shut down the Cyrus master daemon to stop all IMAP/POP access:

   /etc/rc.d/init.d/cyrus stop

2. Stop Postfix to halt all email delivery:

   /etc/rc.d/init.d/postfix stop

3. Copy the existing message store to the new location. Using the **cp -p** flag will maintain the proper
   permissions and ownership of files and directories. For example:

   mkdir -p /new/location

   cp -pR /var/spool/imap /new/location/imap

4. If you are on an Open UNIX 8 system, go to the next step.

   On an OpenLinux system, set the **S** attribute on the new message store hierarchy. When the **S**
   attribute is set on Linux ext2fs file systems, changes are written synchronously to the disk (this is
   equivalent to the **sync** mount option applied to a subset of the files). For example:

```
chattr -R +S /new/location/imap
```

5. Set the `partition-default` parameter in */etc/imapd.conf* to the new path for the message store and comment out the old path. For example:

```
# relocated Cyrus message store for SCOoffice Mail Server use
# partition-default: /var/spool/imap
partition-default: /new/location/imap
```

6. Start Cyrus:

```
/etc/rc.d/init.d/cyrus start
```

7. Start Postfix:

```
/etc/rc.d/init.d/postfix start
```

Note: The */etc/pam.d/imap* and */etc/pam.d/pop* files define the PAM modules that will perform authentication for IMAP and POP services, respectively. For the SCO*office* Mail Server, these are set to use the LDAP PAM module and should not be altered.