



Scalix Administration Guide

Version 11

Revision 3

Scalix Administration Guide

Published by Scalix, Inc.
149 Madison Ave. Suite 302
New York, NY 10016
USA

Copyright © 2008 Scalix, Inc.
All rights reserved.

Product Version: 11
Document Revision: 2

Notice for Open-Source Software

Copyright (c) 1998-2007 The OpenSSL Project. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Notices

The information contained in this document is subject to change without notice.

Scalix Inc. makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Scalix Inc. shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

UNIX is a registered trademark of The Open Group.

Linux is a registered trademark of Linus Torvalds.

Red Hat is a registered trademark of Red Hat Software, Inc.

SUSE is a registered trademark of Novell, Inc.

Java is a registered trademark of Sun Microsystems, Inc.

Firefox is a registered trademark of the Mozilla Foundation.

Microsoft, Exchange, Outlook, Active Directory, PowerPoint, and Internet Explorer are registered trademarks or trademarks of Microsoft Corporation.

Lotus Notes is a registered trademark of Lotus Development Corporation.

All other company names, product names, service marks, fonts, and logos are trademarks or registered trademarks of their respective companies.

Restricted Rights Legend

Use, duplication, or disclosure is subject to restrictions as set forth in contract subdivision (c)(1)(ii) of the Rights in Technical Data and Computer Software clause 52.227-FAR14.

Contents

- Introduction to This Guide 9**
 - About This Guide 9
 - How to Use This Guide 9
 - Related Documents 10
 - Getting Help 10

- Introduction to Scalix 11**
 - Scalix System 11
 - Product Editions. 12
 - User Types 14

- Introduction to Scalix Management Console 15**
 - About Scalix Management Console. 15
 - Logging In 16
 - Navigating 18
 - Filtering 19
 - Logging Out 21

- Managing Basic Settings. 23**
 - Managing Licenses 23
 - Changing Settings Globally 25
 - Configuring General Settings. 26
 - Configuring Mailbox Settings. 30
 - Configuring Password Settings 33
 - Setting Default User Information 35
 - Changing the Number of User Accounts to Display. 36
 - Adding Mail Domains 37
 - Changing the general.cfg File 37

- Managing Mailnodes 39**
 - About Mailnodes 39
 - Viewing Mailnodes 40
 - Creating a Mailnode 41
 - Changing Address Format and Domain for Mailnode. 42
 - Changing a User’s Mailnode 43
 - Deleting User Accounts from a Mailnode 43
 - Deleting a Mailnode 44
 - Commands 44

Managing Administrator Access	45
About Administrator Roles and Permissions	45
Granting Full Scalix Administrator Access	46
Granting Scalix Admin Group Access	47
Granting Group Manager Access	49
Managing User Accounts.	51
About User Accounts	51
Adding a User Account	53
Changing Passwords	57
Modifying User Information	58
Changing User Account Types	59
Deleting User Accounts	60
Setting Mailbox Size Limits	61
Unlocking a User Account after Failed Login	62
Enabling Caching on Individual Mailboxes	62
Enabling Search Indexing	63
Identifying Delegates	64
Commands	64
Managing Groups	65
About Groups	65
Adding a Group / Mailing List	66
Viewing Users in a Group	69
Adding Users to a Group	69
Modifying a Group	70
Deleting a Group	71
Assigning Group Managers	71
Logging in as a Group Manager	72
Commands	73
Managing Resources	75
About Shared Resources	75
Setting Up a Shared Resource	76
Booking a Shared Resource	78
Changing Shared Resource Settings	79
Monitoring the Server	81
Introducing Server Info	81
Stopping and Starting Services	82
Using Logs	83

Monitoring the Active Users	84
Monitoring Disk Space	85
Monitoring Message Queues	86
Viewing Installed Components	87
Commands	87
Using Plug-ins	89
About Plug-ins	89
Viewing and Running Plug-ins	89
Writing Plug-ins	91
Deploying Plug-ins	93
Deployment Script Reference	94
Examples	95
Running Backups and Recovery	99
Strategies	99
Performing Full Backups	100
Performing Incremental Backups	108
Performing Export/Import Backups to Back Up Individual Mailboxes	109
Restoring the Full System	110
Restoring a Single User's Mailbox	111
Managing Public Folders	113
Public Folder Overview	113
Creating Public Folders	114
Listing Public Folders	115
Permissions for Public Folders	116
Maintaining Public Folders	119
Assigning E-mail Addresses to Public Folders	119
Synchronizing Public Folders	120
Forwarding Public Folder Items	124
Posting to Public Folders by E-mail	124
Commands	125
Using Access Control Lists	127
About Access Control Lists	127
Creating Access Control Lists	127
Commands	130
ACL Address Patterns	131
Combining Users and Permissions	133

Working with Scalix Directories	135
Directory Overview	135
Shared Directories	136
Commands	137
Listing Fields in the SYSTEM Directory	138
Creating a New Directory	139
Adding and Modifying a Directory Entry	139
Searching a Directory	139
Using the Client Directory Access Server	141
Handling Undeliverable Mail	143
Introduction	143
Creating a Redirect Account	144
Designating a User to Receive Non-Delivery Notice	144
Changing Hostname and IP Address	145
Introduction	145
Changing a Hostname	145
Changing an IP Address	146
Recovering Deleted Items	147
Introduction	147
Recovering Deleted Items	148
Changing the Default Hold Period	149
Disabling the Recovery Folder Feature	149
Emptying Recovery Folders	150
Setting Message Delivery Rules on the Router	151
About Message Delivery Rules	151
About the Service Router	151
Commands	152
Configuring Message Delivery Rules	153
Examples of Message Delivery Rules	161
Listing Deferred Mail and Forcing Delivery	164
Working with the Scalix Search and Index Service	165
Introduction	165
Document Types Handled	166
Creating Users' Indexes	166
Disabling Indexing	167
Re-Creating the Index	167

Localizing the Scalix Search and Index Service	168
Identifying an Individual Subdirectory (SIS URL)	168
Configuration Options	169
About Configuration Files	169
System-Wide Configuration Options	170
Client-Specific Configuration Options	223
User-Specific Configuration Options	234
Language-Specific Configuration Options	245
Command Line Reference	247
Introduction	247
Access Control List Commands	248
Audit Log Commands	249
Client Directory Access (CDA) Commands	249
Configuration and Installation Commands	250
Directory Commands	250
Directory Relay Server Commands	251
Directory Synchronization Commands	251
Error Manager Commands	251
Event Log Commands	252
Internet Address Commands	252
Internet Mail Gateway Commands	253
LDAP Commands	253
Mailbox Access Commands	254
Mailnode Commands	254
Message Store Commands	255
Miscellaneous Commands	256
Public Distribution List (Group) Commands	256
Public Folder Commands	257
Routing Table Commands	257
Service, Queue, and Daemon Commands	258
System Configuration and Maintenance Commands	259
User Account Commands	259

Introduction to This Guide

About This Guide

This guide outlines how to use Scalix as a Scalix Administrator. It explains how to add and manage user accounts, groups, calendars, contact lists, public folders, and so on. It provides instructions for maintenance, such as backups, and working with queues.

For configuration, such as anti-virus, multiple servers, or routing mail, see the *Scalix Setup and Configuration Guide*.

For information on setup of applications for end users, see the *Scalix Client Deployment Guide*.

How to Use This Guide

This guide uses the following typographical conventions.

Table 1: Conventions Used

Convention	Explanation
<Angle Brackets>	Values that you need to supply are sometimes shown using angle brackets. For example: <code>http://<server_name>/webmail</code>
Numbered and alphabetized lists versus bullets	Numbered and alphabetized lists denote steps to be followed while bullets provide information.
Buttons	The boldface font indicates a button, a link, a field, or other user interface element to click or press as well as a keyboard stroke. For example: Click Finish or type in the Username field.
Code	This smaller font indicates code to type or code that is returned as a response. For example: <code>./scalix-installer</code>
<i>Italics</i>	Indicates a document or section, a directory path, a file, or the name of a window. For example: Open the <i>/var/opt/scalix</i> folder. Or: The <i>Reply</i> screen appears.

Related Documents

Scalix manuals include:

- *Scalix Release Notes*
- *Scalix Installation Guide*
- *Scalix Migration Guide*
- *Scalix Setup and Configuration Guide*
- *Scalix Client Deployment Guide*
- *Scalix Administration Guide*
- *Scalix API Guide*

In addition, there are online help systems in:

- Scalix Management Console
- Scalix Web Access
- Microsoft Outlook (when enabled for the Scalix connector)

Getting Help

For help with installation, contact technical support at **support@scalix.com**

For the latest documents, see

<http://www.scalix.com/community/downloads/documentation.php>

For documents, a knowledge base, and forums, see

<http://www.scalix.com/community/resources/>

Introduction to Scalix

This chapter introduces Scalix, including editions and user types.

Contents

This chapter includes the following information:

- “Scalix System” on page 11
- “Product Editions” on page 12
- “User Types” on page 14

Scalix System

Scalix is software for e-mail, calendaring, and related groupware functions. It is installed onto computers with Linux operating systems and provides an alternative to Microsoft Exchange Server. It can also integrate into existing networks with Microsoft Exchange Server.

The Scalix architecture supports many e-mail clients and devices, without loss of functionality or data integrity. This means support for popular clients, such as Microsoft Outlook and Novell Evolution, as well as Internet Message Access Protocol (IMAP) and Post Office Protocol (POP) clients. End users enjoy advanced features, including:

- Calendaring
- Scheduling with real-time free/busy lookup
- Contact management
- Task management
- Public folders
- Access of e-mail in a Web browser (Webmail) and popular e-mail applications
- Resource booking, such as meeting rooms

Product Editions

There are three editions of Scalix.

Scalix Enterprise Edition – Ideal for companies that demand the full range of functionality in a commercial e-mail and calendaring system. It includes multiserver support, can have any number of Premium users, the full complement of Scalix advanced capabilities, and a variety of technical support options.

Scalix Small Business Edition – Functionally equivalent to Scalix Enterprise Edition except that it allows single-server installations only and does not include the capabilities for high availability and multi-instance support. For Scalix Small Business Edition 50, there are 50 Premium user licenses included. For Scalix Small Business Edition 20, there are 20 Premium user licenses included.

Scalix Community Edition – Free, single-server version of Scalix that is suitable for cost-conscious organizations that want an e-mail and calendaring system but do not require advanced groupware and collaboration functionality for their user population. It includes 10 Premium user licenses, which is the maximum possible, and an unlimited number of Standard users, a subset of Scalix functionality, and fee-based technical support.

The following table compares the editions.

Table 1: Features and Editions (version 11.3 example, subject to change)

Feature	Enterprise Edition	Small Business Edition 50 and 20	Community Edition
User Types			
Premium users	Min Purchase: 50 Max: Unlimited	Included: 50 or 20 Max: 250	Included: 10 Max: 10
Standard users	Free Max: Limits apply and can become unlimited with the purchase of a premium support package	Free Max: Limits apply and can become unlimited with the purchase of a premium support package	Free Max: Unlimited
Core Functionality			
E-mail and calendaring server	Multiserver	Single-server	Single-server
Internal user directory	✓	✓	✓
Choice of graphical interface or command-line interface	✓	✓	✓
IMAP/POP e-mail client access	✓	✓	✓
Web client (Scalix Web Access)	Group scheduling in calendar for Premium users	Group scheduling in calendar for Premium users (max 250)	Group scheduling in calendar for Premium users (max 10)
Microsoft Outlook support	Premium users	Premium users (max 250)	Premium users (max 10)

Table 1: Features and Editions (version 11.3 example, subject to change)

Feature	Enterprise Edition	Small Business Edition 50 and 20	Community Edition
Novell Evolution support	Group scheduling in calendar for Premium users	Group scheduling in calendar for Premium users (max 250)	Group scheduling in calendar for Premium users (max 10)
Public folders	Premium users	Premium users (max 250)	Premium users (max 10)
Recovery folders	Premium users	Premium users	Not available
High availability	✓	Not available	Not available
Multiple instances per server	✓	Not available	Not available
Migration tools	✓	✓	Not available
Upgrade to Scalix Enterprise Edition	Not applicable	With license key; re-installation not required	With license key; re-installation not required
Mobile access	✓	✓	✓
Ecosystem Support			
Meta-directory support via LDAP	✓	✓	✓
iCal and CalDAV support	✓	✓	✓
Microsoft Exchange Server interoperability and co-existence	✓	✓	Not available
Active Directory integration	✓	✓	Not available
Anti-virus	With flexible third-party interface	With flexible third-party interface	With flexible third-party interface
Anti-spam	With flexible third-party interface	With flexible third-party interface	With flexible third-party interface
Archiving	✓	✓	Not available
Wireless e-mail and personal information manager (PIM)	E-mail and PIM via Notify	E-mail and PIM via Notify	E-mail-only via POP/IMAP

User Types

There are three types of user accounts: Premium, Standard, and Internet Mail.

Premium Users

Premium users have access to the full functionality of Scalix. The following capabilities are available only to Premium users:

- Microsoft Outlook and Evolution support
- Group scheduling functionality, including free/busy lookup in Microsoft Outlook, Scalix Web Access, and Evolution clients
- Wireless e-mail and PIM
- Access to public folders
- Personal folder sharing
- Delegate access

Any number of Premium users can be licensed with Scalix Enterprise Edition. There are limits of 250 Premium users for Scalix Small Business Edition and 10 Premium users for Scalix Community Edition.

Standard Users

Access includes e-mail, personal calendar, and contacts through Scalix Web Access and Evolution as well as e-mail access using IMAP and POP clients. Use is ideal for cost-conscious organizations with users who do not have high-end groupware and collaboration requirements.

The maximum number varies with edition.

Internet Mail Users

An Internet Mail user account is an external e-mail account added to the Scalix database. It is not a Scalix user account; the user cannot run Scalix Web Access. You add such an account to have the e-mail account included in a group, for example, add it to the Sales group to include that address when mail is sent to your Sales group. And it can be selected when scheduling a meeting or sending an e-mail.

Flexible, Cost-Effective E-mail For Everyone

The distinction between Premium and Standard users provides the flexibility to cost-effectively provide e-mail for all users. For example, manufacturers and retailers can designate headquarters staff as Premium users because they require advanced groupware capabilities, while less demanding users, such as shop floor or store personnel, require Standard use with e-mail and personal calendaring capabilities. Similarly, educational institutions can decide that faculty and staff are Premium users while students are Standard users. The flexibility is at its best when there is a clear distinction between users, for example Premium users at one location and Standard users at another location who do not need the advanced features.

Introduction to Scalix Management Console

This chapter introduces the Scalix Management Console (SAC), including login, navigation, and filtering.

Contents

This chapter covers the following topics:

- “About Scalix Management Console” on page 15
- “Logging In” on page 16
- “Navigating” on page 18
- “Filtering” on page 19
- “Logging Out” on page 21

About Scalix Management Console

There are two main applications for Scalix: Scalix Management Console (SAC) for administrators and Scalix Web Access for end users. Scalix Management Console and the command-line interface are used to administer Scalix.

Scalix Management Console is a browser-based application. It is a separate component and can be accessed by a compatible Web browser on Microsoft Windows or Linux computers, for example. It provides access to all Scalix servers on a network through a single graphical user interface. This enables both single-server management and global changes with the ease of one centralized interface.

In contrast, the command-line interface manages one server at a time. It provides a full set of commands and allows the setup and running of administration scripts.

Once you have installed and configured your Scalix server, and migrated over existing user data, you can begin maintenance processes. Scalix Management Console enables a wide range of maintenance tasks, including:

- User account management
- Group management (public distribution lists)
- Management of shared resources, such as conference rooms, printers, and projectors
- Starting and stopping Scalix services and daemons
- Monitoring message queues
- Changing server configurations
- Monitoring the system processes, resources, and load

You can extend the console to perform customized tasks through the use of Management Plugins, which are scripts that perform repeated actions, such as checking load or disk usage and scanning logs.

Basic Process

You start on either of two tracks:

- If you migrated a lot of existing users (and their mail data) from a previous mail server, you need to perform the following basic tasks:
 - Add any new user accounts or groups
 - Edit any existing user accounts or groups
 - Check the status of Scalix services and queues, including a quick check of the main Message Store
 - Review and adjust a subset of Scalix settings
- Or, if you are setting up Scalix as a new server, you skip the step about editing existing user records. Adding user accounts is your primary work:
 - Add any new user accounts or groups
 - Check the status of Scalix services and queues
 - Review and adjust a subset of Scalix settings

Logging In

Because you access Scalix Management Console with a Web browser, almost any computer with an Internet connection can be used. For example, you can use a Windows or a Red Hat computer.

To log in to Scalix Management Console

- 1 Start a Web browser. Internet Explorer 6 and 7 and Firefox 2 are supported, and others are known to work.
- 2 Enter the address of the Scalix server and add a /sac extension:

```
http://<your_scalix_mailserver_FQDN>/sac
```

where you substitute the name and domain of your Scalix server for <your_scalix_mailserver_FQDN>. For example

```
http://scalix1.yourcompany.com/sac
```

If that does not work, try using the IP address of your Scalix server, for example

```
http://172.16.1.224/sac
```

where you substitute the IP address of your Scalix server for the one shown. If the IP address works but not the name and domain, it can mean that there is a problem with the Domain Name System (DNS) setup for your Scalix server. See the *Scalix Installation Guide*.

If that does not work, check if Apache is running by entering the IP address of your Scalix server, for example

```
http://172.16.1.224
```

or as root in a terminal window, enter on Red Hat Enterprise Linux

```
ps -ef | grep httpd
```

or on SUSE Linux

```
ps -ef | grep apache
```

With these commands, when Apache is running, it appears on the left side of the window, for example

```
apache 30896 30824 0 13:55 ? 00:00:00 /usr/sbin/httpd
apache 30897 30824 0 13:55 ? 00:00:00 /usr/sbin/httpd
```

If that does not work, try repairing the installation by doing a reconfiguration with the installation wizard. Use the *Scalix Installation Guide*.

With successful access, the login window appears.

- 3 In the login window, enter an administrator user ID and password. The default administrator account is sxadmin.



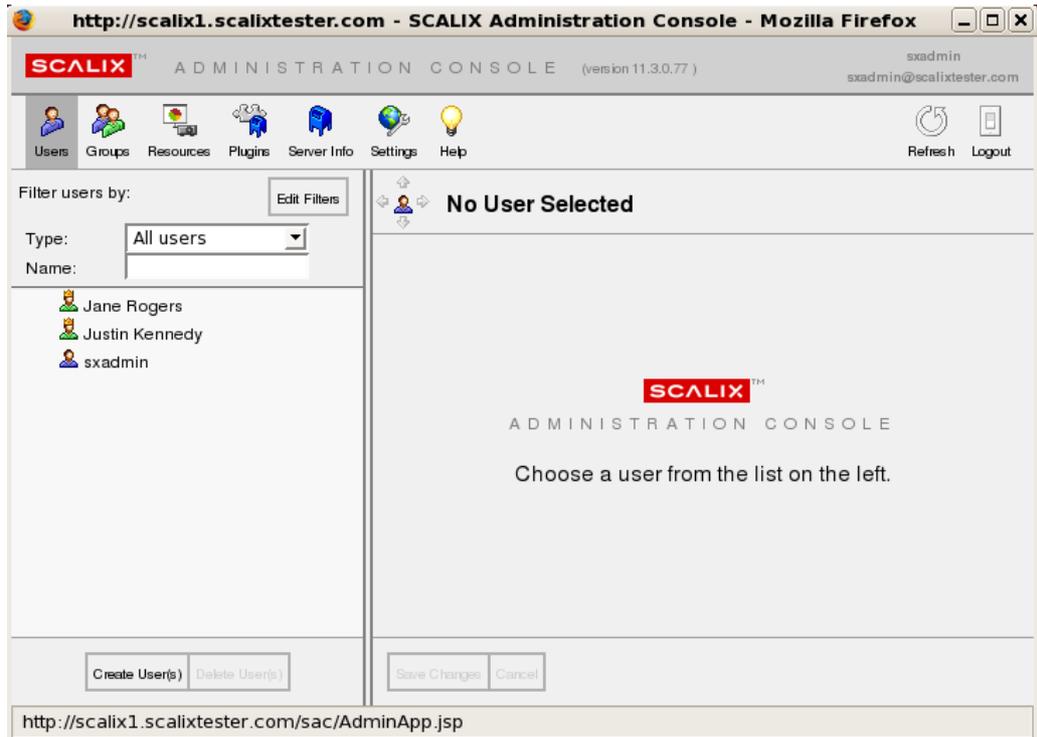
- a For the **Login ID** field, try the following formats:

```
sxadmin
Jane.Rogers@<your_scalix_mailserver_FQDN>
jane.rogers@scalix1.yourcompany.com
```

The format to use depends on the way the user account was set up in Scalix. You can view it for a user as the **Authentication ID** in the **Advanced** tab.

- b In the **Password** field, enter the password for the user account.
- c When Secure Sockets Layer (SSL) is not being used, enable the check box to be able to log in. The check box appears if the Apache server (part of the Scalix system) was not set up to support SSL.
- d Click **Login**.

With successful login, the Scalix Management Console window appears. The content varies by administrator and permissions.



Navigating

One feature that can be overlooked is the navigation button that allows you to go back or forward in the current panel or up or down in the pane on the left side.



Figure 1: Navigation Button

To use the navigation button

- 1 Click the up or down arrows to scroll through items in the contents pane to the left.
- 2 Click the left or right arrows (like a browser's Back or Forward buttons) to move to previous and next displayed items.

Filtering

When you have hundreds or thousands of Scalix user accounts and dozens of public distribution lists or servers to monitor, filtering can be used to help you locate items.

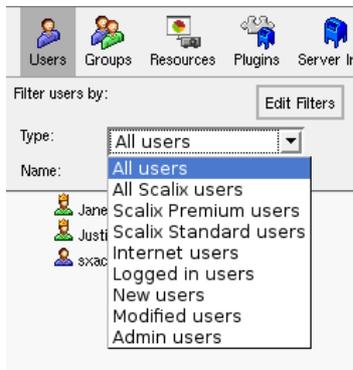
Scalix allows you to filter for user accounts, groups, and resources by two parameters:

- **Type** – From the drop-down list, you can filter for Premium user accounts, Standard user accounts, Internet users, logged in users, and administrators, for example. When in group or resource view, the selection changes accordingly.
- **Name** – Type in part of all of the name of the user, group, or resource that you want to find. Those matching the pattern you type in appear in the window.

You can use both filters at the same time.

To filter user accounts, groups, or resources

- 1 On the toolbar, select what you want to filter: **Users**, **Groups**, or **Resources**.
- 2 As the window begins to populate, filter by **Type** of user you want to view and/or type in part or all of the **Name** you want to find. The window filters dynamically as you type or select from the drop-down menu.



The filters for user accounts by **Type** are defined in the table.

Table 1: User Account Filters

Type	Description
All Users	Lists all user accounts in the system (the default).
All Scalix Users	Lists all Scalix user accounts, whether Premium or Standard.
Scalix Premium Users	Lists user accounts designated as Premium users. See the previous chapter for information about Premium users.
Scalix Standard Users	Lists user accounts designated as Standard users. See the previous chapter for information about Standard users. The default administrator account, sxadmin, is a Standard user, and this can be changed.
Internet Users	Lists all user accounts without local mailboxes, but whose address is included in the Scalix directory. All such non-Scalix users are labeled with a distinct icon.

Table 1: User Account Filters

Type	Description
Logged In Users	Lists all user accounts currently connected to Scalix, except the default sadmin account when logged in.
New Users	Lists all user accounts of any type added during this session.
Modified Users	Lists all user accounts modified during the current session.
Admin Users	Lists all “administration access” user accounts (no matter what their level of permissions), except the default sadmin account when logged in.

Adding Other Filters

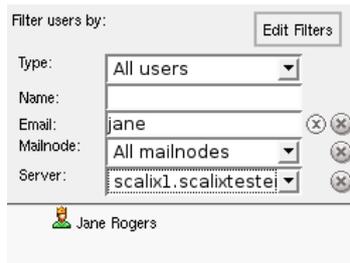
If the filters offered in the drop-down menu are not what you want, you can add others. An example is to search for all e-mail accounts starting with “jane” on the Scalix server called “scalix1.scalixtester.com”. In this example, you add the e-mail and server filter option.

To add and remove other filtering options

- 1 Click the **Edit Filters** button. A window appears.
- 2 Specify the filters in the window.



- a Enable the check box of the required filtering option:
 - **Email** – To enter the full address or the domain name to narrow the number of results that display
 - **Mailnode** – To enter the name of the node through which the user’s account is routed
 - **Server** – To enter the server on which the user’s account is located
- 3 Click **Set Filters**. This adds a search field to the main window.



- 4 To delete text from the field, click the small x that appears when you begin typing. To remove the filter, click the X on the right side of the field.

Logging Out

Although it is safe to log out of Scalix by simply quitting your browser, we recommend following the logout process to prevent problems.

To log out of Scalix Management Console

- 1 In the upper right-hand corner, click the **Logout** icon.



- 2 A confirmation window appears. Confirm the logout by clicking **Yes**. The Scalix Management Console connection is closed and the login window appears.

Managing Basic Settings

This chapter covers basic system settings performed through the Scalix Management Console. That includes license management, domain names, e-mail address format, mailbox size limits, out-of-office notice frequency, password configurations, and default user information such as country.

Contents

This chapter includes the following information:

- “Managing Licenses” on page 23
- “Changing Settings Globally” on page 25
- “Configuring General Settings” on page 26
- “Configuring Mailbox Settings” on page 30
- “Configuring Password Settings” on page 33
- “Setting Default User Information” on page 35
- “Changing the Number of User Accounts to Display” on page 36
- “Adding Mail Domains” on page 37
- “Changing the general.cfg File” on page 37

Managing Licenses

All editions except Scalix Community Edition require a license to use Scalix. The maximum number of Premium and Standard user accounts and other functionality are determined by the type of license, which varies by product edition and your purchase. For example, Scalix Enterprise Edition includes a minimum of 50 Premium user accounts, 20 or 50 for Scalix Small Business Edition, and 10 for Scalix Community Edition. For more information on product editions, user types, and functionality, see the chapter called “Introduction to Scalix” on page 11.

For Scalix Enterprise Edition and Scalix Small Business Edition, if you installed Scalix without a license key, your system installed as Scalix Community Edition and your user accounts as Standard until the correct license key is entered in Scalix Management Console.

At this time, verify in Scalix that you have a license, the number of Premium user accounts allowed, and expiry of the license. You can also upgrade the license, for example when you want to increase the number of users. Otherwise, if you do not have a valid license, frustration can result when features do not function as expected.

Licenses are generally delivered by e-mail, and you copy and paste the license into the installation wizard or Scalix Management Console.

When they expire, e-mail notification is sent to the default administrator account, for example sxadmin.

To view the license

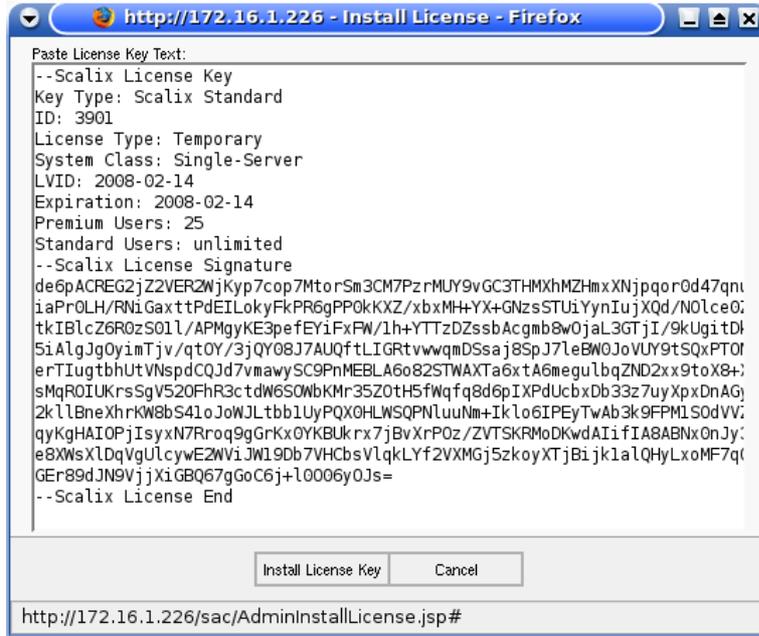
- 1 In Scalix Management Console, click the **Settings** icon on the toolbar.
- 2 Select the Scalix server by clicking the **Mail Server** entry on the left side.
- 3 Click the **License Keys** tab. The license displays, including single-server/multiserver capability, license expiry, and numbers of Premium and Standard user accounts allowed. If the window is blank, it means no license was entered during installation.

**Note**

Ensure licenses for all servers are the same across a Scalix system.

To import/install a license

- 1 Open the e-mail message containing the license key text.
- 2 Access the **License Keys** tab as outlined in the previous procedure.
- 3 In the lower right-hand corner, click **Install License Key**. A window appears.
- 4 Provide the license in the *Install License* window:
 - a Copy the entire license text from the e-mail, including "--Scalix License Key" at the beginning and "--Scalix License End" at the end.
 - b Right-click in the *Install License* window and paste the text.



- c Click **Install License Key**. The license is imported, and appears in the tab. This license remains in effect until upgraded, if needed.

Changing Settings Globally

When you have multiple Scalix servers, settings can be changed globally. This ensures consistency and saves time because you do not need to repeat tasks. This chapter outlines use of single-server changes, but you have the option of performing them at the global level. Simply select **Mail Servers** for global changes instead of an individual server entry.

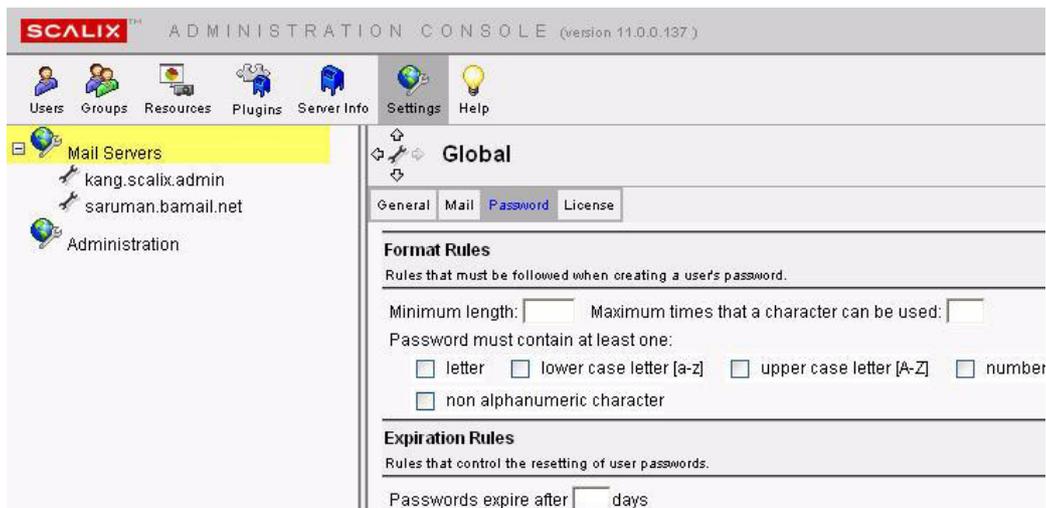


Figure 1: Option to Change All Servers when More than One being Used

If you first make changes to all servers globally, you can override server-specific settings by making individual modifications to a single server.

Configuring General Settings

The **General** tab in Scalix Management Console enables configuration of domain name, user name display, authentication IDs, SmartCache, and e-mail address format. These are outlined here.

Changing the Server Domain Name

Two domains can be specified: a domain for authenticating administrator login, and a domain for e-mail addresses. By default the same domain is used for both.

For example, when the domain name is “scalixtester.com”, an administrator logs in with a scalixtester.com user account and the e-mail address can be Firstname.Lastname@scalixtester.com

You can change the domains. For example, you can specify that any new administrator accounts log in with a scalixtest.com server domain and the e-mail domain instead is scalixtester.com. The change applies to access of Scalix Management Console.

Scalix allows two types of address generation rules:

- Global (system-wide) address-generation rules
- Mailnode-specific address generation rules (there is more on mailnodes in “Managing Mailnodes” on page 39).

Scalix stores up to five global address-generation rules, but only one mailnode address-generation rule, which overrides any global rules currently in use.

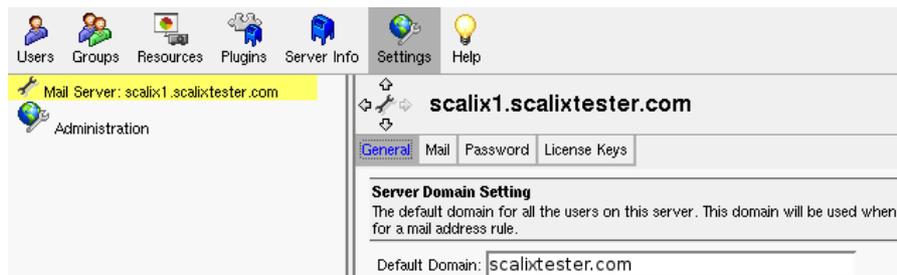


Figure 2: Domain Used for the Server is scalixtester.com

To change server domain settings for new user accounts

- 1 In Scalix Management Console, click the **Settings** icon on the toolbar.
- 2 Select the server on the left side of the window under **Mail Server**.
- 3 Click the **General** tab.
- 4 In the **Default Domain** field, type the name of the domain to use for the server.
- 5 At the bottom of window, click the **Save Changes** button. For the example provided, where the server domain is changed to scalixtest.com and the e-mail address domain remains scalixtester.com, when you create a new administrator account then only access to Scalix Management Console changes:

Scalix Management Console = http://scalix1.scalixtester.com/sac

Login = Janet.Smith@scalixtest.com

Scalix Web Access = http://scalix1.scalixtester.com/webmail

Login = Janet.Smith@scalixtester.com or Janet.Smith@scalixtest.com

E-mail = Janet.Smith@scalixtester.com

Setting User Name and Authentication ID Formats

You can modify the rules that control how a new user's name is formatted, both as a display name on e-mail messages and as an authentication ID, which can be used to log in to the system. The display name and authentication ID both take from the user's name (first and last and, optionally, middle initial) in different formats that can be customized.

There are three settings that you can change:

- **Display Name Rule** – The “friendly” name that displays for the user account in Scalix and on e-mails. This is not the e-mail address.
- **Authentication ID Rule** – The name or identification used to log in to the system
- **No Domain On Authentication ID Rule** – Determines whether the user must enter the full domain name to log in or just their user account name

The screenshot shows the 'User Name Settings' section with the following configuration: Display Name Rule set to 'First Last', Authentication ID Rule set to 'First.Last', and the 'No Domain On Authentication ID' checkbox checked. Below this is the 'SmartCache Control Settings' section with the 'Enable SmartCache' checkbox checked. The 'Mail Address Settings' section shows a Mail Address Rule of 'First.Last' and a Mail Address Domain of 'scalixtester.com'. An 'Add Rule' button is visible in the top right of the Mail Address Settings section.

Figure 3: Changing How New User Accounts Display and Authenticate

Example:

Display Name Rule = Last First

Authentication ID Rule = Last.First and No Domain on Authentication ID

Mail Address Rule = First.Last

New administrator Janet Smith's display in Scalix = Smith Janet

Use authentication ID rule to log in to Scalix Management Console = Smith.Janet

Use it or e-mail address to log in to Scalix Web Access = Smith.Janet or Janet.Smith@scalixtester.com

Name as displayed to the user in Scalix Web Access = Smith Janet

Name displayed to others when the user sends mail = From: Smith Janet <Janet.Smith@scalixtester.com>

To change user name and authentication settings for new user accounts

- 1 In Scalix Management Console, click the **Settings** icon on the toolbar.
- 2 Select the server on the left side of the window under **Mail Server**.
- 3 Click the **General** tab.
- 4 Change the settings:

Display Name Rule – Select the preferred user name format. For example, Last First displays the name in Scalix and Scalix Web Access in that format.

Authentication ID Rule – Select the preferred authentication ID format. For example, Last.First requires that user access in Scalix Web Access and Scalix Management Console use that format.

No Domain On Authentication ID – Enable the check box to allow the user to log in without specifying the domain. Disable the check box to require login with the full domain name. For example, when no domain is required, the user uses the Last.First format to log in instead of Last.First@yourdomain.com. When the domain is required, it must be specified here in Scalix.

- 5 At the bottom of the window, click **Save Changes**.

Alert

If you want full domain names used in authentication IDs, be sure to communicate to new users that they must update their client account settings accordingly.

Note

If users' names do not appear the way you want in mail being sent, set `UXO_OVERRIDE_FRIENDLY_NAMES=TRUE` in the `/var/opt/scalix/<nn>/s/sys/general.cfg` file and restart the Internet mail gateway. This overrides user settings and allows you to set the format corporate-wide for the friendly name. For example, a user with an e-mail address `d.smith@yourcompany.com` displays a friendly name of Donald Smith. The change applies to all user accounts, not just new ones.

You can also set the company name to be the Common Name (instead of friendly names like Donald Smith) by setting it in the CN attribute using the `ommodent` command.

Controlling SmartCache Use for User Accounts

To improve the speed and responsiveness of e-mail service in Microsoft Outlook, use the Scalix SmartCache feature. This creates copies of all users' mailboxes on their client computers as well as on the server, allowing them to work from files on the local computer, speeding up performance and preserving bandwidth.

With SmartCache, the system checks the server only when sending and receiving new messages, meaning fewer trips to and from the sever.

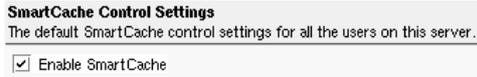
SmartCache applies only to Premium user accounts, which can use Microsoft Outlook.

SmartCache is enabled by default in Scalix.

The server-wide setting done here can be overridden on a user-by-user basis. In addition, there are different ways to prepare a user's mailbox for caching. Please note that the server-wide setting is not global; if you disable SmartCache use and create a Premium user account, the account is enabled for SmartCache. The setting outlined here determines what happens for the end-user; if you disable SmartCache, it is disabled by default for the user in Microsoft Outlook but they can still enable it in the user profile.

To enable or disable SmartCache use for user accounts

- 1 In Scalix Management Console, click the **Settings** icon on the toolbar.
- 2 Select the server on the left side of the window under **Mail Server**.
- 3 Click the **General** tab.
- 4 Enable or disable the **Enable SmartCache** check box.



- 5 At the bottom of the window, click **Save Changes**. This server setting only affects the default setting of SmartCache on the client side (Microsoft Outlook), and it can be changed by the end user.

Note

If you disable the SmartCache feature and create a Premium user account, that user account is automatically enabled for SmartCache use. You can disable it at the user account level.

Setting E-mail Address Formats and Domains

The format used for e-mail addresses can be changed, and e-mail domains can be added. For example, you can set it so that new user accounts have the format First.Last, for example Jane.Blackwell@scalixtester.com. One e-mail domain is used by default, and you can create up to five rules to add up to five domains. For example, you currently use the mail address domain of scalixtester.com and you add a rule for scalixtest.com. When you create a new user account, it can be set to receive mail for both scalixtester.com and scalixtest.com. You need to have a Scalix license for each domain, so do not add a rule for an unlicensed domain.

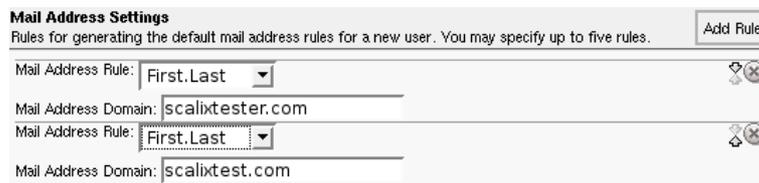


Figure 4: Adding an E-mail Domain for New User Accounts

To set e-mail address formats and domains for new user accounts

- 1 In Scalix Management Console, click the **Settings** icon.
- 2 Select the server on the left side of the window under **Mail Server**.
- 3 Click the **General** tab.
- 4 Change an existing e-mail format and domain:
 - Mail Address Rule** – To change the format for e-mail addresses
 - Mail Address Domain** – The domain to use for the e-mail address, for example yourcompany.com. Do not add domains for which you do not have Scalix licenses.
- 5 Create a rule by clicking **Add Rule** and providing the information, after which the rule is added to the window.

- 6 At the bottom of the window, click **Save Changes**. The change is applied and any new rule is added. When you create a new user account, the changes and any new rules are applied. As shown here, two e-mail domains apply to the user. You can use these alternate mail addresses to create or modify user accounts.

Note

If users' names do not appear the way you want in mail being sent, set `UXO_OVERRIDE_FRIENDLY_NAMES=TRUE` in the `/var/opt/scalix/<nn>/s/sys/general.cfg` file and restart the Internet mail gateway. This overrides user settings and allows you to set the format corporate-wide for the friendly name. For example, a user with an e-mail address `d.smith@yourcompany.com` displays a friendly name of Donald Smith. The change applies to all user accounts, not just new ones.

You can also set the company name to be the Common Name (instead of friendly names like Donald Smith) by setting it in the CN attribute using the `ommodent` command.

Configuring Mailbox Settings

Mailbox size limits, warnings, and out-of-office notification frequency can be set. There is no size limit by default, and you want to set it when you have limited storage capacity or when a few users take most of the space, for example. Because there is no limit on size by default, there are also no warning messages generated by default. There is no frequency specified by default to limit the frequency of out-of-office notifications.

If needed, you can override these system settings on an individual mailbox level.

Setting Mailbox Size and Warning Messages

You can limit the amount of disk space used by user e-mail and configure warning messages. First, you can check the space consumed on the disk and by each user, as a way to guide your decision on what to set the mailbox limit to.

To check mailbox space being used

- 1 In Scalix Management Console, click the **Server Info** icon on the toolbar.
- 2 Select the server on the left side of the window under **Mail Server**.
- 3 Click the **Storage** tab. Used and free space are displayed, as well as mailbox space used by each user.



To set capacity limits on all mailboxes on the system

- 1 In Scalix Management Console, click the **Settings** icon on the toolbar.
- 2 Select the server on the left side of the window under **Mail Server**.
- 3 Click the **Mail** tab.
- 4 Change the settings:

Maximum Mailbox Size – Specify the maximum amount of space, in MB, that a user’s e-mail can take in Scalix. Typical values are 100 MB to 1 GB (1000 MB), for example allow each user 200 MB for mail. Leave the field blank when there is no limit.

Send warning on outgoing mail...and reject when over the limit – Enable the check box to send a message to a user when their mailbox is near the limit when they send an e-mail, and do not send the outgoing e-mail when the mailbox exceeds the limit. Disable the check box if you do not want a message to be sent to the user and to send the outgoing e-mail anyway.

Warning Percentage – When the **Send warning...** check box is enabled, specify the level at which messages are to be sent. For example, send a message to the user when their mailbox is 90 percent full.

Reject Percentage – When the **Send warning...** check box is enabled, specify the level at which messages are not to be sent. For example, do not send an outgoing e-mail when the user mailbox is 95 percent full.

Warning Text – When the **Send warning...** check box is enabled, specify the message to send to the user. For example, “Your mailbox is almost full. When your mailbox is full, outgoing e-mail will be rejected. Please delete some messages.”

Reject incoming mail when over the limit – When a user’s mailbox is full, do not accept new mail addressed to the user

Send mail to user when over the limit – When a user’s mailbox is full, accept new mail addressed to the user

Send warnings every x days – Specify how often to send the warning message to the user when limits are triggered by outgoing mail. For example, send the message every second day instead of each time.

General	Mail	Password	License Keys
Mailbox Limits			
Set the limit on the size of a user's mailbox. Also set the sanctions that are imposed when the limit is exceeded.			
Maximum Mailbox Size:		500	MB (A blank value indicates unlimited size of mail boxes)
<input checked="" type="checkbox"/> Send warning on outgoing mail when near limit; reject outgoing mail when over the limit.			
Warning Percentage:		90	%
Reject Percentage:		95	%
Warning Text:		Mailbox full! Delete some messages.	
<input type="checkbox"/> Reject incoming mail when over the limit.			
<input checked="" type="checkbox"/> Send mail to user when over the limit.			
Send warnings every		1	days.

- At the bottom of the window, click **Save Changes**.

Note You can set Inbox and Outbox limits. Use the UAL_INTRAY_SIZE_LIMIT and UAL_OUTTRAY_SIZE_LIMIT options as outlined in the “Configuration Options” chapter.

Limiting Out-of-Office Replies

To avoid inundating recipients with out-of-office replies, limit the number of replies sent during a given period. You can set the system to send only one out-of-office reply per day, or every other day, or any other number of days. For example, if someone sends five e-mails on the first day a user is on vacation, they receive only one out-of-office reply.

To limit out-of-office replies

- In Scalix Management Console, click the **Settings** icon on the toolbar.
- Select the server on the left side of the window under **Mail Server**.
- Click the **Mail** tab.
- Specify the interval between messages in the **Send out-of-office message every x days** box, for example every 1 day. Leave the box blank to have a message sent each time.
- At the bottom of the window, click **Save Changes**.

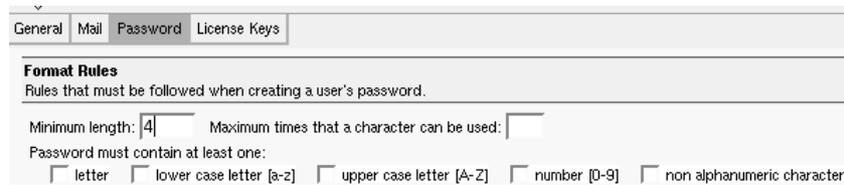
Note This setting corresponds to the LD_AUTOREPLY_EXPIRY_TIME option in the general.cfg file. You can also, or instead, limit the number of replies by setting LD_AUTOREPLY_CHECK_ON=TRUE in the general.cfg file so that only one automatic reply is sent to each unique sender address.

Configuring Password Settings

Password variables include the minimum number of characters required, the type of characters, repeat use of passwords, expiry, and maximum number of failed login tries before the system blocks further attempts by the same user.

Setting Password Formats

Password format rules include the minimum length of passwords, the maximum number of times any one character can be used, and the types of characters. For example, you can require that passwords have both lower case and upper case letters as well as numbers.



The screenshot shows a web interface with tabs for 'General', 'Mail', 'Password', and 'License Keys'. The 'Password' tab is active. Under the heading 'Format Rules', there is a sub-heading 'Rules that must be followed when creating a user's password.' Below this, there are two input fields: 'Minimum length:' with the value '4' and 'Maximum times that a character can be used:' with an empty field. Underneath, there is a section 'Password must contain at least one:' followed by five checkboxes: 'letter', 'lower case letter [a-z]', 'upper case letter [A-Z]', 'number [0-9]', and 'non alphanumeric character'. All checkboxes are currently unchecked.

Figure 5: Setting a Minimum Password Length of Four Characters

To set password format rules

- 1 In Scalix Management Console, click the **Settings** icon on the toolbar.
- 2 Select the server on the left side of the window under **Mail Server**.
- 3 Click the **Password** tab.
- 4 Under the **Format Rules** options, fill in the fields, including:
 - Enter a minimum number of characters, letters, or numbers
 - Enter the number of times a character can be repeated, if at all
 - Check all the character-inclusion options to be applied
- 5 At the bottom of the window, click **Save Changes**.

Note

You can also view password defaults using the `omshowpwd` command.

Setting Password Expiry and Repeat Use

Password expiry rules establish the number of days after which passwords expire, and the number of days and times after which users can re-use old passwords.



The screenshot shows a web interface with the heading 'Expiration Rules' and a sub-heading 'Rules that control the resetting of user passwords.' Below this, there are three input fields: 'Passwords expire after' with the value '365' and the unit 'days', 'Can repeat the same password after' with an empty field and the unit 'times', and 'Can repeat the same password after' with an empty field and the unit 'days'.

Figure 6: Setting Passwords to Expire After a Year

To set password expiry rules

- 1 Access the **Password** tab as outlined in the previous section.
- 2 Set the expiry rules:
 - **Passwords expire after x days** – The time period (in days) before passwords automatically expire
 - **Can repeat the same password after x times** – The number of times after which a user can re-use an old password
 - **Can repeat the same password after x days** – The number of days after which a user can re-use the same password
- 3 At the bottom of the window, click **Save Changes**.

Note

You can view password defaults using the `omshowpwd` command.

You can also set password rules directly in the configuration files; see the “Configuration Options” chapter.

Blocking Login Attempts After Failure

You can set the number of failed login tries to trigger user account rejection. Upon rejection, the user can be warned that they must wait a set period of time before trying again. In some cases, no such warning is given and they see a message about the user account and password being incorrect even when they are correct.

The default is to specify no number, meaning that the user can try as many incorrect logins and not be blocked.

To set login rules

- 1 In Scalix Management Console, click the **Settings** icon on the toolbar.
- 2 Select the server on the left side of the window under **Mail Server**.
- 3 Click the **Password** tab.
- 4 In the **Maximum number of login tries**, specify the threshold, for example 5. If a user tries to log in and is unsuccessful five times, they are unable to log in. The account is locked, and the Scalix administrator needs to remove the threshold or unlock the user account (under **Users > Advanced** tab).
- 5 At the bottom of the window, click **Save Changes**.

Alert

If a user exceeds the maximum number of login tries, they are locked out of the system. This requires that they contact the system administrator and request that their mailbox be unlocked as outlined in “Unlocking a User Account after Failed Login” on page 62.

Setting Default User Information

You can specify some information to use when creating new user accounts, such as company name, city, and country. If your user base is restricted to a distinct office or area, these options pre-load user information, saving time and effort later in data entry. You can set the fields to pre-populate with the information that is common to most of your users, and allow the others to overwrite as needed.

These settings do not affect existing user accounts or those created outside the Scalix system. They apply to new user accounts.

To set default user information for new user accounts

- 1 In Scalix Management Console, click the **Settings** icon on the toolbar.
- 2 Click **Administration** on the left side of the window.
- 3 Under the **Default User Information Settings** option, set the values:

Company – The name of your company or organization, such as Xandros Inc.

City – The location of the users for new user accounts, for example Paris or Honolulu

State/Province – The state, canton, province, and so on to use for new user accounts. Specify the country first because the State/Province field changes accordingly.

Zip/Postal Code – The mailing zip or postal code, for example 90210 or K2P 0W8. Specify the country first because this field can display as invalid otherwise.

Country – Select the country to use for new user accounts

Language – Select the default language of the new users. Options include English and German. Setting this field does not set the language of Scalix Web Access for the users. It merely records what language they speak.

- At the bottom of the window, click **Save Changes**. New user accounts reflect the information in the **Contact Info** tab.

The screenshot displays the Scalix Administration interface. On the left, the 'Administration' sidebar is open to 'General' settings. The 'Default User Information Settings' section shows fields for Company (Mahi Boat Cruises), City (Honolulu), State/Province (Hawaii), Zip/Postal Code (90210), Country (United States), and Language (English (American)). On the right, the user profile for 'Johnnie Kameamea' is shown with the 'Contact Info' tab selected. This section contains fields for Company, Department, Office, Title, Street, City (Honolulu), State/Province (Hawaii), Zip/Postal Code (90210), Country (United States), and Language (English (American)). There are also fields for Work Phone, Work Phone 2, Home Phone, Home Phone 2, Mobile Phone, Fax, Pager, and Notes.

Changing the Number of User Accounts to Display

The default is to display 100 user accounts or groups in Scalix Management Console, and you can change this value. When the number of entries exceeds the threshold, you see “Incomplete List” displayed. Note that increasing the value slows down the loading speed of records in Scalix Management Console.



Figure 7: “Incomplete List” Means Not All Records Displayed

To change the number of user accounts or groups displayed

- In Scalix Management Console, click the **Settings** icon on the toolbar.
- Click **Administration** on the left side.
- Change the **Maximum number of items** field, or delete the value displayed to show all records.
- At the bottom of the window, click **Save Changes**.
- Click the **Users** or **Groups** icon on the toolbar.
- Click **Refresh** at the top right of the window. The display changes to reflect the setting.

Adding Mail Domains

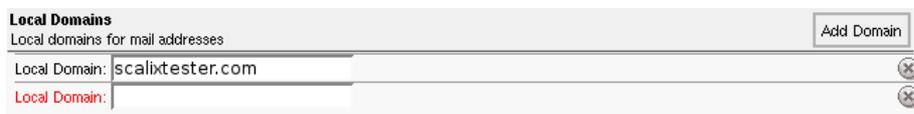
You can add local domains for use in managing your user base, provided your Scalix license incorporates them.

Alert

If you want to add a domain that is not within the terms of your license, you have to get a new license or upgrade the current one.

To add local domains

- 1 In Scalix Management Console, click the **Settings** icon on the toolbar.
- 2 Click **Administration** on the left side.
- 3 Under the Local Domains options, click **Add Domain**. A new, blank row appears.



- 4 Type the domain.
- 5 At the bottom of the window, click **Save Changes**. The domain is now available when creating a new user account and when modifying a user account.

Changing the *general.cfg* File

Modifying settings in the *general.cfg* file can be done through the command-line interface or in a text editor at the Scalix server. The file is in the following location:

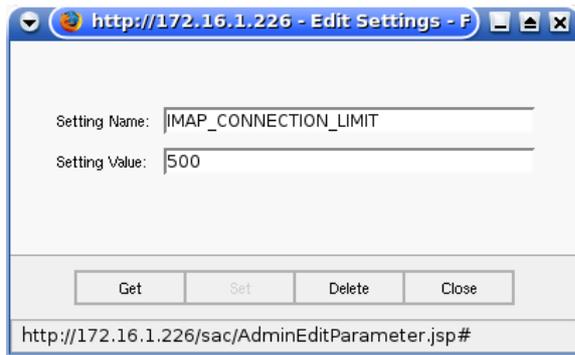
```
/var/opt/scalix/<nn>/s/sys/general.cfg
```

where nn varies with Scalix installation. You also have the option to use Scalix Management Console to modify the settings while sitting at another computer. You need to know the name of the setting to change, for example IMAP_CONNECTION_LIMIT, which is the maximum number of concurrent IMAP connections allowed. The *general.cfg* file and the parameters are explained in the chapter titled, “Configuration Options” on page 169.

To change the *general.cfg* file with Scalix Management Console

- 1 In Scalix Management Console, click the **Settings** icon on the toolbar.
- 2 Select the server on the left side of the window under **Mail Server**.
- 3 In the **General** tab, click the **Edit Settings** button in the lower right corner.

- 4 In the *Edit Settings* window that appears, change or create settings.



- a In the **Setting Name** field, enter the variable name, for example IMAP_CONNECTION_LIMIT. The field is case-sensitive.
- b Click **Get**. The default value, when found, displays in the **Setting Value** field as a whole number or a text entry, such as TRUE or FALSE, BEFORE or AFTER, and so on.

If the configuration does not exist or if the text was entered incorrectly, Scalix displays the following message:
No value found for this setting. You may type in a value and click 'Set' to store it.
- c To change the value or add a new record, enter the value in the **Setting Value** field and click **Set**.

Managing Mailnodes

This chapter covers mailnodes, a unique Scalix option that organizes an e-mail user base. It explains how to view, create, modify, and delete mailnodes, as well as how to move user accounts from one mailnode to another.

Contents

This chapter includes the following information:

- “About Mailnodes” on page 39
- “Viewing Mailnodes” on page 40
- “Creating a Mailnode” on page 41
- “Changing Address Format and Domain for Mailnode” on page 42
- “Changing a User’s Mailnode” on page 43
- “Deleting User Accounts from a Mailnode” on page 43
- “Deleting a Mailnode” on page 44
- “Commands” on page 44

About Mailnodes

A mailnode is like a mail stop. Mailnodes organize mail user communities into manageable groups, such as by department, employment status, or office location. Each Scalix server is associated with a mailnode, which was created during installation, and you can create additional mailnodes in Scalix Management Console, including those with a different Internet address and domain name.

Once you create the needed mailnodes, you can do the following, depending on your e-mail user base:

- If starting out with a new system and adding all user accounts at this time, you can sort your new users into any mailnodes as you work
- If you already have an established user base, you cannot sort the existing user records into new mailnodes (in Scalix Management Console), but you can sort all newly added users into mailnodes

In addition, there are other mailnode functions:

- Change a mailnode’s address
- Review the list of users associated with a mailnode
- Review the groups associated with a mailnode

Note that once a user is associated with a mailnode, you cannot move or reassign them in Scalix Management Console. This is done on the Scalix command-line interface instead because it requires migrating the user and mail data from one mailnode to another.

Viewing Mailnodes

You can check existing mailnode settings.

To view the status of a mailnode

- 1 In Scalix Management Console, click the **Server Info** icon on the toolbar.
- 2 At the left side of the window is the server (blue postal mailbox) and one or more mailnodes (gray bin). Click the mailnode.



Mailnode options appear in the window in four tabs:

General – Default

Users – To view all user accounts assigned to a mailnode. To see information about any individual user, click the name.

Groups – To see all groups assigned to a mailnode. To see information about any individual group, click its name.

Resources – To see all resources assigned to a mailnode. To see information about any individual resource, click its name.

Note

You can also view mailnodes by selecting the server on the left side of the window, then the Mailnodes tab.

Creating a Mailnode

You can create additional mailnodes on a server, including customizing new nodes with specific Internet addresses and domain names. For example, you can split user accounts into TorontoWest, TorontoCentral, and TorontoEast mailnodes.

Please note that you then need to move users among mailnodes using commands.

To create a mailnode

- 1 In the toolbar, click the **Server Info** button.
- 2 Select the server at the left side of the window. The server is represented by a blue postal mailbox.
- 3 Click the **Mailnodes** tab. Existing mailnodes are listed.
- 4 Click **Add Mailnode** in the lower right corner. An *Add Mailnode* window appears.

- 5 In the *Add Mailnode* window, add it.
 - a Configure the new mailnode:
 - Mailnode name** – Enter a single-word name/title for this new node, for example OttawaEast or UKOffice
 - Mail Address Rule** – Select the mail address format, for example First.Last
 - Mail Address Domain** – Enter the domain information, for example the existing domain or a new one. The format is <your_scalix_mailserver_FQDN>, for example scalix1.scalixtester.com
 - b Click **Finish**. The mailnode is added to the server and appears in the list. When you add a new user account or group, you can assign the mailnode to the new account. To move an existing user account to the mailnode, you need to use the command-line interface; see “Changing a User’s Mailnode” on page 43.

Changing Address Format and Domain for Mailnode

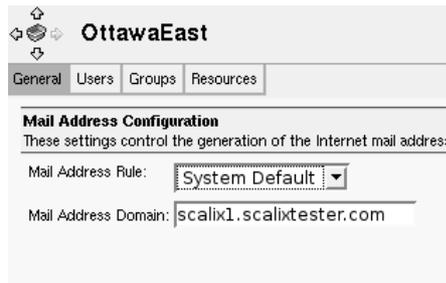
You can customize mailnodes to use specific Internet addresses and domain names.

If you create an e-mail address-generation rule on a mailnode, and if a user is associated with that selected mailnode, then his/her address is generated not by global rules, but by the mailnode-specific rule.

Note Domains can be entered/used only when included in your Scalix license.

To change mailnode configurations

- 1 In Scalix Management Console, click the **Server Info** icon on the toolbar.
- 2 Select the mailnode at the left side of the window.
- 3 Click the **General** tab.
- 4 Change the configuration:
 - Mail Address Rule** – Select the format to use for new e-mail addresses created, for example First.Last
 - Mail Address Domain** – To change the existing domain (or assign one to this node), type the domain in the field. The format is <your_scalix_mailserver_FQDN>, for example scalix1.scalixtester.com



- 5 At the bottom of the window, click **Save Changes**. Existing user accounts and groups are unaffected.

Changing a User's Mailnode

You can move a user account from one mailnode to another, for example from the mailnode OttawaEast to OttawaWest. The command-line interface is used.

To change a user's mailnode

- 1 Run the `ommodu` command on the user account, for example

```
ommodu -o "Florian User/old,mailnode" -n "Florian User/new,mailnode"
```

If your users have old internal e-mail in their mailboxes, they can become unrepliable because the old mailnode is stored as part of the FROM addresses in the messages. You can work around this by adding a line reading `SR_RESOLVE_MASK=4` to your `/var/opt/scalix/sys/general.cfg` file and restarting the service router. This tries to look up recipient addresses using the “first four” attributes in the X.400-style Scalix address, meaning the G, I, S, and Q (Given Name, Middle Initials, Surname, Generation Qualifier) attributes.

Note

The command to change a distribution list mailnode is `ommodpdl`.

Deleting User Accounts from a Mailnode

You can delete individual user accounts from a mailnode or all user accounts from a mailnode. The user accounts are deleted, including their mail.

To delete user accounts from a mailnode

- 1 In Scalix Management Console, click the **Server Info** button.
- 2 Select the mailnode on the left side of the window.
- 3 Click the **Users** tab.
- 4 To delete an individual user account, click its X at the right side of the window. To delete all user accounts, click **Delete Listed Users**.
- 5 Confirm the deletion.
- 6 Click the **Users** icon on the toolbar.
- 7 Click the **Refresh** button. The user accounts disappear from the list and a message displays to this effect.

Alert

Deleting users from a mailnode deletes the user accounts, which means you remove the record and all related mail and scheduling archives.

Note

You can delete groups from a mailnode in the Groups tab.

Deleting a Mailnode

Mailnodes can be deleted.

To delete a mailnode

- 1 In Scalix Management Console, reassign any users or groups using the mailnode to other mailnodes. First, view the user accounts and groups affected by selecting the mailnode in the **Server Info** window. Second, reassign the user accounts and groups. If you instead delete the user accounts or groups from the mailnode, you delete the user accounts from Scalix and all associated mail.
- 2 Now, delete the mailnode. Click the **Server Info** icon on the toolbar.
- 3 Select the server on the left side of the window.
- 4 Click the **Mailnode** tab.
- 5 Click the X at the right side of the window for the mailnode that you want to delete.
- 6 Confirm the deletion. If there are users or groups still assigned to the mailnode, you are prompted to change them and cannot delete the mailnode.

Commands

Mailnode commands are listed in the table. See also “Directory Relay Server Commands” on page 251 and “Internet Address Commands” on page 252.

Table 1: Mailnode Commands

Command	Description
omaddmn	Add a mailnode.
omdelmn	Delete one or more mailnodes.
ommodmn	Modify a mailnode.
omshowmn	List local mailnodes.

Managing Administrator Access

This chapter explains the different levels of administrative access to Scalix Management Console: levels of access, how to grant them, and when to use them.

Contents

This chapter includes the following information:

- “About Administrator Roles and Permissions” on page 45
- “Granting Full Scalix Administrator Access” on page 46
- “Granting Scalix Admin Group Access” on page 47
- “Granting Group Manager Access” on page 49

About Administrator Roles and Permissions

There are four administrative roles:

- **Root** – User cannot access Scalix Management Console but can run commands on the command-line interface for all computers in a Scalix network. The user cannot log in to Scalix Management Console because he/she is not a Scalix user. Use is not outlined here.
- **Full Administrator** – User has full access to Scalix Management Console and can run most commands on the command-line interface. One full administrator, `sxadmin`, is created by default during installation. Using Scalix Management Console, you can create other such accounts.
- **Scalix Admin Groups** – User has varying access to Scalix Management Console to undertake specific tasks and cannot run Scalix commands at the command-line interface. There are four Admin Groups, each overseeing a different aspect of the system:
 - `ScalixAdmins` – Access to Scalix Management Console
 - `ScalixGroupAdmins` – Access to Users and Groups to manage Groups
 - `ScalixUserAdmins` – Access to Users
 - `ScalixUserAttributesAdmins` – Access to personal contact information and e-mail address of Users
- **Group Manager** – User has limited access to Scalix Management Console. They cannot enter Scalix commands at the command-line interface. They can modify e-mail addresses and personal information of user accounts and manage specified group(s).

In short, when you want to provide administrator access to Scalix, you typically designate a user to be a Full Administrator, but can limit functions by using the Scalix Admin Groups or Group Manager role.

If you log in to Scalix Management Console as the default administrative user, `sxadmin`, you can delegate the lesser roles to others.

Note Users' Scalix Management Console passwords are the same as their e-mail client passwords.

Granting Full Scalix Administrator Access

Scalix Administrators, also known as full administrators, have access to all features and aspects of Scalix Management Console. They can run most commands on the command-line interface. They can create and manage other users with lower levels of access.

You can create as many full administrator accounts as you want.

Note Full administrators are not listed in any of the four Scalix Admin Groups and do not need to be.

To grant Scalix Administrator status, the user needs a fully-functioning Scalix account, either Standard or Premium user. The sxadmin account is a Standard user by default.

To enable full administrator permissions

- 1 In Scalix Management Console, click the **Users** icon on the toolbar. Current user accounts display on the left side of the window.

Tip Recall that you can use the filters menu to make the list more manageable.

- 2 Select the user account for which you want to assign full administrator permissions.
- 3 Click the **Advanced** tab.



- 4 Enable the **Is full administrator** check box.
- 5 Click **Save Changes**. The user can now log in to Scalix Management Console.

Granting Scalix Admin Group Access

There are four Scalix Admin Groups with varying levels of access to Scalix Management Console. Members of these groups can use Scalix Management Console, but are not permitted command-line access.

All admin group members must have Scalix user accounts.

The admin groups are listed in the table.

Table 1: Scalix Admin Groups

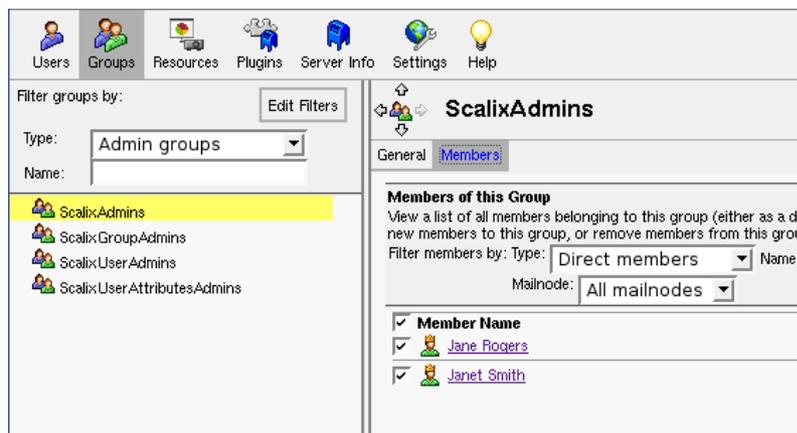
Role	Scalix Management Console Access
ScalixAdmins	Members of this group have permission to see and use all Scalix Management Console features.
ScalixGroupAdmins	Members of this group see the Users and Groups functions and can: <ul style="list-style-type: none"> • Add new groups • Modify existing groups • Add and delete members of groups
ScalixUserAdmins	Members of this group see the Users functions and can: <ul style="list-style-type: none"> • Add new user accounts • Modify existing user accounts • Delete existing user accounts
ScalixUserAttributesAdmins	Members of this group see User functions and can: <ul style="list-style-type: none"> • Edit e-mail addresses and personal contact information of user accounts

Viewing Current Admin Groups

You can view the users assigned to the different administrative groups and their properties.

To view the current Scalix admin groups and their membership

- 1 In Scalix Management Console, click the **Groups** icon on the toolbar.
- 2 From the **Type** drop-down filter, select **Admin groups**. The four Admin Groups display. Note that the default sxadmin account is not included in the ScalixAdmins group because they are a full Scalix Administrator.

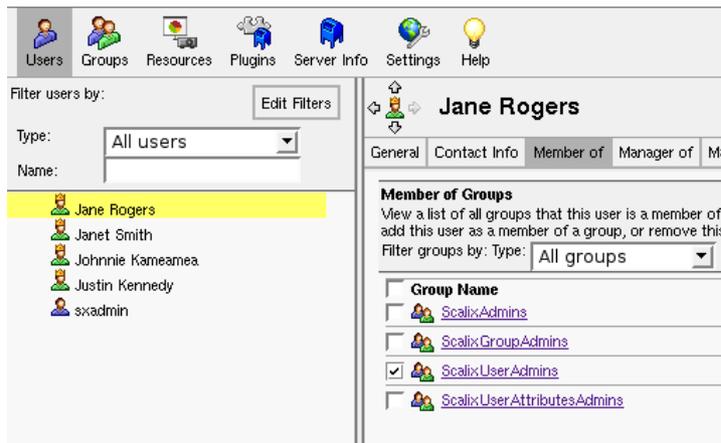


Assigning Users to Admin Groups

To grant membership in one of the four administrative groups, the user must already have a Scalix user account.

To assign users to an administrative group

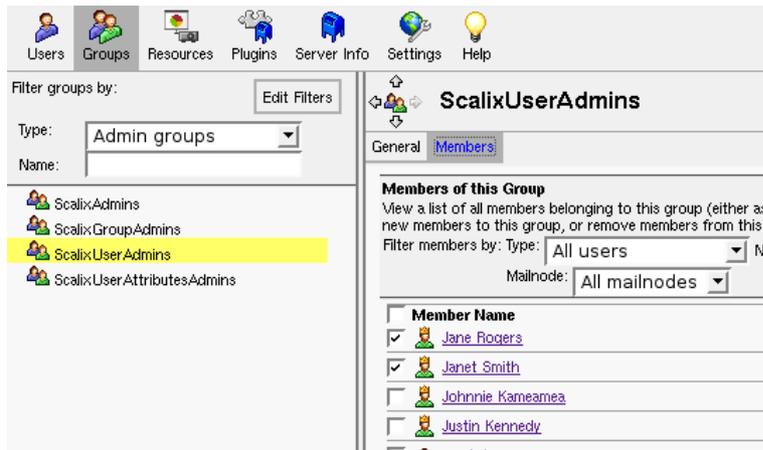
- 1 In Scalix Management Console, click the **Users** icon on the toolbar.
- 2 Select the user account to be given administrative access.
- 3 Click the **Member of** tab.
- 4 From the drop-down list, select **All Groups**. The four Admin Groups are listed.



- 5 Enable the check boxes to which you want the user to have access.
- 6 Click **Save Changes**.

An alternative method for adding users to administrative groups

- 1 In Scalix Management Console, click the **Groups** icon on the toolbar.
- 2 From the **Type** drop-down filter on the left side, select **Admin groups**. The four Admin Groups display.
- 3 Select one.
- 4 Click the **Members** tab.
- 5 From the second **Type** drop-down filter, select **All users**. All user accounts display and those that are part of the Admin Group have the box checked.
- 6 To add any users, enable the check box for the user accounts.
- 7 Click **Save Changes**.



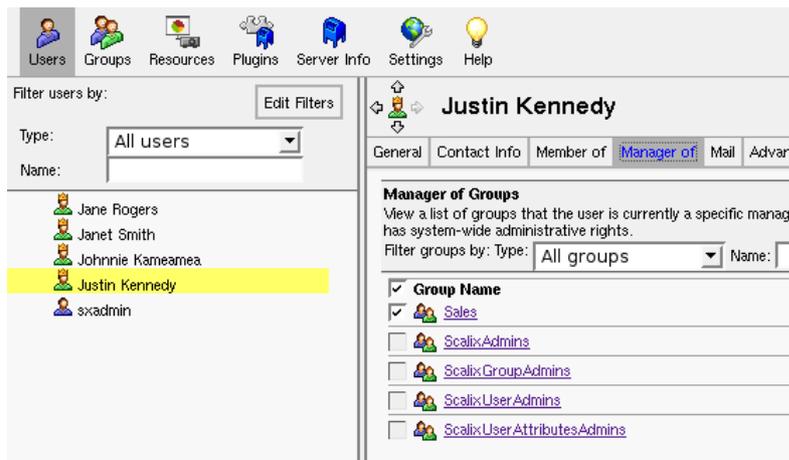
Granting Group Manager Access

The final level of administrative access is the Group Manager role. This user can log in to Scalix Management Console. They can change e-mail addresses and personal contact information of user accounts and manage specified groups.

To grant group manager status, the user must have a Scalix account.

To designate a user as a group manager

- 1 In Scalix Management Console, click the **Users** icon on the toolbar.
- 2 Select the user account to be given administrative access.
- 3 Click the **Manager Of** tab.
- 4 In the **Member Of Groups** option, enable the check box of the group that the user is to manage. The second figure shows the view displayed when logged with such permission; the Users and Groups icons display and not the rest.



The screenshot displays the Scalix Administration interface. At the top left, there are navigation icons for 'Users', 'Groups', and 'Help'. On the top right, there are 'Refresh' and 'Logout' buttons. Below the navigation, a 'Filter users by:' section includes a dropdown menu set to 'All users' and an 'Edit Filters' button. A list of users is shown on the left, with 'Johnnie Kameamea' highlighted in yellow. The main area shows the profile for 'Johnnie Kameamea', including a 'Never logged in scalix1' status. The profile is divided into 'General' and 'Contact Info' tabs. The 'General' tab is active, showing fields for 'First Name' (Johnnie), 'Middle Initial', 'Last Name' (Kameamea), and 'Suffix'. Below these is the 'Display Name' (Johnnie Kameamea). The 'Email Addresses' section contains a note about mailbox aliases and a table with one entry: 'Johnnie Kameamea' with a secondary email 'Johnniek@scalixtester.com'. An 'Add Address' button is located to the right of the email list.

Users Groups Help Refresh Logout

Filter users by: Edit Filters

Type: All users

Name:

- Jane Rogers
- Janet Smith
- Johnnie Kameamea**
- Justin Kennedy
- svadmin

Johnnie Kameamea Never logged in scalix1

General Contact Info

First Name: Johnnie Middle Initial: Last Name: Kameamea Suffix:

Display Name: Johnnie Kameamea

Email Addresses
If the user is a Scalix mail user, then these are all aliases for the user's mailbox.
If the user is an external user, then only one external mail address should be provided.

Johnnie Kameamea	<Johnniek@scalixtester.com>
------------------	-----------------------------

Add Address

Managing User Accounts

This chapter covers the creation, management, and deletion of user accounts. It also addresses user types, passwords, and mailbox size limits.

Contents

This chapter includes the following information:

- “About User Accounts” on page 51
- “Adding a User Account” on page 53
- “Changing Passwords” on page 57
- “Modifying User Information” on page 58
- “Changing User Account Types” on page 59
- “Deleting User Accounts” on page 60
- “Setting Mailbox Size Limits” on page 61
- “Unlocking a User Account after Failed Login” on page 62
- “Enabling Caching on Individual Mailboxes” on page 62
- “Enabling Search Indexing” on page 63
- “Identifying Delegates” on page 64
- “Commands” on page 64

About User Accounts

There are three types of user accounts:

- **Premium user** – All Scalix features
- **Standard user** – Some Scalix features
- **Internet Mail user** – No Scalix features but part of the Scalix database

Premium users have the following features that Standard users do not:

- Microsoft Outlook and Evolution support
- Wireless e-mail and personal information manager (PIM)
- Group scheduling functionality, including free/busy lookup in Microsoft Outlook, Scalix Web Access, and Evolution clients
- Access to public folders
- Personal folder sharing

- Delegate access
- Full CalDAV support; Standard users are limited to personal calendars

The default sadmin account is a Standard user account by default, not a Premium user account.

An Internet Mail user account is an external e-mail account added to the Scalix database. It is not a Scalix user account; the user cannot run Scalix Web Access. You add such an account to have the e-mail account included in a group, for example, add it to the Sales group to include that address when mail is sent to your Sales group. And it can be selected when scheduling a meeting or sending an e-mail.

Table 1: Options by User Type

Feature	Premium User	Standard User	Internet Mail User
Microsoft Outlook support	✓		
Evolution support	✓		
Scalix Web Access	✓	✓	
IMAP, POP support	✓	✓	
Scalix Mobile Client	✓	✓	
Wireless e-mail and PIM	✓		
Group scheduling	✓		
Public folder access	✓		
Personal folder sharing	✓		
Delegate access	✓		

In other words, Standard users access the Scalix server using the Internet Message Access Protocol (IMAP) or the Post Office Protocol (POP) and do not have access to group calendaring. Internet Mail users are outside your company/organization.

User accounts can be added to groups. For example, an employee of a sales department can be added to the Sales group. If you add the Sales group before you add the user account, the user can be assigned to that group. Otherwise, you can create the group afterwards and assign user accounts to it. The group also acts as a mailing list/public distribution list; an employee who is a member of the Sales group receives all e-mail addressed to Sales.

User accounts can be given Scalix Administrator privileges. You have the option in the wizard to do so, but for full administrative privileges, do it instead after user account creation. See the chapter “Managing Administrator Access” on page 45.

There are three ways to add user accounts: in Scalix Management Console, by migrating existing records, or a bulk provisioning. This chapter outlines use of Scalix Management Console. For migration, see the *Scalix Migration Guide*.

Adding a User Account

Using Scalix Management Console, you create Scalix user accounts, set their level of service, give them authentication IDs, enter their personal information, assign them to mailnodes, and so on. Three procedures follow:

- Adding a Premium or Standard user account
- Adding an Internet mail user account
- Adding user accounts in bulk

To add a Premium or Standard user account

- 1 In Scalix Management Console, click the **Users** icon on the toolbar.
- 2 At the bottom of the window, click the **Create User(s)** button. The button appears when your administrative privileges allow you to add user accounts. The Create New User wizard appears.

- 3 Select the type of user for this account:
 - **Scalix Premium User** – Permits use of Microsoft Outlook, Evolution, and Scalix Web Access, and has access to all Scalix features
 - **Scalix Standard User** – Has limited access to Scalix features

Note

Recall that there can be limits on the number of user accounts permitted. See “Product Editions” on page 12, or check your Scalix license under Settings > Mail Server > License Keys.

- 4 Enter the **First Name**, **Middle Initial** (optional), and **Last Name** for the user account you are creating. Scalix uses this information to automatically fill in other

fields, which adopt the input according to rules set up (“Configuring General Settings” on page 26). When the **Display Name**, **Mail Address**, and/or the **Authentication ID** fields cannot be edited, this is due to an existing rule. Otherwise, you can over-ride the autocompleted fields, for example use e-mail address and authentication ID formats of jimmym instead of Jimmy.Marsters, so the user logs in with jimmym instead of Jimmy.Marsters and his e-mail address is jimmym@yourdomain.com instead of Jimmy.Marsters@yourdomain.com

- **Display Name** – The name to show in Scalix Management Console for the user account
- **Mail Address** – The e-mail address for the user, where the first field is the name displayed in the e-mail address and the second and third fields are the e-mail address. For example, the name Jimmy Marsters displays for jimmym@yourdomain.com
- **Mailnode** – The Scalix mailnode to use. When you have more than one mailnode specified, you can select one, for example OttawaEast or OttawaWest
- **Authentication ID** – What the user uses to log in to Scalix Web Access, for example
- **Password** – The password for the user to log in to Scalix Web Access, for example
- **Confirm Password** – The password retyped
- **User must change password on first login** – Enable to force the user to specify a new password when they log in for the first time. Otherwise they use the password that you type in this window.
- **Is locked** – Enable to prevent the user from using the user account. The user cannot log in.
- **User can use SWA** – Enable to allow the user access to Scalix Web Access. Enabled by default.
- **Add Sender header to delegate’s outgoing messages** – Enable to add e-mail header information to e-mails. Enabled by default.

Note When illegal characters are entered, the text is red.

- 5 This completes the essential user account information. You now have the following options:
 - Click **Next** to add contact and group information for this user.
 - Click **Finish** to add the user to the system. You can add the other information later.
- 6 If you clicked **Next**, the second wizard screen appears. This is where you enter contact information.

The screenshot shows a web browser window titled "http://172.16.1.226 - Create New User - Firefox". The page is titled "Create New User" and contains a "Contact Information" section. Below the title, it says "Enter in personal information that can be published in the address book." and has a checked checkbox for "Display in address book.". The form fields are as follows:

Company:	Star Tours Inc.	Work Phone:	
Department:		Work Phone 2:	
Office:		Home Phone:	(310) 232-7393
Title:		Home Phone 2:	
Street:	332 Rodderick Street	Mobile Phone:	(310) 824-3937
City:	Beverly Hills	Fax:	(310) 824-3940
State/Province:	California	Pager:	
Zip/Postal Code:	90209	Notes:	
Country:	United States		
Language:	English (American)		

At the bottom of the form, there are five buttons: "< Back", "Next >", "Finish", "Save and Create Another User", and "Cancel". The URL at the bottom of the browser window is "http://172.16.1.226/sac/AdminAddUserWizard.jsp#".

- 7 Fill in the fields, or use any available pull-down menus to complete them.
- 8 After you complete the new user contact information, you have the following options:
 - Click **Next** to add this user to any groups
 - Click **Finish** to add the user to the system. You can enter group information later.
- 9 If you clicked **Next**, the third wizard screen appears. This is where you add the user account to groups and/or give it administrative privileges.

The screenshot shows the same web browser window, but now on the "Group Membership" screen. The title is "Create New User" and the section is "Group Membership". It says "Select the groups that the user belongs to." Below this, there is a "Filter groups by:" section with a "Type:" dropdown set to "All groups" and a "Name:" text box. Below the filter, there is a list of groups with checkboxes:

Group Name	Selected
<input checked="" type="checkbox"/> Sales	<input checked="" type="checkbox"/>
<input type="checkbox"/> ScalixAdmins	<input type="checkbox"/>
<input type="checkbox"/> ScalixGroupAdmins	<input type="checkbox"/>
<input type="checkbox"/> ScalixUserAdmins	<input type="checkbox"/>
<input type="checkbox"/> ScalixUserAttributesAdmins	<input type="checkbox"/>

At the bottom of the form, there are five buttons: "< Back", "Next >", "Finish", "Save and Create Another User", and "Cancel". The URL at the bottom of the browser window is "http://172.16.1.226/sac/AdminAddUserWizard.jsp".

- 10 If any groups have been added to the system, such as Sales, they are appear in the list. Otherwise the four administrative groups appear:
 - **ScalixAdmins** – Access to Scalix Management Console
 - **ScalixGroupAdmins** – Access to Users and Groups to manage Groups

- **ScalixUserAdmins** – Access to Users
- **ScalixUserAttributesAdmins** – Access to personal contact information and e-mail address of Users

Enable the check boxes of the groups the user is to belong to. If you add a user to a group, they also become part of the mailing list for that group. For example, a member of the Sales group receives all e-mail addressed to Sales@yourdomain.com. For administrative privileges, you can instead give the user full privileges after creating the user account.

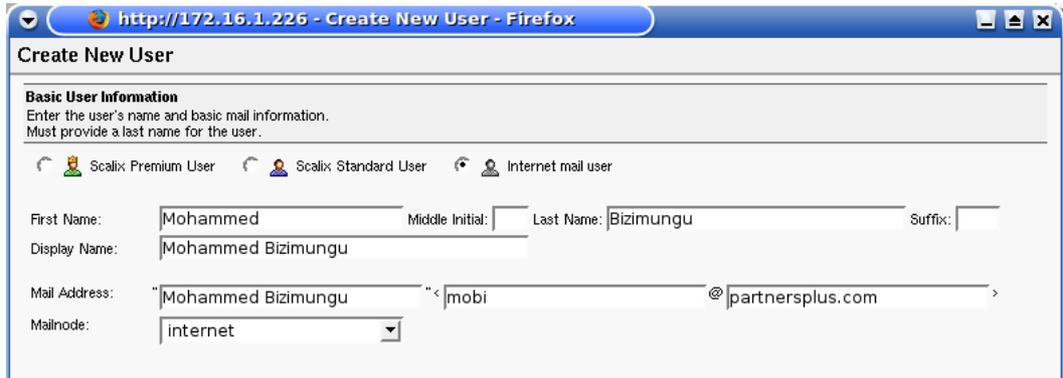
- 11 Click **Finish** to add the user to the system.
- 12 To give the user full Scalix administrator privileges, in the **Users** panel, click the **Advanced** tab for the user account, and enable the **Is full administrator** option.

Tip

You can use commands to view groups and users in the groups. “omshowpdl -l all” lists groups, such as ScalixUserAdmins and any groups created, such as Sales or group2. “omshowpdln -l “sales” displays all the user accounts belonging to the sales group.

To add an Internet Mail account

- 1 In Scalix Management Console, click the **Users** icon on the toolbar.
- 2 At the bottom of the window, click the **Create User(s)** button. The button appears when your administrative privileges allow you to add user accounts. The Create New User wizard appears.



- 3 Enable the following option:
 - **Internet mail user** – To include an external e-mail account in the Scalix database. The account does not have access to Scalix Web Access. It can be added to groups.
- 4 Enter the **First Name**, **Middle Initial** (optional), and **Last Name** for the user account you are creating.
 - **Display Name** – The name to show in Scalix Management Console for the user account
 - **Mail Address** – The e-mail address for the user, where the first field is the name displayed in the e-mail address and the second and third fields are the e-mail address
 - **Mailnode** – The Scalix mailnode to use. The choices are internet and internet.tnef, where TNEF refers to an e-mail attachment format used in Microsoft Out-

look and Microsoft Exchange Server. These are both Internet mail gateways set up by default when Scalix is installed.

- 5 Click **Next** to modify the contact and group information as outlined in the previous procedure, and add the account. If you do not modify the contact information, the account appears as if part of your company/organization.

To add user accounts in bulk

- 1 Try the “omaddu --bulk” command. See the MAN page for information.

Changing Passwords

You can change the password of a user account.

To change the password for a user account

- 1 In Scalix Management Console, click the **Users** icon on the toolbar.
- 2 Select the user account.
- 3 Click the **General** tab.
- 4 In the lower right-hand corner, click **Change Password**. The *Change Password* window appears.



- 5 Enter the new password, and then retype it in the second field.
- 6 If required, enable the **User must change password on first login** check box. This prompts the user to create a new password the next time they log in to the Scalix server.
- 7 Click the **Change Password** button. The password is changed.

Modifying User Information

The e-mail addresses and personal information stored for a user account can be changed. You can make a user account/e-mail address private so that it does not display in the address book.

Changing Contact Information

If needed, you can change a user's company, address, department, phone numbers, and more.

To change the contact information for a user account

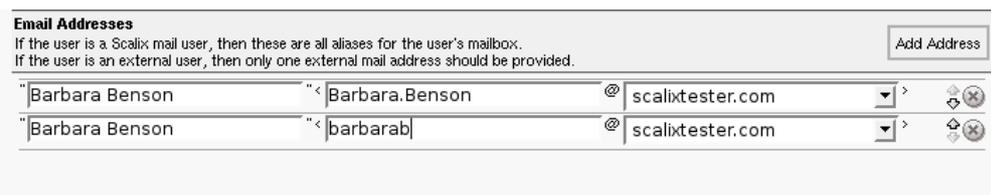
- 1 In Scalix Management Console, click the **Users** icon on the toolbar.
- 2 Select the user account.
- 3 Click the **Contact Info** tab.
- 4 Change the information. Note the **Display in address book** check box, which gives you the option to make the entire user account public or private. For example, when disabled, the user account does not appear as a contact/e-mail address when other users address e-mails.
- 5 At the bottom of the window, click **Save Changes**.

Changing and Adding E-mail Addresses

You can change users' e-mail addresses after they have already been assigned and add more.

To change a user's e-mail addresses

- 1 In Scalix Management Console, click the **Users** icon on the toolbar.
- 2 Select the user account.
- 3 Click the **General** tab.
- 4 Under the **Email Addresses** options, modify the alias and domain values. To add a second e-mail address for the employee, click **Add Address**. For example, user Barbara.Benson@yourcompany.com can also have the e-mail address barbarab@yourcompany.com.
- 5 You can shuffle the entries in the address list using the up and down arrows at the right. The address at the top of the list becomes the default address that the system uses for all messages addressed to or sent by this user.
- 6 At the bottom of the window, click **Save Changes**.



Deleting E-mail Addresses

You can delete users' e-mail addresses.

To delete an address from a user's address list

- 1 In Scalix Management Console, click the **Users** icon on the toolbar.
- 2 Select the user account.
- 3 Click the **General** tab.
- 4 Delete the e-mail address by clicking its X at the right side of the window. The address is immediately deleted.
- 5 At the bottom of the window, click **Save Changes**.

Changing User Account Types

You can switch a user account between Standard and Premium types. There is no option to switch to an Internet Mail account because that type of user is external. To switch an Internet Mail account to a Scalix user account, delete the Internet Mail account and add a new user account.

To change a user account type

- 1 In Scalix Management Console, click the **Users** icon on the toolbar.
- 2 Select the user account.
- 3 Click the **Advanced** tab. The tab does not appear for an Internet Mail user.
- 4 Enable the preferred option: **Is premium user** or **Is standard user**.
- 5 At the bottom of the window, click **Save Changes**.

The screenshot shows the 'Advanced' tab in the Scalix Management Console. The 'Login Identification' section is active, showing the 'Authentication ID' as 'Barbara.Benson'. Below this, there are two radio buttons for user type: 'Is premium user' (selected) and 'Is standard user'. Other options include 'Is full administrator', 'Is locked', 'User can use S/WA', 'Add Sender header to delegate's outgoing messages', and 'Enable SmartCache' (checked). A 'Prepare SmartCache' button is also visible.

Deleting User Accounts

You can delete one or multiple user accounts. You can delete all user accounts in a mailnode.

When you delete a user account, you remove the record and all related mail and scheduling archives. In short, you delete every Scalix record for that user.

To delete a user account

- 1 In Scalix Management Console, click the **Users** icon on the toolbar.
- 2 Select the user account. To delete more than one, use the **Ctrl** or **Shift** keys to select multiple user accounts.
- 3 Click **Delete User(s)**.
- 4 Confirm the deletion at the prompt. The user account(s) are deleted, as well as all user data.

Alert

When you delete a user account, you also delete the user's e-mail, calendar, and other data.

To delete all user accounts from a mailnode

- 1 In Scalix Management Console, click the **Server Info** icon on the toolbar.
- 2 On the left side, select the mailnode, for example scalix1 or OttawaEast.
- 3 Click the **Users** tab. A list of users in the mailnode displays.
- 4 Click **Delete Listed Users**.
- 5 Confirm the deletion at the prompt. All user accounts with that mailnode are deleted, as well as all user data.

Alert

When you delete a user account, you also delete the user's e-mail, calendar, and other data.

Setting Mailbox Size Limits

Mailbox size allowed can be controlled on a global or user level. For set it globally, see “Setting Mailbox Size and Warning Messages” on page 30. Individual limits override server settings. The easiest approach is to set it at the global level, then set an individual user account. For example, you set all users to have a 200 MB capacity limit and grant the president of your company and the sales team 500 MB each. Typical values are 100 MB to 1 GB (1000 MB).

To set mailbox size on a user account

- 1 In Scalix Management Console, click the **Users** icon on the toolbar.
- 2 Select the user account.
- 3 Click the **Mail** tab.
- 4 From the **Maximum Mailbox Size** drop-down list, select an option:
 - **Enter Limit** – To specify the maximum size of a user’s mailbox. Enter the size in MB, for example 200 MB to 1000 MB (1 GB).
 - **Unlimited** – To allow the user’s mailbox size to take as much space as needed
 - **Use Server Limit** – To specify the maximum size of a user’s mailbox according to global settings (**Settings > Mail Server > Maximum Mailbox Size**). This is the default.
- 5 When a limit is used, specify what happens to mail when reached for that particular user. If you do not enable any setting here, the global ones apply.
 - **Send warning on outgoing mail...and reject when over the limit** – Enable the check box to send a message to a user when their mailbox is near the limit when they send an e-mail, and do not send the outgoing e-mail when the mailbox exceeds the limit. Disable the check box if you do not want a message to be sent to the user and to send the outgoing e-mail anyway. The warning message is defined at the global level (**Settings > Mail Server > Maximum Mailbox Size**).
 - **Reject incoming mail when over the limit** – When a user’s mailbox is full, do not accept new mail addressed to the user
 - **Send mail to user when over the limit** – When a user’s mailbox is full, accept new mail addressed to the user
- 6 At the bottom of the window, click **Save Changes**.

General	Contact Info	Member of	Manager of	Mail	Advanced
<p>Mailbox Limits Set the limits on the user’s mailbox. Also set the sanctions that are imposed on a user when the limit is exceeded.</p> <p>Used Mailbox Size: 25 KB Used Wastebasket Size: 1 KB Percentage of Quota Used: No limit set</p> <p>Maximum Mailbox Size: <input type="text" value="Use Server Limit"/></p> <p><input type="checkbox"/> Send warning on outgoing mail when near limit; reject outgoing mail when over the limit. <input type="checkbox"/> Reject incoming mail when over the limit. <input type="checkbox"/> Send mail to user when over the limit.</p>					

Unlocking a User Account after Failed Login

By default, a user can make unlimited incorrect login attempts, but the number of tries can be set (“Blocking Login Attempts After Failure” on page 34), after which the user cannot log in, even when the user account and password entered are correct. The user account is locked when the threshold is breached. The user may or may not see a message to that effect. You need to unlock the user account to allow access.

To unlock a user account

- 1 In Scalix Management Console, click the **Users** icon on the toolbar.
- 2 Select the user account.
- 3 Click the **Advanced** tab.
- 4 Disable the **Is Locked** check box, which has a check mark when the account is locked.
- 5 At the bottom of the window, click **Save Changes**.

Tip

You can reset the user's password at this time, which you can do by clicking Change Password. Tell the user too what the authentication ID format is, for example first.last@yourcompany.com or First.Last or First.Last@yourcompany.com.

Enabling Caching on Individual Mailboxes

To improve the speed and responsiveness of a user's e-mail service in Microsoft Outlook, use the SmartCache feature. This creates a copy of the user's mailbox on his or her computer as well as on the server, allowing them to work on the local computer, speeding up performance and lowering bandwidth.

With SmartCache, the system checks the server only when sending and receiving new messages, meaning fewer trips to and from the sever.

You can set SmartCache for all users on a server by enabling it through the server setting explained in “Controlling SmartCache Use for User Accounts” on page 28. Or you can set it on a user-by-user basis here, which overrides the system-wide setting. Please note that the setting outlined here affects whether SmartCache is enabled or enabled in Microsoft Outlook at the user computer and that the user can change the value; it does not configure SmartCache.

The setting is enabled by default. It applies to Premium user accounts because they can use Microsoft Outlook.

If preferred, you can download the user's entire mailbox in one single file, which speeds the initial cache creation process. This method, initiated by clicking the Prepare SmartCache button, is optional and best used for large mailboxes. If you choose not to use this method,

the cache creates one message at a time the next time that user logs in to Microsoft Outlook.

The Prepare SmartCache button is only used when the cache is first created, or when the user changes computers and the cache has to be rebuilt. From then on, the user's messages cache each time they synchronize with the server.

To enable SmartCache for a user account

- 1 In Scalix Management Console, click the **Users** icon on the toolbar.
- 2 Select the user account.
- 3 Click the **Advanced** tab.
- 4 Enable the **Enable SmartCache** check box.
- 5 At the bottom of the window, click **Save Changes**.
- 6 At a convenient time, create the mailbox for the local machine by clicking the **Prepare SmartCache** button. This is a resource-intensive procedure, so if the mailbox is large, wait until you have the time and bandwidth to allow the process to complete. The amount of time it takes depends on the size of the mailbox.

Enabling Search Indexing

The ability to search for messages, contacts, and appointments in Scalix Web Access is enabled by default, and you can manage this for each user. Also, if the user's search index corrupts, you can repair it.

To enable search indexing

- 1 In Scalix Management Console, click the **Users** icon on the toolbar.
- 2 Select the user account.
- 3 Click the **Advanced** tab, which appears for Standard and Premium user accounts.
- 4 Enable the **Enable SIS Indexing** check box. Its location appears in the **SIS Index URL** field, which cannot be changed.
- 5 At the bottom of the window, click **Save Changes**.

To repair the search function

- 1 Click the **Recreate SIS Index** button.
- 2 Confirm the repair at the prompt.

Search and Index Server (SIS) Settings
 Modify SIS Index settings for this user. Recreate SIS Index

Enable SIS Indexing

SIS Index Url:

Identifying Delegates

You can set the system to identify delegates in the header of an e-mail message. With this setting enabled (default), outgoing messages sent by a delegate have a header identifying the actual sender.

The setting applies to Scalix Web Access. For more information on how to set this in Microsoft Outlook, see Microsoft Outlook's online help.

To identify messages as from delegates

- 1 In Scalix Management Console, click the **Users** icon on the toolbar.
- 2 Select the user account for which you want to enable identification as a delegate.
- 3 Click the **Advanced** tab.
- 4 Enable the **Add Sender header to delegate's outgoing messages** check box.
- 5 At the bottom of the window, click **Save Changes**.

Commands

You can also use commands to add and delete user accounts.

Table 2: User Account Commands

Command	Description
omaddu	Add a user account.
omadmidp	Configure system IDs for use by Scalix users.
omconfpwd	Configure password controls.
omdelu	Delete one or more user accounts.
ommoddl	Modify distribution list entries and auto-action addresses, for example when a user changes their name.
ommodu	Modify a user account.
omshowpwd	Show password controls, such as expiry period and minimum length of passwords.
omshowu	List users or display details about a specific user.

Managing Groups

This chapter covers the creation, administration, and use of groups (public distribution lists) in Scalix Management Console.

Contents

This chapter includes the following information:

- “About Groups” on page 65
- “Adding a Group / Mailing List” on page 66
- “Viewing Users in a Group” on page 69
- “Adding Users to a Group” on page 69
- “Modifying a Group” on page 70
- “Deleting a Group” on page 71
- “Assigning Group Managers” on page 71
- “Logging in as a Group Manager” on page 72
- “Commands” on page 73

About Groups

In the Scalix system, the terms “group” and “public distribution list” are used interchangeably. A public distribution list is a mailing list. When you create a group called Sales and add user accounts as members, then all e-mails addressed to Sales are sent to all user accounts belonging to the Sales group. Groups can contain individual users, other groups, or both.

There are two levels of group membership:

- **Direct** – User was assigned to the group
- **Effective** – User became a member because another group to which the user belongs was added to the group

Adding a Group / Mailing List

There are four groups by default, related to administrator access to Scalix. These users can use Scalix Management Console but cannot run Scalix commands at the command-line interface. (The users are not full Scalix administrators, which you designate with full administrator option in the **Advanced** tab.)

Table 1: Default Groups

Group	Scalix Management Console Access
ScalixAdmins	Members of this group have permission to see and use all Scalix Management Console features.
ScalixGroupAdmins	Members of this group see the Users and Groups functions and can: <ul style="list-style-type: none"> • Add new groups • Modify existing groups • Add and delete members of groups
ScalixUserAdmins	Members of this group see the Users functions and can: <ul style="list-style-type: none"> • Add new user accounts • Modify existing user accounts • Delete existing user accounts
ScalixUserAttributesAdmins	Members of this group see User functions and can: <ul style="list-style-type: none"> • Edit e-mail addresses and personal contact information of user accounts

You can add, edit, and delete groups. When you add a group, you add an e-mail address. For example, adding a group called sales creates an e-mail address called sales@yourdomain.com and all users in the group receive mail addressed to sales@yourdomain.com

To create a group

- 1 In Scalix Management Console, click the **Groups** icon on the toolbar.
- 2 At the bottom of the window, click **Create Group(s)**. A Create New Group wizard appears.

http://172.16.1.226 - Create New Group - Firefox

Create New Group

Basic Group Information
Enter in the group's name.

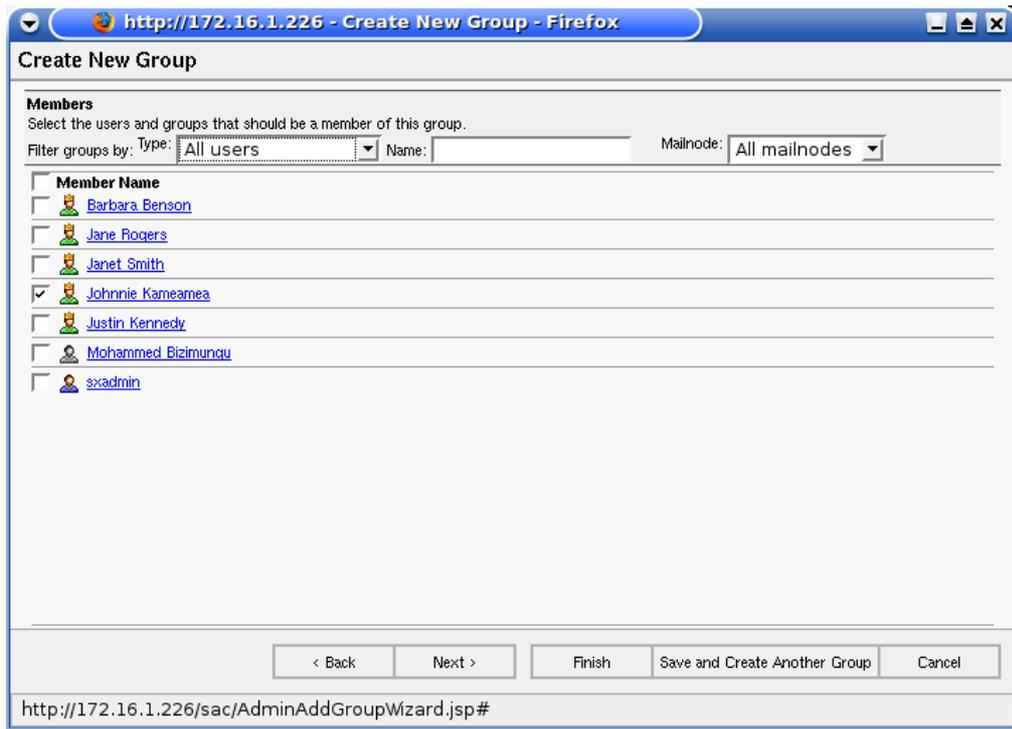
Group Name: Display in address book.

Group server location:

< Back Next > Finish Save and Create Another Group Cancel

http://172.16.1.226/sac/AdminAddGroupWizard.jsp#

- 3 Identify the group:
 - **Group Name** – Provide a name for the group, for example training or NewYork or TechSupport. The name is used in the e-mail address, for example TechSupport@yourcompany.com
 - **Display in address book** – When disabled, the group does not appear when users access the contacts/address list when addressing an e-mail for example. The users in the group appear, but not the group itself.
 - **Group server location** – Select the mailnode
- 4 This completes basic information. You now have the following options:
 - Click **Next** to add user accounts to the group.
 - Click **Finish** to add the group to the system. You can add members later.
- 5 If you clicked **Next**, the second wizard screen appears. This is where you add members.



- 6 With **All users** selected from the **Type** drop-down list, enable the check boxes of the user accounts to be members of the group.
- 7 This completes individual membership information. You now have the following options:
 - Click **Next** to add groups to the group.
 - Click **Finish** to add the group to the system. You can add groups later.
- 8 If you clicked **Next**, the third wizard screen appears. This is where you add groups.
- 9 Enable the check boxes of the groups that you want to belong to the new group. For example, you can add the Marketing group to the SalesMarketing group.
- 10 Click **Finish**. The group is added to the system.

Viewing Users in a Group

You can view which user accounts have been assigned to a group. The user interface and commands can be used.

To view user accounts in a group

- 1 In Scalix Management Console, click the **Groups** icon on the toolbar.
- 2 From the **Type** drop-down filter, select **All groups**.
- 3 Select a group. The members of the group are listed.

To view user accounts in a group using commands

- 1 The `omshowpdl` and `omshowpdln` commands can be used to view users in a group, which is referred to as a public distribution list (PDL). Examples are as follows.

```
omshowpdl -l all
```

displays all groups, such as ScalixUserAdmins and any groups created, such as Sales or group2.

```
omshowpdln -l "sales"
```

displays all users in a group called sales.

Adding Users to a Group

There are two ways to add members to existing groups:

- Modify a user account (through the **Member of** tab)
- Modify the group (through the **Members** tab)

To add a user account to a group by modifying the user account

- 1 In Scalix Management Console, click the **Users** icon on the toolbar.
- 2 Select the user account.
- 3 Click the **Member of** tab.
- 4 In the **Type** drop-down list, select **All groups**.
- 5 Enable the check boxes of the groups to which the user account is to belong.
- 6 At the bottom of the window, click **Save Changes**.

To add user accounts to a group by modifying the group

- 1 In Scalix Management Console, click the **Groups** icon on the toolbar.
- 2 Select the group.
- 3 Click the **Members** tab.
- 4 From the **Type** drop-down list, select **All users**.
- 5 Enable the check boxes of the user accounts to include in the group.
- 6 At the bottom of the window, click **Save Changes**.

Modifying a Group

You can change a group's name as well as give it a second address.

Changing a Group Name and E-mail Address

You can change a group name.

To change the name of a group

- 1 In Scalix Management Console, click the **Groups** icon on the toolbar.
- 2 Select the group.
- 3 Click the **General** tab.
- 4 To change the name, edit the **Group Name** field, for example change "Sales" to "sales".
- 5 Change the e-mail address entries to reflect the change.
- 6 At the bottom of the window, click **Save Changes**.

Adding a Group E-mail Address

To add a second e-mail address to be used by the group

- 1 In Scalix Management Console, click the **Groups** icon on the toolbar.
- 2 Select the group.
- 3 Click the **General** tab.
- 4 Click the **Add Address** button on the right side of the window. A new data row appears.

Email Addresses				Add Address
If this is a scalix group then these are all aliases for the group. If this is an external group then only one mail address should be provided .				
"sales"	<sales	@scalixtester.com	>	⬆ ⬇ ⬆
"	<	@scalixtester.com	>	⬆ ⬇ ⬆

- 5 Enter an alias for the group. The first field is the name of the group that appears for the address, for example Mktg Dept, and the second field forms the first part of the e-mail address, for example mktg.
- 6 Use the up and down arrows to shuffle the new address within the group's address list. The address at the top of the list is the default address that the system uses.
- 7 At the bottom of the window, click **Save Changes**.

Deleting a Group

You can delete groups from Scalix when you have appropriate administrator permissions. Deleting a group does not delete the individual user accounts of members.

To delete a group

- 1 In Scalix Management Console, click the **Groups** icon on the toolbar.
- 2 Select the group(s).
- 3 At the bottom of the window, click the **Delete Group(s)** button.
- 4 Confirm the deletion at the prompt. The group is deleted, but not the user accounts.

Assigning Group Managers

There are four ways to allow users to manage groups: make them full administrators, add them to the ScalixAdmins group, add them to the ScalixGroupAdmins group, or make them a manager of group(s). See the “Managing Administrator Access” chapter for descriptions. A Group Manager role has limited scope.

Group managers can:

- Add or delete members from their group
- Modify group-specific information about members

Group managers must:

- Have a Scalix user account
- Be a member of the group they are managing

Assigning a Group Manager

It is easy to make a user a group manager.

To make a user a group manager

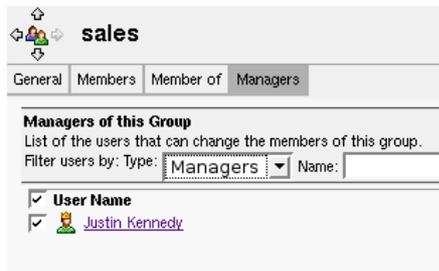
- 1 In Scalix Management Console, click the **Users** icon on the toolbar.
- 2 Select the user account.
- 3 Click the **Manager Of** tab.
- 4 Select **All groups** from the drop-down list.
- 5 Enable the check boxes of the groups that the user can manage.
- 6 At the bottom of the window, click **Save Changes**.

Determining Who is Group Manager

You can view who has permission to manage a group.

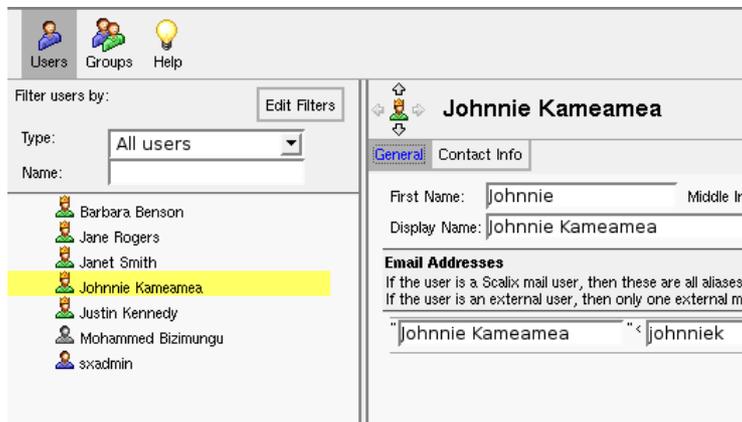
To determine who is group manager

- 1 In Scalix Management Console, click the **Groups** icon on the toolbar.
- 2 Select the group.
- 3 Click the **Managers** tab. Any managers appear in a list.



Logging in as a Group Manager

When a group manager logs in to Scalix Management Console, he or she has access to the Users and Groups modules. The manager can view all user accounts and perform limited administration tasks for the group(s) for which he or she is the manager.



You can do the following:

- Sort the members by direct or effective status
- Look for new member candidates and add them to the group
- Delete current members from the group

Commands

Command for groups are listed in the table.

The pdl commands let you add and modify public distributions lists, but not designate members.

The aci commands give users control of the public distributions lists. For example, with the omaddaci command, you specify users who can read and modify a public distribution list.

Table 2: Group Commands

Command	Description
omaddpdl	Add a public distribution list.
omaddpdln	Add an entry to a public distribution list.
omdelpdl	Delete one or more public distribution lists.
omdelpdln	Delete one or more entries from a public distribution list.
ommodpdl	Modify a public distribution list.
ommodpdln	Modify public distribution list entries.
omshowpdl	List public distribution lists. Example: omshowpdl -l all to display all groups. Example: omshowpdl -l "sales" to display all user accounts in a group called sales.
omshowpdln	List entries in a public distribution list.
omaddaci	Add an Access Control Item member.
omchkaci	Check Access Control Item capabilities for a user.
omdelaci	Delete an Access Control Item member.
ommodaci	Modify an Access Control Item member.
omshowaci	Show the contents of Access Control Item.

Managing Resources

This chapter covers how to create, book, and manage shared resources, such as conference rooms and printers.

Contents

This chapter includes the following information:

- “About Shared Resources” on page 75
- “Setting Up a Shared Resource” on page 76
- “Booking a Shared Resource” on page 78
- “Changing Shared Resource Settings” on page 79

About Shared Resources

Using Scalix Management Console, you can manage shared resources, such as conference rooms, company projectors, printers, and other equipment. Scalix allows you to set up a shared resource so that it can be booked and tracked by users.

As an administrator, you set up the resource in Scalix Management Console, then others can reserve or view reservations in their client, specifically Microsoft Outlook or Scalix Web Access.

Only Premium users can book resources; Standard users cannot.

Setting Up a Shared Resource

Any resources to be booked by users must first be set up in Scalix Management Console. You need to be a full administrator or belong to the ScalixAdmins group in order to see the Resources icon on the toolbar. When you add a resource, you are also adding an e-mail address for the resource.

To set up a shared resource

- 1 In Scalix Management Console, click the **Resources** icon on the toolbar.
- 2 In the lower left corner, click **Create Resources**. A Create New Resource wizard launches.
- 3 Configure the resource. Provide a name, password, and other information for it as follows:
 - **Name** – Also used for the e-mail address. For example, when you use the name Boardroom 1, the e-mail name is Boardroom 1 and the e-mail address is Boardroom.1@yourcompany.com
 - **Mailnode** – From the drop-down list, select a mailnode through which the resource’s reservations route. For more on mailnodes, see “Managing Mailnodes” on page 39.
 - **Create as Premium Resource** – When disabled, every Premium user has full access to the resource.

When enabled, select users can log in to the resource account from Scalix Web Access and Microsoft Outlook. This enables you to set fine-grained access control on the resource calendar, determining who can book a resource and who cannot. Access is set in the client as you do any folder.

This also enables delegates to open the resource calendar if given that level of access (also set in the client as a folder property), and it enables blocking direct resource booking if you prefer to designate one central person (such as an office assistant) to manually approve every booking.

- **Can have recurring events** – When enabled, this means that the resource can be reserved in a regular, recurring time slot, such as every Friday at 3 p.m.
- **Can book concurrent events** – When this box is checked, the resource can be booked by multiple people for the same time

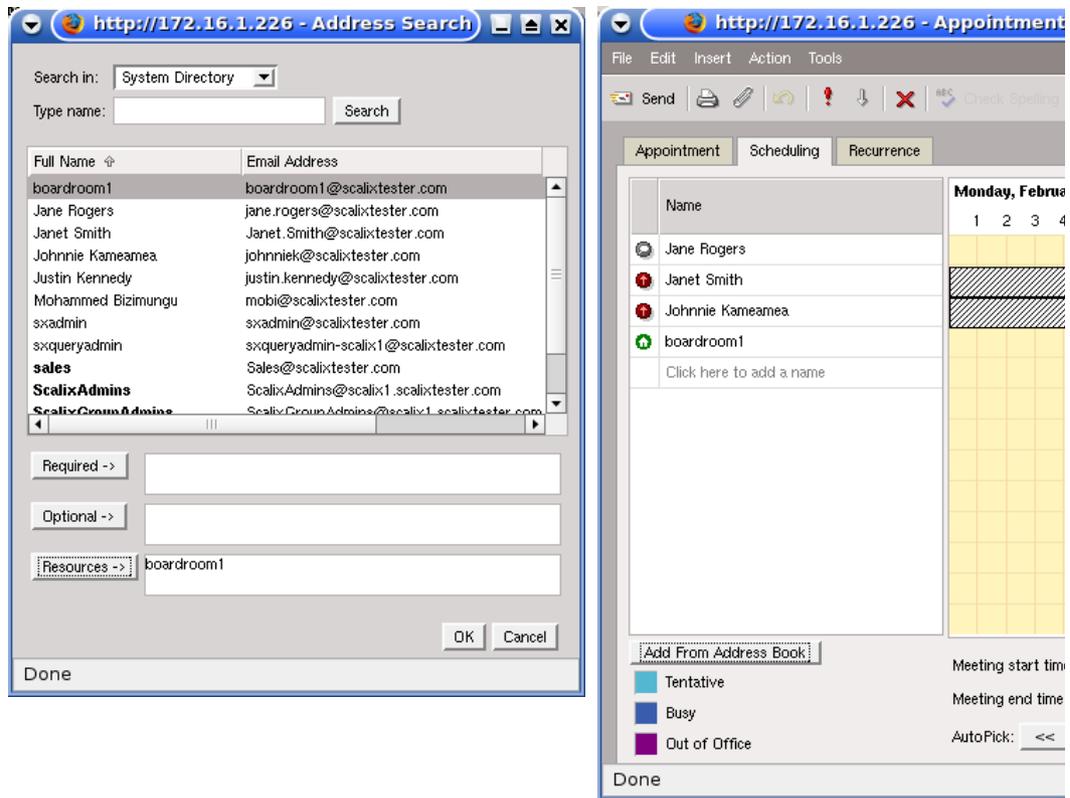
- 4 At the bottom of the window, click **Next** or **Finish**. Use **Next** to check the contact information of the resource, such as company name, telephone number of a boardroom, or location of a projector.
- 5 If you clicked **Next**, the *Contact Information* screen appears. Here, you record information about the shared resource, such as the telephone number for a conference room or the location of a shared projector.
- 6 Click **Finish**. The resource is added to the list and an e-mail address is created for it.

Booking a Shared Resource

Shared resources are booked by end users in their client applications, meaning Microsoft Outlook and Scalix Web Access. Other clients, such as Thunderbird and Evolution, do not have this feature. Only Premium users can book resources.

To book a shared resource in Microsoft Outlook or Scalix Web Access

- 1 Open client application.
- 2 In the list of folders on the left side of the window, click **Calendar**.
- 3 Reserve the resource in the same way you add an attendee to a meeting. For example, to hold a meeting in a boardroom, you create an appointment, adding both attendees and the resource. That way, you view free/busy times of attendees and the resource.
- 4 When finished, click **Send**. The resource is booked and an e-mail is sent to attendees.



To view bookings of a resource

- 1 Log in to Scalix Web Access as the resource, for example boardroom1@yourcompany.com. The password was specified when the resource was created.
- 2 View the calendar.

Changing Shared Resource Settings

You can modify and delete shared resources and change their passwords.

Modifying a Shared Resource

If needed, you can change the properties for any shared resource. That includes its name, e-mail address, location, availability to Standard versus Premium users, and more.

To modify a shared resource

- 1 In Scalix Management Console, click the **Resources** icon on the toolbar.
- 2 Select the resource. Its properties appear.
- 3 In the **General**, **Contact Info** and **Advanced** tab, change information as required.
- 4 At the bottom of the window, click **Save Changes**.

Changing Passwords

You can change a shared resource's password. This is the password used to log in to Scalix Management Console as the resource, for example to view the schedule of a boardroom.

To change a shared resource's password

- 1 In Scalix Management Console, click the **Resources** icon on the toolbar.
- 2 Select the resource.
- 3 Click the **General** tab.
- 4 In the lower right-hand corner, click **Change Password**. The Change Password window appears.

- 5 Enter the new password, and then retype it in the second field.
- 6 If required, enable the **Resource must change password on first login** check box. This prompts the user to create a new password the next time the resource is logged in to the Scalix server.
- 7 Click the **Change Password** button. The password is changed.

Deleting a Shared Resource

You can delete a shared resource from the system. Once deleted from the Scalix Management Console, it no longer appears in users' clients.

To delete a shared resource

- 1 In Scalix Management Console, click the **Resources** icon on the toolbar.
- 2 Select the resource(s).
- 3 In the lower left-hand corner, click **Delete Resource**.
- 4 Confirm the deletion at the prompt. The resource is removed from the list.

Monitoring the Server

This chapter covers the management of basic server functions, including services, disk space, logging levels, and message queues.

Contents

This chapter includes the following information:

- “Introducing Server Info” on page 81
- “Stopping and Starting Services” on page 82
- “Using Logs” on page 83
- “Monitoring the Active Users” on page 84
- “Monitoring Disk Space” on page 85
- “Monitoring Message Queues” on page 86
- “Viewing Installed Components” on page 87
- “Commands” on page 87

Introducing Server Info

The Server Info feature allows you to manage server processes to ensure smooth and proper function of the Scalix system. The elements manageable are:

- **Mailnodes** – A category that you can create to help you organize your user base. A mailnode is similar to a mail stop; it organizes your mail users into mail groups, for example based on department or location. Your Scalix server has one mailnode by default, but you can add more and then sort your users and groups into the various nodes as you prefer. See the chapter “Managing Mailnodes” on page 39.
- **Services** – Processes that you can start and stop while the Scalix server is operating and set logging levels
- **Daemons** – Processes that Scalix starts automatically when you start the Scalix server and that operate continuously while the Scalix server is running. All daemons are listed under “Services”.
- **Queues** – Pass messages and requests to Scalix services involved in message processing. Some services have associated queues, others do not.

There are a number of server-specific tasks that you can perform with the assistance of the Server Info features in Scalix Management Console.

Stopping and Starting Services

You can use Scalix Management Console to stop and/or start any of the services, daemons, or queues. It can be done globally and for individual resources.

At the global/server level, services are sorted into two lists: key and other. The most important services (key) are listed by default, and you can expand the list by clicking the **Display all services** option (shown in next figure).

To stop and start services globally

- 1 In Scalix Management Console, click the **Server Info** icon on the toolbar.
- 2 At the left side, select the server, for example scalix1.yourcompany.com
- 3 Click the **Services** tab. This tab lists key services by default, but you can browse all other Scalix services by clicking **Display all services**.

Note that each service has either a green light or red light, to indicate its status.

- 4 To stop all services, click the **Stop All Services** button at the bottom right of the window. Confirm the action at the prompt.

To stop an individual service, click its **Stop** button, which is visible when a service is running. Confirm the action at the prompt.

- 5 To start all services, click the **Start all Services** button at the bottom right of the window.

To start an individual service, click its **Start** button, which is visible when a service is not running.

The screenshot shows the Scalix Management Console interface. The top toolbar includes icons for Users, Groups, Resources, Plugins, Server Info, Settings, and Help. The left sidebar shows a tree view of the server hierarchy: scalix1.scalixtester.com > OttawaEast > scalix1 > Services. The main pane displays the 'Scalix Services' tab, which lists several services with their status (green light for running) and a 'Stop' button. The services listed are: IMAP Daemon, Internet Mail Gateway, LDAP Daemon, Local Delivery, PDP3 Interface, Remote Client Interface, and Service Router. The 'Stop' button is visible for each service, indicating they are currently running. The interface also shows a 'Refresh' button and a 'Refreshed at 15' timestamp.

Service Name	Status	Running since	Additional Info
IMAP Daemon	Running (Green Light)	02.01.08	
Internet Mail Gateway	Running (Green Light)	02.01.08	with 1 messages
LDAP Daemon	Running (Green Light)	02.01.08	
Local Delivery	Running (Green Light)	02.01.08	with 0 messages
PDP3 Interface	Running (Green Light)	02.01.08	with 0 users
Remote Client Interface	Running (Green Light)	01.29.08	with 0 users
Service Router	Running (Green Light)	02.01.08	with 0 messages

To stop and start a service

- 1 In Scalix Management Console, click the **Server Info** icon on the toolbar.
- 2 Select a service from the list on the left side.
- 3 To stop the service, click **Stop Service** at the bottom right of the window. Confirm the action at the prompt.
- 4 To start the service, click **Start Service** at the bottom right of the window.

Using Logs

You can set the level of detail to log for services, for example log only errors or log warnings and errors. These are event logs. You can view log files.

To set the log level for a service

- 1 In Scalix Management Console, click the **Server Info** icon on the toolbar.
- 2 Select a service.
- 3 Click the **General** tab.
- 4 From the **Logging Level** drop-down list, select a level.
- 5 At the bottom of the window, click **Save Changes**.

To view a log

- 1 In Scalix Management Console, click the **Server Info** icon on the toolbar.
- 2 Select a service.
- 3 Click the **Event Log** tab.
- 4 Click the **Get Log** button on the right side. Information displays when available. To increase the amount of information shown, select **All Messages** from the **Display level** drop-down list and/or change the date for log filtering.

General **Event Log**

Service Event Log
List of log messages for this service. you may filter it by date/time as well as the type of message

Display level: **All Messages** Number of lines: 1000

Filter log by: From date: **Three days ago** From time:
To date: **Today** To time:

Get Log

```
REPORT Local Delivery(Local Delivery) 02.11.08 16:01:30
[OM 7602] Local Delivery Shut Down
Last Msg Sender: Jane Rogers/scalix1
Last Msg Id: 701636868.261202758179954.JavaMail.root(a).scalix1.scalixtester.com
Last Msg DirectRef: 00011805c9f63cae

REPORT Local Delivery(Error Manager ) 02.11.08 16:01:30
[OM 8802] Error Manager Server Shut Down

REPORT Local Delivery(Error Manager ) 02.11.08 16:02:10
[OM 8801] Error Manager Server Started Up
```

Note

Saving the event log or any customized samples as data files is done at the Scalix command-line interface. See “Event Log Commands” on page 252.

Monitoring the Active Users

You can monitor the currently connected client users and assess the processes generated by their connection.

To view user accounts currently logged in

- 1 In Scalix Management Console, click the **Server Info** icon on the toolbar.
- 2 At the left side, select the Scalix server, for example scalix1.yourcompany.com
- 3 Click the **Active Users** tab, which lists all connected users who are logged in to Scalix Web Access. It does not display users logged in to Scalix Management Console. The following summary is provided:

- Each user's name
- The kind of connection made (IMAP, MAPI, or POP)
- The ID assigned to each user-generated process

There are usually two entries for each user logged in.

- 4 You can refresh the list manually or start an automatic refresh/update process.
 - Click the **Refresh** button to manually update this tab's contents.
 - Enable the check box by **enable automatic refresh**. The default refresh rate is once a minute.

The screenshot shows the Scalix Management Console interface. The left-hand navigation pane is expanded to show the 'Server Info' section for 'scalix1.scalixtester.com'. The main content area is titled 'Active Users on the Scalix Server' and contains a table of active user processes. The table has three columns: 'User Name', 'Connection Type', and 'Started at'. The data in the table is as follows:

User Name	Connection Type	Started at
Justin Kennedy	SWA client (20047)	Started at 15:16:42
Justin Kennedy	Unknown Client (20044)	Started at 15:16:42
Justin Kennedy	SWA client (20014)	Started at 15:16:33
Janet Smith	Unknown Client (19984)	Started at 15:16:22
Janet Smith	SWA client (19970)	Started at 15:16:17
Jane Rogers	Unknown Client (19960)	Started at 15:16:04
Jane Rogers	SWA client (19945)	Started at 15:16:00

Below the table, there is a 'Refresh' button and a checkbox labeled 'enable automatic refresh' with a refresh rate of 'every 60 seconds'.

Monitoring Disk Space

You can use Scalix Management Console to obtain a high-level view of activity in the Scalix server Message Store, such as disk space used. It does not allow you to perform any direct management of the Message Store.

To check the Message Store

- 1 In Scalix Management Console, click the **Server Info** icon on the toolbar.
- 2 On the left side, select the server, for example scalix1.yourcompany.com
- 3 Click the **Storage** tab. The following information displays:
 - **Total Mailbox Size** – The cumulative total of all current mailboxes, including folder items, inbox items, and calendar items
 - **Total Wastebasket Size** – The cumulative total of items in the Trash that have not been expressly deleted
 - **Total Message Store Size** – The used and available capacity of this server’s Message Store

A colored bar shows used (red) and available space (green).

- 4 You can also browse the most active (highest-capacity) mailboxes, and see how much space each mailbox takes (including undeleted trash).

The default view is **10** mailboxes, but you can change this number.

The screenshot shows the Scalix Management Console interface for the server scalix1.scalixtester.com. The 'Storage' tab is selected, displaying the following information:

Scalix Message Store Size
 This is information about the total Scalix message store size for this server as well as specific information on the largest mailboxes on the server.

Total Mailbox Size: 4,542 MB
 Total Wastebasket Size: 6 KB
 Total Message Store Size: 4,548 MB of 19,172 GB used

Overview: A progress bar shows 19.2GB used (red) and 100% total capacity. The bar is mostly red, indicating high usage.

List 10 mailboxes.

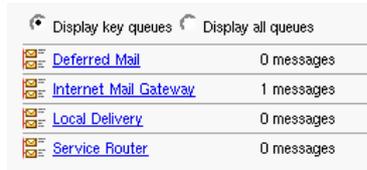
User name	Mailbox Size ↓	Wastebasket Size	Total Size
Jane Rogers	4,386 MB	1 KB	4,387 MB
sradmin	52 KB	1 KB	53 KB
Barbara Benson	25 KB	1 KB	26 KB
Janet Smith	23 KB	1 KB	24 KB
Justin Kennedy	21 KB	1 KB	22 KB
Johnnie Kameamea	9 KB	0 KB	9 KB

Monitoring Message Queues

You can view message queues globally and individually, and you can purge messages from a queue.

To check all message queues

- 1 In Scalix Management Console, click the **Server Info** icon on the toolbar.
- 2 On the left side, select the server, for example scalix1.yourcompany.com
- 3 Click the **Queues** tab. A summary of queues displays.



Queue Type	Message Count
Deferred Mail	0 messages
Internet Mail Gateway	1 messages
Local Delivery	0 messages
Service Router	0 messages

To check individual message queues

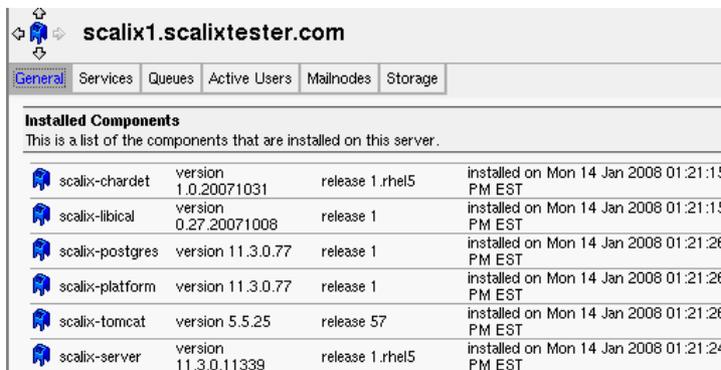
- 1 In Scalix Management Console, click the **Server Info** icon on the toolbar.
- 2 Select the queue you want to monitor, for example **Local Delivery** or **Internet Mail Gateway**. If the queue you want to monitor is not visible, expand the **Other Queues** category. The following information is provided for a queue:
 - The number of messages processed in the last 60 seconds
 - The number of messages in the queue over a five minute period
 - The total number of messages processed in the queue in the last 15 minutes
- 3 You can customize the message list settings:
 - Use the menus to set the **Type**, **Priority**, and **Number** of messages listed.
 - Filter the messages by entering the text of a particular subject or sender.
 - If you choose, you can permanently store these settings for later reuse by clicking **Save Changes** (at the bottom of the window).
- 4 Click the **Refresh** button.
- 5 The message list updates according to your specifications.
- 6 If needed, you can delete all listed messages by clicking **Delete Listed Messages** in the lower right corner of the window.

Viewing Installed Components

You can use Scalix Management Console to review installation-specific information about your Scalix server and its primary components. This is useful when you are troubleshooting problems.

To view the Scalix components installed

- 1 In Scalix Management Console, click the **Server Info** icon on the toolbar.
- 2 In the left side of the window, select the server, for example scalix1.yourcompany.com
- 3 Click the **General** tab. The following information is displayed:
 - The version number of each Scalix component
 - The release number
 - The date the component was installed or upgraded



Installed Components			
This is a list of the components that are installed on this server.			
scalix-charDET	version 1.0.20071031	release 1.rhel5	installed on Mon 14 Jan 2008 01:21:15 PM EST
scalix-libical	version 0.27.20071008	release 1	installed on Mon 14 Jan 2008 01:21:15 PM EST
scalix-postgres	version 11.3.0.77	release 1	installed on Mon 14 Jan 2008 01:21:26 PM EST
scalix-platform	version 11.3.0.77	release 1	installed on Mon 14 Jan 2008 01:21:26 PM EST
scalix-tomcat	version 5.5.25	release 57	installed on Mon 14 Jan 2008 01:21:26 PM EST
scalix-server	version 11.3.0.11339	release 1.rhel5	installed on Mon 14 Jan 2008 01:21:24 PM EST

Commands

You can also use commands to stop and start services. The services are:

Notification Server	Remote Client Interface
Database Monitor	Test Server
LDAP Daemon	Request Server
Directory Relay Server	Print Server
IMAP Server Daemon	Directory Synchronization
SMTP Relay	Bulletin Board Server
Mime Browser Controller	Background Search Service
Event Server	Dump Server
Service Router	CDA Server
Local Delivery	POP3 interface
Internet Mail Gateway	Archiver
Sendmail Interface	Omscan Server
Local Client Interface	

For example, to stop the Notification Server, enter

```
omoff "Notification Server"
```

The daemons are as follows and can be listed with the omstat command:

Service Router	Print Server
Local Delivery	Bulletin Board Server
Internet Mail Gateway	Background Search Service
Local Client Delivery	CDA Server
Remote Client Interface	POP3 interface
Test Server	Omscan Server
Request Server	

Table 1: Service, Queue, and Daemon Commands

Command	Description
omisoff	Check Scalix services are off.
omoff	Stop one or more services.
omon	Start one or more services.
omrc	Start Scalix.
omreset	Reset status of services or remove Scalix.
omresub	Resubmit messages.
omresubdmp	Resubmit messages processed by the Archive server.
omsetsvc	Display the status of a service in detail; configure auxiliary processes.
omshut	Stop Scalix.
omstat	List Scalix daemons.

Using Plug-ins

This chapter outlines plug-ins for frequently run tasks.

Contents

This chapter includes the following information:

- “About Plug-ins” on page 89
- “Viewing and Running Plug-ins” on page 89
- “Writing Plug-ins” on page 91
- “Deploying Plug-ins” on page 93
- “Deployment Script Reference” on page 94
- “Examples” on page 95

About Plug-ins

Plug-ins allow you to save and run frequent tasks in Scalix Management Console, such as checking load, disk usage, scanning logs, listing public folders, and checking the Message Store. Plug-ins extend the functionality of Scalix Management Console and provide the ability to launch one-way scripts from the graphical user interface.

For security reasons, only full administrators can run these plug-ins and they must have plug-in permissions.

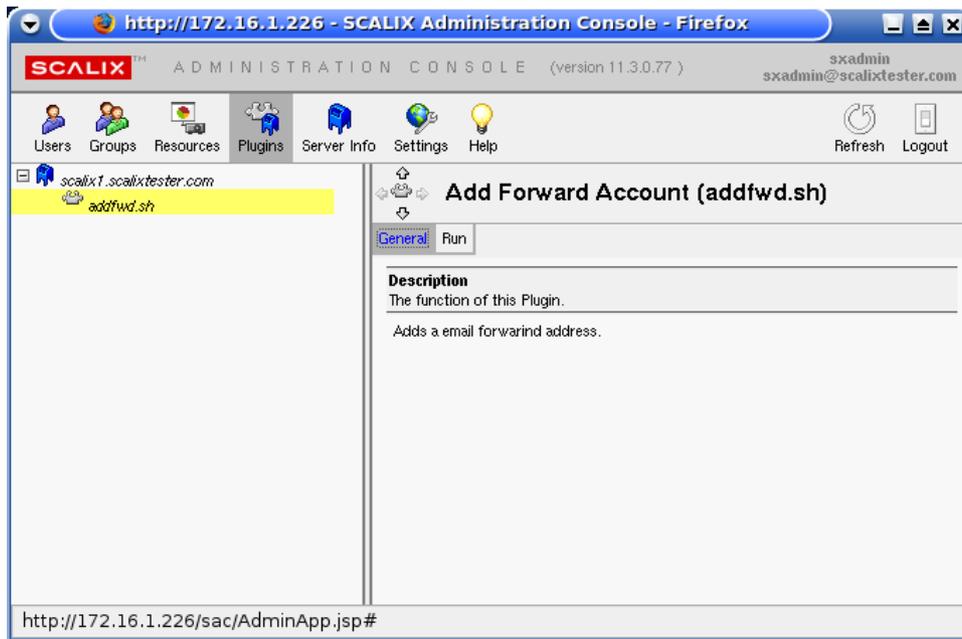
There are other restrictions:

- Plug-ins cannot download files or executables from the Internet
- Plug-ins cannot remove or delete anything from the Scalix system’s file system
- Plug-ins cannot remove or delete bulk users and groups
- Plug-ins cannot consume large amounts of system resources, run repeatedly, or for long periods of time

Scalix provides several templates in the Administration Resource Kit and you can write your own. No plug-ins are provided by default in the product. Examples are included at the end of the chapter.

Viewing and Running Plug-ins

As with other functions, Scalix Management Console lists available plug-ins in a hierarchy, with individual plug-ins appearing underneath the servers on which they run. There also is an **All Servers** node with plug-ins that have global impact.



To view and run plug-ins

- 1 In Scalix Management Console, click the **Plugins** icon on the toolbar.
- 2 Select the plug-in you want to run. (No plug-ins are provided by default, so none display by default.)
- 3 Click the **General** tab to view the plug-in's function.
- 4 To run the plug-in, click the **Run** tab.
- 5 Complete the fields as needed. The fields vary depending on the script being used.
- 6 If results are called for, they appear in a pop-up window entitled, **Plugin Results**.
- 7 To refresh the results, click **Enable automatic refresh** in the upper right-hand corner, fill in the time interval desired, then click **Refresh**.

Writing Plug-ins

The goal of the plug-in framework is to facilitate a simple mechanism to run custom scripts. You can write your own plug-ins. Make them simple and low in resource usage. The framework is not intended for complicated programs that consume large amounts of host resources.

Programming Language

The choice of language for plug-in development is yours, as long it has an execution or run-time environment on the production machine. If using Perl, Python, or Java, the production server (or the target host) must have the appropriate runtime environment.

Note that all plug-ins are forked and executed by the remote execution service, so they can create further processes. All resources consumed during the execution of these plug-ins must be reaped, especially child processes created, or threads created or sockets and temporary files used. Where possible, judicious usage of threads must be observed for potential deadlock issues.

Management plug-ins must be owned by the root user and must have UNIX 700 permission set. Avoid using any setuid programs.

Writing the Plug-in

When writing your own plug-in, there are several factors to keep in mind:

- **Exit Status** – Each plug-in must exit with non-zero status upon failure. Do not make the exit status 1 because failed shell scripts exit with 1.
- **Error Message** – In case of problems, return an error message on a single line. The error must be written to stderr. For example, a failed plug-in error message can look like this: `script_name: Failed to locate the user, <user name>, on the server directory on host <host name>.`
- **Naming Conventions** – Do not use script or language extensions, such as `.py`, `.pl`, or `.sh`. In addition, do not use for plug-in names any shell interpretable characters, such as `*`, `!`, `$`, `""`, ```, `~`, or other unconventional characters, such as `()`, `[]`, or `{ }`. Underscore and dashes are acceptable (`_` and `-`), but preferably the script or plug-in name is a single word, less than 20 characters. For example, `checkqueues`, `monitordisk`, and `docolloate_entries`.
- **Usage or Help Information** – All plug-ins must have a `-- help` option. This help option must provide the following information about the script:

Version – This is a place-holder for backward compatibility of parameter parsing

Friendly Name – Give each plug-in a unique name, known as the “friendly name.” For example, a `checktemperature` script can have a friendly name of “Check Temperature”, and the output looks like:

```
NAME:
```

```
Check Temperature
```

This must be a single line of output with token `NAME:`, and on the next line, followed by the name.

Description – This can be multiline output that describes the script’s function. Its format is as follows:

DESCRIPTION:

This script checks the room temperature usage for the SAN appliance in the remote data center at the Exodus Facilities in Santa Clara.

Parameters List – This final line has the token PARAMETERS: and a six-column, tab-separated output on the next line, describing the attributes of each argument or option. On each line of output, each column must have the following attributes:

column 1: Option flags

column 2: Symbolic or human-readable name for the flag

column 3: Default value if any for the flag

column 4: Type of value: number, boolean, or string

column 5: Type of argument: single, multi, or none.

column 6: Short description of the flag or option.

For example, these values must be printed or echoed by the script onto stdout and must have the six columns in the following tab-separated manner:

PARAMETERS:

```
-t temperature 78 number single "Temperature of the Data Center"
```

```
-- help help "" "" "" "Usage Information for checktmp"
```

Output Type – This token represents the type of output generated by the plug-in. The two expected types are text/html or text/plain, with text/plain being the default.

The output format or the results from the run of a plug-in must each be on a separate line. The output displays on the console, as is, from the run.

Altogether the output of the sample script when executed with “checktmp -- help” is shown as follows. New tokens begin in the first column and are separated from the previous set by a new line.

VERSION:

1.0

NAME:

Check Temperature.

DESCRIPTION:

This script checks the room temperature of the data center in Virginia Exodus collocated servers.

PARAMETERS:

```
-t temperature 78 int single "Temperature of the Data Center"
```

```
-- help help "" "" "" "Usage Information for checktmp"
```

OUTPUT-TYPE:

text/html

Two examples are provided in the next sections. You can get the code from:

http://www.scalix.com/wiki/index.php?title=Administration_Plugins

Deploying Plug-ins

Once a plug-in is written, you can deploy it.

All plug-ins must be deployed by a system administrator with root access on the target or production server. That is, Scalix Management Console does not provide an upload facility for security reasons.

The scripts and all associated files are added to the following folder:

```
/var/opt/scalix/<nn>/s/plugin/
```

where nn varies with Scalix installation, and the directory is instance-specific.

A default deployment script (sxcfgplugin.py) is provided for the system administrator to bootstrap or deploy plug-ins and initialize respective access control list (ACL) items for specified user(s). The user authorized to execute the script must exist (or its directory entry) on the target host where the script is deployed.

All deployed scripts must have UNIX 700 permission, and the owner and group must be root.

Programming Language Considerations

Python

If you deploy a python script, remove any .py extension, and preferably compile it. The first line of any python script must have `#!/usr/bin/python`, which negates the need to proceed its invocation with the prefix python runtime environment.

Perl

Observe similar guidelines as for Python, short of compilation.

Shell

Strip all .sh or .csh, or .ksh extensions or prefixes. Make the first line of code `#!/path_to_shell`

C/C++

All C/C++ programs deployed as plug-ins must be compiled.

Java

All Java programs deployed as plug-ins must be compiled and a shell wrapper provided around it to invoke the Java runtime environment with its desired Java options. The remote execution server only invokes the shell wrapper, supplying it with the received argument list, via the console.

Deploying the Plug-in

Finally, add the plug-in to the system.

To deploy a plug-in

- 1 Copy the plug-in to the deployment directory:

```
cp <plugin_name> /var/opt/scalix/<nn>/s/plugin/
```

where nn varies with Scalix installation.

- 2 To create an ACL for a resource-type request:

```
omaddacl -t plugin -l <plugin_name>
```

- 3 Provide execute permission for the specified user, after which only full administrators with “execute” permissions have access to the plug-ins within the console.

```
omaddacln -t plugin -l <plugin_name> -n ORN_user_admin -c "execute"
```

or

```
omaddacln -t plugin -l <plugin_name> -a ORN_PDL -c "execute"
```

Deployment Script Reference

To deploy plug-ins, use the deployment script, `sxcfgplugin.py`. It has several options:

```
-- add [options]
-- delete [options]
-- list [options]
-- deploy [options]
-- undeploy [options]
-- help
```

Use the “add” subcommand to allow new users to be added to the plug-in ACL:

```
-- add -l { <plugin_name> | all } -u user_authid -i {<instance_name> | all }
}
```

Use “delete” to remove users:

```
-- delete -l {<plugin_name> | all } - user_authid -i {<instance_name> | all }
}
```

List all the plug-ins deployed for an “instance” or list all plug-ins for which the -u user_authid has execute access:

```
-- list -i {<instance_name> | all} [-u authid]
```

Deploy the plug-in:

```
-- deploy { -D <source_directory> | -l <plugin_path_name> } { -i <instance_name> | all } [-u user_authid]
```

If -D is specified, take all plug-ins under that directory and deploy them, or -l plugin_path_name deploys only a single plug-in for all instances or a single specified instance.

The -u user_authid option creates the appropriate ACLs as well. This is the equivalent of doing an -- add operation, after -- deploy.

Undeploy the plug-in from the specified instance or all instances:

```
-- undeploy -l <plugin_name> -i {<instance_name> | all }
```

This involves removing all the ACLs associated with the ACL and removing the file.

Examples

Two examples are provided.

Creating a Public Folder and Optionally Assigning it an E-mail Address

Create a plug-in called addpf to create a Public Folder, install it into Scalix Management Console as a plug-in, download the file, and then run this command:

```
sxcfgplugin.py --deploy -l addpf.sh -u sxadmin -i <instancename>
```

Here is the code to create the file called addpf.sh:

```
#!/bin/bash
#
# Copyright (C) 2008 Scalix Corporation. All Rights Reserved.
#
```

```
help() {
    echo ""
    echo ""
    echo "VERSION:"
    echo "1.0"
    echo ""
    echo "NAME:"
    echo "Add Bulletin Board"
    echo ""
    echo "DESCRIPTION:"
    echo ""
    echo "omadbb adds a Bulletin Board."
    echo "PARAMETERS:"
```

```

    echo "-m Parent Folder    string    single    Parent Folder (disable for
Top Level)"
    echo "-s Name of Folder    string    single    Name of Folder"
    echo "-c Common Name (CN)    string    single    Email address to assign
to folder"
    echo "-e Email Address    string    single    Email address to assign to
folder"
    echo "-n Mailnode $mailnode    string    single    Email address to assign
to folder"
    echo "--help    Help    \"\"    \"\"    \"\"    Usage Information"
    echo ""
    echo "OUTPUT:"
    echo ""
    echo "text/plain"
}
#
# main script
#

declare params
declare match
declare subject
declare emailaddress
declare mailnode
declare CN
params=""
match=""
subject=""
DDV1=""
emailaddress=""
mailnode=`/opt/scalix/bin/omshowmn | grep "***" | sed "s/^\.*[*].\(.*\)/
\1/g"`
CN=""

while [ "$1" != "" ]; do
    case "$1" in

```

```

--help) help;
                                exit 0
                                shift;;
-m) match="$2";
                                DDV1="$2>"
                                params="$params -m $2";
                                shift;;
-s) subject="$2";
                                DDV1="$DDV1$2"
                                params="$params -s $2";
                                shift;;
-e) emailaddress="$2";
                                shift;;
-c) CN="$2";
                                shift;;
-n) mailnode="$2";
                                shift;;
*) params="$params $1 $2";
                                shift;;

esac
shift
done
/opt/scalix/bin/omadbbb $params

if [ -n "$emailaddress" ]
then
    /opt/scalix/bin/omaddent -e "S=+BB/OU1=$mailnode/CN=$CN/DDT1=BB-NAME/
DDV1=$DDV1/IA=$emailaddress"
fi

exit 0

```

Creating an E-mail Forwarding Account

Use a plug-in called addfwd to create an e-mail forwarding account.

Create the addfwd.sh file by getting the code from

http://www.scalix.com/wiki/index.php?title=Administration_Plugins

It requires the sxaa file in the `/opt/scalix/bin` folder. The file allows a system administrator to administer server-based Scalix rules (autoactions) from the command line. See `man sxaa` for usage.

To install the plug-in, download the file and then run this command:

```
sxcfgplugin.py --deploy -l addfwd.sh -u sxadmin -i <instancename>
```

Running Backups and Recovery

This chapter covers backup and recovery strategies and procedures to protect your data and system configurations.

Contents

This chapter includes the following information:

- “Strategies” on page 99
- “Performing Full Backups” on page 100
- “Performing Incremental Backups” on page 108
- “Performing Export/Import Backups to Back Up Individual Mailboxes” on page 109
- “Restoring the Full System” on page 110
- “Restoring a Single User’s Mailbox” on page 111

Strategies

Back up your Scalix data on a regular basis and daily at least. A good backup encompasses all contents of the Scalix home folder (normally *var/opt/scalix* in a single-server or typical installation scenario). It includes not only e-mail messages and their folders, but also calendar items, public folders, and system configurations. You can back up to tape, to the same computer, or to a different one.

Because the Scalix system is a series of flat Linux folders, the backup procedure can take the form of a simple snapshot or copy procedure. But because many of those files are interrelated and dynamically reference one another, files and pointers (reference information) are continually created and deleted during messaging transactions, making for a dynamic environment. As a result, capturing a full and accurate snapshot requires temporarily suspending the system to ensure a complete and consistent copy.

There are several methods for backup and recovery, each with its own strengths and limitations. No single solution meets all needs and some combination can be the best approach for your organization. The options include:

- Full Backup and Restore – Most comprehensive with smallest size, but can be cumbersome for restoring a single user’s data and cannot restore individual items
- Disaster Recovery – Restores (and replaces) everything on the system, including messages, calendar items, contacts, routing, and system settings
- Mailbox Export and Import – Best for restoring a single user’s data or individual items, but results in a larger backup

Some possible strategies are:

- Do regular full backups for safety
- Do occasional full backups with regular incremental backups. For example, back up the full system weekly, but record changes nightly (the increment) since the last full backup
- Do regular full backups for the system as a whole and complement that with export/import backups for key executives and employees to enable single-user restore for the most important employees
- Do regular full backups and infrequent export/import backups on the system as a whole

Other decisions are:

- Do you want to back up to tape, to a different partition on the same computer, or to a different server?
- Do you want to stop the system entirely before taking a snapshot or temporarily suspend write activity?

Performing Full Backups

For a full backup and restore scenario, it is best to use logical volume management (LVM) to take a snapshot of the entire folder structure, including the message store, public folders, folders, and system synchronizations on all servers and store the data on tape in a safe location.

For full backup, there are two options:

- Back up the entire system every time – The most comprehensive and failsafe method but takes longer and results in larger file size
- Back up the entire system the first time to establish a baseline, then use the synchronization command to record only the changes that have occurred since that baseline. This is less comprehensive, but faster and results in smaller backup size.

To restore, you have several choices:

- Full recovery – Restore the entire system to the original servers, including all folders
- Partial recovery – Restore the entire system to a secondary server (or servers) then extract the part(s) you need and copy them in to the live system

After deciding on approach, there are choices about how to stop the system long enough to get an accurate snapshot. Because the Scalix database consists of files representing different components that dynamically reference each other (such as mailboxes, folders, messages, and attachments), files and pointers (reference information) are continually created and deleted during messaging transactions, making for a dynamic environment. Any backup actions taken while the system is active can result in an incomplete and inconsistent copy.

To solve this problem, there are two options when doing a full backup:

- Shut down Scalix (omshut), and then copy, tar, tar-gz, or rsync the contents of the Scalix home folder to another location, then restart Scalix (omrc)
- Temporarily suspend write activity to Scalix (omsuspend), create a snapshot of the instance home directory, release the suspension, and then copy, tar, tar-gz, or rsync the

contents of the snapshot to another location. A five-second suspension of activity normally suffices.

Best Practices for Full Backups

Some best practices for backups:

- Take advantage of snapshot capabilities. LVM, provided with Linux, provides snapshot functionality.
- After an initial backup, you can use the `rsync` command to back up changes
- When using the `rsync` method, use another Linux host if possible. This provides a redundant spare if needed, a message recovery server, and multiple daily copies.
- Where applicable, use compression in the form of a `tar -zxvf` command.
- Back up all of the Scalix home directory, including subfolders and their files
- When backing up to a different server, the permissions must be the same on both servers
- When using `rsync`, use the `-H` switch to ensure that hard links are retained. For example:

```
rsync -azvH
```

where `a`=archive, `z`=compress data during transport, `v`=verbose, and `H`=retain hardlinks. If hard links are lost, the size of the message store can grow significantly.

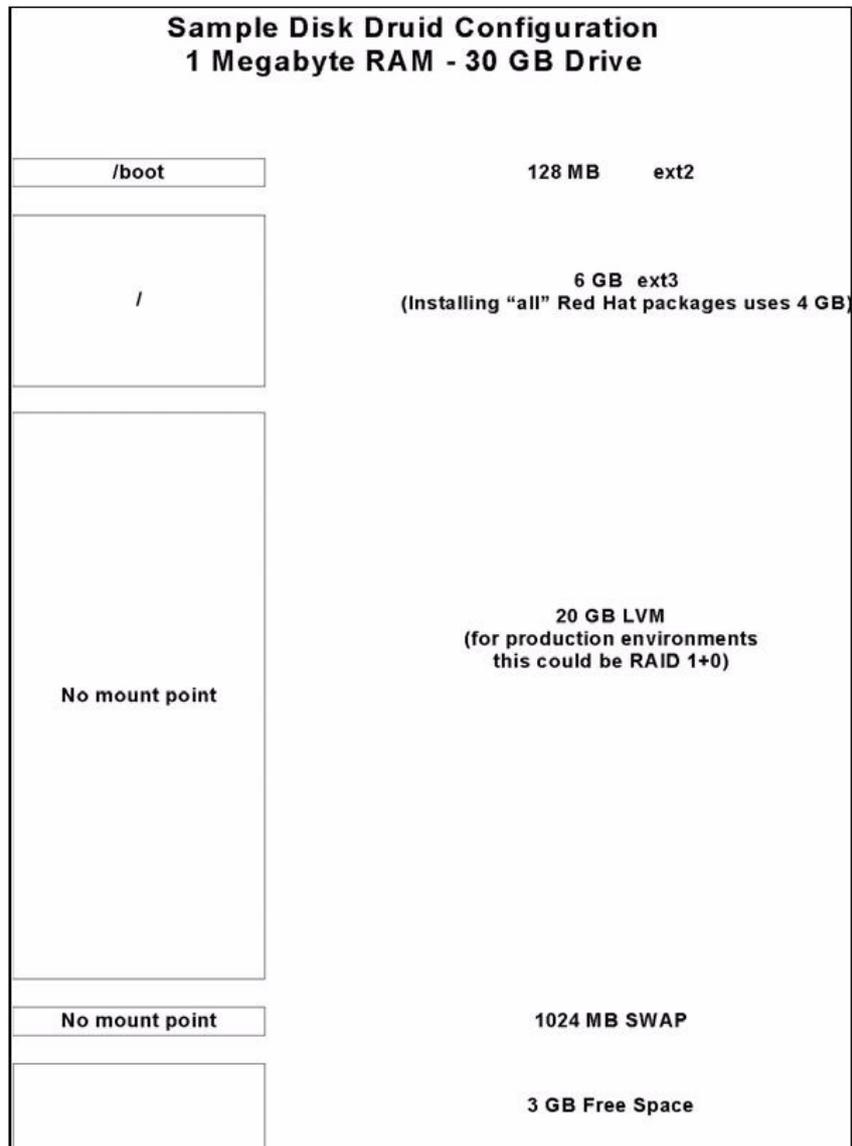
Configuring Scalix for Full LVM Backups

If you intend to use LVM to make a snapshot of the system for backup purposes, all Scalix servers must be configured with specific mount points. If you did not do that when installing the server, do it now.

The following diagram displays one configuration on Red Hat. There was 30 GB of storage available at installation and 20 are now allocated for LVM. The mount points are not established until further configuration is done.

Note

Actual configuration of production servers typically involves more disks and overall storage.



To configure a Scalix server with mount points for LVM

- 1 Take a look at the disk configuration using the fdisk command:

```
fdisk -l
```

which returns something like

```
Disk /dev/hdc: 30.0 GB, 30005821440 bytes
255 heads, 63 sectors/track, 3648 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Device Boot      Start      End  Blocks  Id System
/dev/hdc1  *           1        16   128488+  83  Linux
/dev/hdc2             17       147   1052257+  82  Linux swap
/dev/hdc3          148      2696   20474842+  8e  Linux LVM
```

```

/dev/hdc4          2697      3648   7646940    f  win95 Ext'd (LBA)
/dev/hdc5          2697      3345   5213061    83  Linux

```

- Execute the command `vgscan`. This scans all disks for volume groups and builds the files `/etc/lvmtab` and `/etc/lvmtab.d/*`. These files are the databases for all other LVM commands.

```
vgscan
```

which returns something like

```

Reading all physical volumes. This may take a while...
vgscan--"/etc/lvmtab" and "/etc/lvmtab.d" successfully created
avgscan--WARNING: This program does not do a VGDA backup of your volume group

```

- Execute the command `pvcreate` with the path to use, to initialize a disk or partition for use by LVM:

```
pvcreate /dev/hdc3 -ff
```

where you substitute your LVM disk or partition for `hdc3`. The command returns something like

```
pvcreate -- physical volume "/dev/hdc3" successfully created
```

- Create a volume group with the command `vgcreate`:

```
vgcreate vgscalix /dev/hdc3
```

which returns

```

vgcreate -- INFO: using default physical extent size 4 MB
vgcreate -- INFO: maximum logical volume size is 255.99 Gigabyte
vgcreate -- doing automatic backup of volume group "vgscalix"
vgcreate -- volume group "vgscalix" successfully created and activated

```

- If it is not already there, create the Scalix folder under the directory `/var/opt`. During subsequent installation of Scalix, it correctly recognizes this folder, where it then installs and creates all appropriate files and subfolders.

```
mkdir scalix
```

- Execute the command `lvcreate` to create a logical volume in an existing volume group. From our original 20 GB, we create a 10 GB logical volume `lvscalix` in the `vgscalix` volume group.

```
lvcreate -L10000M -nlvscalix vgscalix
```

which returns

```

lvcreate -- doing automatic backup of "vgscalix"
lvcreate -- logical volume "/dev/vgscalix/lvscalix" successfully created

```

- Run the `mkfs` command. This creates a new file system on a specified device and initializes the volume label, file system label, and startup block.

```
mkfs -t ext3 /dev/vgscalix/lvscalix
```

which returns

```
mke2fs 1.32 (09-Nov-2002)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
1281696 inodes, 2560000 blocks
128000 blocks (5.00%) reserved for the super user
First data block=0
79 block groups
32768 blocks per group, 32768 fragments per group
16224 inodes per group
Superblock backups stored on blocks:
32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632
writing inode tables: done
Creating journal (8192 blocks): done
writing superblocks and filesystem accounting information: done
```

- 8 This file system is automatically checked every 28 mounts or 180 days, whichever comes first. Use `tune2fs -c` or `-i` to override that.

```
mount /dev/vgscalix/lvscalix ~/s
vi /etc/fstab (add the line at the bottom)
```

which returns

```
LABEL=/          /          ext3  defaults    1 1
LABEL=/boot     /boot     ext2  defaults    1 2
none           /dev/pts  devpts gid=5,mode=620 0 0
none           /proc     proc  defaults    0 0
none           /dev/shm  tmpfs  defaults    0 0
/dev/hdc2      swap      swap  defaults    0 0
/dev/cdrom /mnt/cdrom  udf,iso9660 noauto,owner,kudzu,ro 0 0
/dev/vgscalix/lvscalix ~/s ext3  defaults    1 3
```

- 9 Now mount it:

```
mount ~/s
```

Performing the Full Backup

Every backup is different. The specifics vary by the server setup, the method, the size of the data files and more. So no single script covers all scenarios.

One example of a backup script is outlined here. This script takes daily snapshots of the data volume in the message store and then mounts it for backup. It can be invoked by a cron job or backup software.

You can get a backup script at

http://www.scalix.com/wiki/index.php?title=Admin_Resource_Kit

A suggestion is to use this backup script and the example provided here.

Sample script for daily message store backups

1 Set up paths and variables:

```

LVGRP=/dev/vgscalix
SXLV=lvscalix
BULV=sxbackup
LVSIZE=20G
MNTPT=/mnt/sxbackup
LOGRCPT=
DEVICE=/backup

SXBIN=/opt/scalix/bin
LVBIN=/sbin
BIN=/usr/sbin
LOG=/tmp/sxbackup.log
DAY=`date +%F`

touch $LOG

if [ -z "$LVGRP" ];
then
    echo "The Logical Volume Group Variable (LVGRP) has not been set"
    exit
fi

if [ -z "$SXLV" ];
then
    echo "The Scalix Volume variable (SXLV) has not been set"
    exit
fi

if [ -z "$BULV" ];
then
    echo "The Backup Volume variable (BULV) has not been set"
    exit
fi

if [ -z "$LVSIZE" ];
then

```

```

    echo "The Backup Volume Size Variable (LVSIZE) has not been set"
    exit
fi

if [ -z "$MNTPT" ];
then
    echo "The Mount Point Variable (MNTPT) has not been set"
    exit
fi

if [ -z "$LOGRCPT" ];
then
    echo "The Log Recipient Variable (LOGRCPT) has not been set"
    exit
fi

if [ -z "$DEVICE" ];
then
    echo "The Tarball Directory Variable ($DEVICE) has not been set"
    exit
fi

#
#
sxbck_begin ()
{
    date > $LOG

    echo "Taking snapshot & Mounting Scalix Data Volume"|tee -a $LOG

```

- 2 Verify that the mount point exists. If it does not, create it. (This code is also in the backup script.)

```

if ! test -d "$MNTPT"
then
    mkdir $MNTPT >> $LOG 2>&1

```

- 3 Verify that the mount point was created, if not exit:

```

if ! test -d "$MNTPT"
then
    echo "!! Error creating the $MNTPT directory"|tee -a $LOG
    exit
fi
fi

```

- 4 Suspend Scalix and synchronize the disks:

```

echo "Suspending writes to Scalix"|tee -a $LOG
$SXBIN/omsuspend -s 10&
/bin/sync

```

```

echo "Creating the Logical volume $LVGRP/$SXLV"|tee -a $LOG

```

```
# create the snapshot volume and mount it
$LVBIN/lvcreate -L $LVSIZE -s -n $BULV $LVGRP/$SXLV >> $LOG 2>&1

echo "Enable writes to Scalix"|tee -a $LOG
# release the suspend
$SXBIN/omsuspend -r

echo "Mount $LVGRP/$BULV to the Mount Point $MNTPT"|tee -a $LOG
# mount the snapshot volume
mount $LVGRP/$BULV $MNTPT >> $LOG 2>&1
```

5 This next section uses tar. We recommended you use something more robust in case you need to do a single user restore. If you do that, comment this section out and have the backup software execute.

6 Do a “sxsnapshot -begin” before backing up and “sxsnapshot -end” upon completion of the backup.

7 If you want to back up directly to tape, set DEVICE to something like this:

```
#DEVICE=/dev/rmt0
```

8 Back up to tape device:

```
echo "tar to device $DEVICE.$DAY.tar the contents of $MNTPT..."|tee -a
$LOG
tar cf $DEVICE.$DAY.tar $MNTPT >> $LOG 2>&1
```

9 If the device is a file system, then compress it:

```
echo "gzip'ing the $DEVICE.$DAY.tar file..."|tee -a $LOG
gzip -f $DEVICE.$DAY.tar >> $LOG 2>&1
```

10 This ends the commented section. If you did use tar, resume from here.

```
}

sxback_end ()
{

    #Unmount backup file system
    echo |tee -a $LOG
    echo .....|tee -a
$LOG
    date >> $LOG
    echo "Unmounting Scalix Backup volume"|tee -a $LOG
    umount $MNTPT >> $LOG 2>&1
    echo "Removing the snapshot logical volume"|tee -a $LOG
    $LVBIN/lvremove -f $LVGRP/$BULV >> $LOG 2>&1
```

11 Send the result to the Administrator. Configure a .forward file in the root home directory and forward all mail to the error manager (sxadmin by default). Identify the user account that functions as the error manager to receive error notification e-mails with the omshowenu command.

```
echo "Mailing the report to $LOGRCPT"|tee -a $LOG
mail -s "Scalix Backup Results" $LOGRCPT < $LOG
```

```

}
usage ()
{
    echo "USAGE: $0 [ -begin | -end ]"
    exit 1
}

if [ $# -ne 1 ]; then usage; fi
case $1 in
    -begin)    sxback_begin ;;
    -end)     sxback_end  ;;
    *)        usage      ;;
esac

```

Performing Incremental Backups

After performing an initial baseline backup, you can use a variation on the synchronization command to back up changes. This is faster and results in a smaller backup file size than redoing a full backup.

The general syntax when using `rsync` is:

```
rsync -options source target
```

Alert

Mixing up source and target options can cause critical problems.

Deletions do not replicate with synchronization, so when using this method for backup, some deletions are not reflected in the backup tape. To make sure that they do, use the `--delete` command.

You can use the synchronization command to back up the changes on the same server or a different server.

To back up changes on a single server

- 1 Run the following command:

```
rsync -avz --delete /var/opt/ /backup
```

This recursively copies all files from the `/var/opt` folder to the `/backup` folder. The files transfer in “archive” mode, which ensures that symbolic links, devices, attributes, permissions, ownerships, and so on are preserved. In addition, compression is used to reduce the size of data portions.

In this example, the `/backup` folder contains a `/scalix` folder (with all subfolders), and perhaps a `/jakarata-tomcat-5.0.2x` directory (with all subfolders). This means that the `/var/opt` partition must have as much space available as is stored in the contents of `/var/opt/`, which is typically rare. Run it initially, then run it again, notice the second time that only a few files copy. Write a message into a mailbox on Scalix, run it again, and notice more files copy from the `/user` and `/data` folders.

To back up changes to a different server

- 1 Run the following command:

```
rsync -avz --delete /var/opt/ backup.company.local:backup
```

This does the same as the previous procedure, only it copies to the `/backup` directory on the host “`backup.company.local`”. The `backup.company.local` host is NFS-mounted from the Scalix server. On the backup computer you can then set a nightly cron job to build a day-of-week .tgz file to another area, which is backed up to tape weekly.

Performing Export/Import Backups to Back Up Individual Mailboxes

An alternative to full backup is to use the export/import method by which you store and restore individual users’ mailboxes. Using this method, you back up individual mailboxes or public folders as separate files. That includes all attachments, referenced items, and so on.

The advantage to this method is that the export file is easier to handle. You can copy it, move it around, import it, and more.

The disadvantage is that the sum file size of all individual mailbox backups can be as much as two times larger than the sum total of a full backup procedure. The reason is the way Scalix stores items. Consider the example of an attachment sent to 10 people. In Scalix, the attachment does not replicate in 10 mailboxes. Rather, the 10 mailboxes contain pointers to one single copy of the attachment, which is housed in the message store on the Scalix server. So when you export individual mailboxes and all of their contents, that attachment is repeated 10 times. This increases the size of the backup significantly and can be prohibitive in large enterprise systems.

Tip

The export/import procedure is also helpful for migrating users from one server to another.

Exporting

Exporting copies the contents of a user’s mailbox or a series of public folders into one, single archive file. This can include e-mail messages, calendar items, contacts, public folder contents, and user settings. E-mail, calendars, and address books are backed up when you back up an individual user account.

To export a mailbox

- 1 Make sure the user is logged out.
- 2 Create a folder to back up to, for example `/backup` or `/var/opt/scalix/<nn>/backup`
- 3 On the server on which the user’s mailbox is stored, run the export command, specifying the name of the user whose mailbox you want to back up and the backup folder.

```
sxmbosexp --u “User Name” -a /backup/<mailboxname>.mbox
```

where `<mailbox name>` takes the form of first initial and last name (jsmith). For example

```
sxmbosexp --u “Jane Rogers” -a /backup/jrogers.mbox
```

or

```
sxmailboxexp -u "Jane Rogers" -a /var/opt/scalix/jrogers.mbox
```

Importing

Once you have exported individual mailboxes or public folders, you can import them to restore data. This is especially helpful if one of your users deletes a large amount of data or experiences corruption that requires a reset to a previous point in time. It is also useful for migrating a complete mailbox.

To import a mailbox

- 1 Make sure the user is logged off.
- 2 On the server on which the user's mailbox is stored, run the import command, specifying the name of the archive file you want to import. It must be an archive file created through the export procedure outlined in the previous section or the command `omcpoutu`. By default, the data is restored to a mailbox with the same name as the original stored data, but with the `--user` option, you can target any existing mailbox.

```
sxmailboximp -a /backup/<mailbox name>.mbox
```

where `<mailbox name>` takes the form of first initial and last name (jsmith).

You can do selective imports. To import all folders with the exception of one, use the command

```
sxmailboximp -a /backup/<mailbox name>.mbox --exclude F-<folder ID>
```

(To get the ID number for the folder you do not want to import, use `sxmailboxlist`.)

To import two folders, use the command

```
sxmailboximp --archivefile /backup/<mailbox name>.two --folder F-<folder ID> --folder F-<folder ID>
```

To restore a single public folder, use the command

```
sxmailboximp -a /backup/public.folders -f F-<folder ID>
```

Restoring the Full System

Full disaster recovery returns the entire system by building a new server. That includes all mailbox data, public folders, folders, and configurations.

For more on disaster recovery, contact Scalix.

Restoring a Single User's Mailbox

If one of your users experiences corruption in some part of his or her message store, you can restore just that mailbox. There are two methods for single-user recovery:

- Full backup method
- Export/import method

To restore a single user's mailbox from a full backup

- 1 Restore the full backup to a secondary server using whatever tool you used to archive the backup (such as tar).
- 2 Extract the specific mailbox data from the secondary server using the `sxmbosexp` command.
- 3 Copy it in to the live server using the `sxmbboximp` command.

To restore a single user's mailbox from an export backup

- 1 If you have an export of the user's mailbox using the `sxmbosexp` or `omcpoutu` command, you can do an import procedure to restore a single user's data. See "Importing" on page 110.

Managing Public Folders

This chapter covers how to configure, access, synchronize, and maintain public folders. It also outlines how to set public folder permissions and assign e-mail addresses to the folders.

Contents

This chapter includes the following information:

- “Public Folder Overview” on page 113
- “Creating Public Folders” on page 114
- “Listing Public Folders” on page 115
- “Permissions for Public Folders” on page 116
- “Maintaining Public Folders” on page 119
- “Assigning E-mail Addresses to Public Folders” on page 119
- “Synchronizing Public Folders” on page 120
- “Forwarding Public Folder Items” on page 124
- “Posting to Public Folders by E-mail” on page 124
- “Commands” on page 125

Public Folder Overview

Public folders are similar to shared folders. They enable sharing of information, such as documents, e-mail messages, or calendars with other users. You can organize them by common interests, team projects, departments, or any other need. They also are useful for sharing meetings, appointments, or contacts. For example, you can give people access to weekly meeting information or to view and add to a list of contacts used within your company.

Within the Scalix system, public folders are shared areas in the Message Store. Users can add items to them by cutting and pasting, dragging and dropping, sending mail messages to the public folder, and so on.

Public folders can contain the following items:

- E-mail messages
- Documents, such as spreadsheets, text, or word-processing files
- Calendars
- Contacts
- Other (“nested”) public folders

Public folders can be set up with permissions to restrict access to certain users or classes of user. In addition, expiry dates can be set so that short-lived information is automatically deleted after a specified period.

Only Premium user accounts can use public folders. The default sxdadmin account is a Standard user. Standard users do not see the public folders and cannot create them.

Scalix commands and directories use the term “Bulletin Board” and the abbreviation “bb” to refer to public folders.

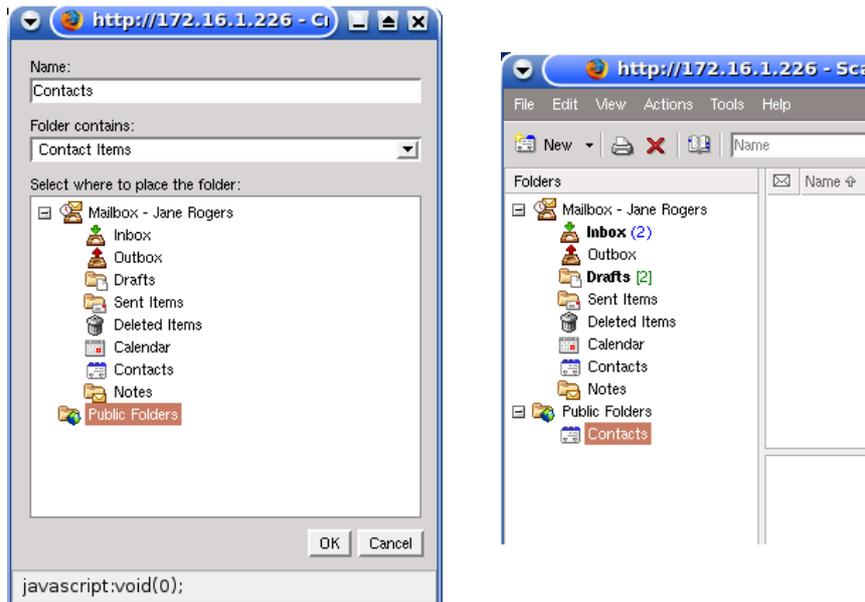
Creating Public Folders

You can create public folders as a Premium user in a client, such as Scalix Web Access, or as root at the command line. You cannot create a public folder within a POP or IMAP e-mail application, such as Thunderbird, or as a Standard user. When you, as a Premium user, view a public folder in a POP or IMAP application such as Thunderbird, you can view the public folder, for example contact phone numbers for a Contacts public folder, but you cannot add to that public folder in Thunderbird.

Note The creator of a public folder gets full read, write, edit, modify, and delete capabilities by default. When you add a public folder by command line, there is no owner.

To create a public folder in Scalix Web Access

- 1 Click **File > New > Folder**. In the window that appears, type a name for the entry, select an option from the drop-down list (e-mail and posts, contacts, or calendars), then click **Public Folders** to create it there.
- 2 Click **OK** to exit from the window and create the folder.



To create a public folder using commands

- 1 To create a top-level folder, run the following command:

```
omaddbb -s <"Folder Name">
```

for example

```
omaddbb -s "Engineering Offsite"
```

- 2 Set the permissions level for this folder. See "Setting Public Folder Permissions" on page 117.
- 3 To create a subfolder under that one, use the following command. This is a second-level folder.

```
omaddbb -m "TOP" -s <"Folder Name">
```

- 4 To create another subfolder under the second level, use the following command. This is a third-level folder. The delimiter between the top level and the next level is the > angle bracket that appears after the word "TOP".

```
omaddbb -m "TOP><Folder Name>" -s <"Folder Name">
```

where the first folder name is the name of the parent and the second is the name of the new folder you are creating.

Note

When adding public folders, you can set expiration dates for the contents. See "Maintaining Public Folders" on page 119 or the omaddbb MAN page.

If Premium users cannot access public folders, ensure that the IMAP_PUBLIC_FOLDERS option in the `/var/opt/scalix/<nn>/s/sys/general.cfg` file is not set to FALSE.

Listing Public Folders

You also can list public folders.

To list public folders

- 1 Run one of the following commands.

For top-level folders – `omlistbbs`

For all levels of folders – `omlistbbs -d 0`

where the options are those listed in the table.

Table 1: Options for the Public Folder List Command

Option	Description
-m	The name of the folder (match), within quotes, to list.
-d	The number of levels (depth) to list. The default is 1. To list all levels below the current one, specify a depth of 0.
-s	Display the size of the public folder in KB.
-S	Display whether a permission file is associated with the folder. A "+" character at the end of the folder's line means one is.

The output looks similar to the following, where public folders called Contacts and Public 1 have been created:

0 BULLETIN BOARD AREA	(no owner)
1 Contacts	Jane Rogers/scalix1
2 Public 1	(no owner)

Permissions for Public Folders

Access to public folder functionality depends on the permissions of the clients. The level of access any single user is granted determines whether they can see a folder, read its contents, change those contents, add to them, or delete from them.

Anybody who sets up a folder hierarchy can assign other users access to manage their folders and subfolders. And those managers can, in turn, assign permission levels for the folders and subfolders they own.

By default, subfolders assume the permissions of the parent folder, and these settings can be changed.

The four levels of permission are:

- Read
- Write
- Edit
- Delete

These levels of permission are combined into two roles.

The user roles are:

- **Default** – Has read permissions on all folders
- **Local Users** – Has read, edit, and delete permissions on folders that are stored on their server
- **Scalix Administrators** – Has read, write, edit and delete permissions on all folders

Specific roles are:

- **None** – Cannot read, write, edit, or delete
- **Contributor** – Can create items and see folders, but cannot edit or delete
- **Reviewer** – Can read items and see folders, but cannot edit or delete
- **Non-editing author** – Can create and read items as well as see folders, but cannot edit or delete
- **Author** – Can create and read items as well as see folders. Can edit and delete those items they created themselves.
- **Publishing author** – Can create and read items, see folders, and create subfolders. Also can edit and delete those items they created.
- **Editor** – Can create and read items, and see folders. Can edit and delete those items they created themselves and any items in their principal's mailbox.
- **Publishing Editor** – Can create and read items, see folders, and create subfolders. Also edit and delete those items they created themselves and any items in their principal's mailbox.

- **Owner** – Can create and read items, create subfolders, and acts as the owner of folders. Also edit and delete those items they created and any items in their principal's mailbox.
- **Custom** – Any combination of creating, reading, and viewing messages, folders, or calendar items

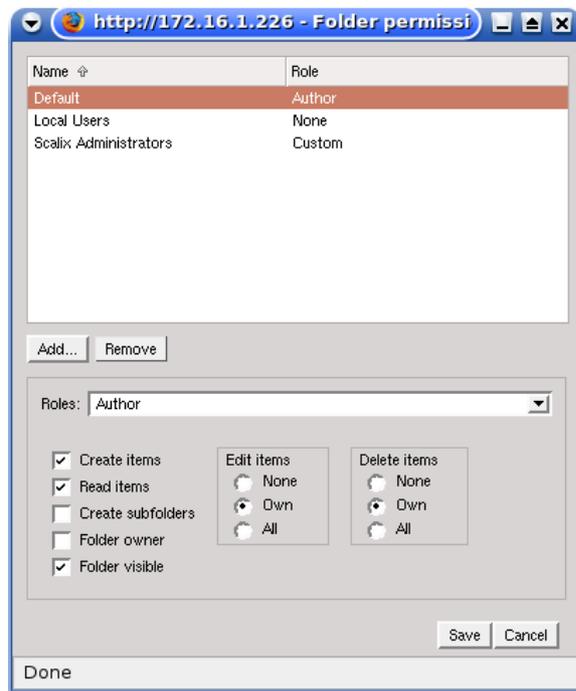
Setting Public Folder Permissions

By default, the owner of a public folder can read, write, edit, and delete items while everybody else can read them. There are two ways to change permissions:

- Client
- Command line

To set permissions in Scalix Web Access

- 1 Right-click the public folder and select **Edit Permissions**. A permissions window opens.



- 2 At the top of the window, select the role you want to set permissions for: default author, users, or Scalix administrators.
- 3 At the bottom of the window, set the permissions by selecting a specific role from the drop-down list and/or enabling/disabling check boxes. For example, for a public contacts folder, you want everyone to be able to read, add, edit, and delete items, and you want the folder to be visible.
- 4 Click **Save** to apply the changes and exit from the window.

To set permissions using commands

- 1 Run the following command:

```
omaddacln -t bulletin -l <"Folder Name"> -c update
```

where some of the options are outlined in the table.

Table 2: Options for Permissions Commands

Option	Description
-t	The resource type, which in this case is bulletin, short for bulletin board or public folder
-l	The name of the resource, which in this case is the name of the folder for which you want to set permissions or the path. An example of the path is "Top <Folder Name>"
-c	The capabilities you want to set, which can be: s — see r — read u — update d — delete m — modify

Other commands that relate to permissions are shown in the following table. All take the same options outlined in the previous table. For more on options, see each command's MAN page.

Table 3: Commands for Setting Permissions on Public Folders

Option	Description
omaddacln	Adds capabilities for users to an Access Control List (permissions) for a specific resource. The capabilities are a combination of those given to the user based on the O/R address and any groups to which they belong. To use this command, you must have root or configuration capability.
omshowacl	Displays (shows) the contents of an Access Control List (permissions), showing the capabilities given to specific users for specific folders. To use this command, you must have root or configuration capability.
omdelacl	Deletes an Access Control List (permissions). To use this command, you must have root or configuration capability.
omchkacln	Displays (checks) the capabilities of a user in an Access Control List (permissions).

Maintaining Public Folders

To prevent public folders from becoming too large or irrelevant, you can delete items individually or in bulk, remove outdated items, or configure the system to automatically remove items after a certain period of time has elapsed.

There are many ways to do this:

- **Delete individually or in bulk** — Deletes all public folders or items from a public folder or its subfolders
- **Expiry date** — Deletes all contents of the folder automatically on a designated date
- **Expiry delay** — Deletes all contents of the folder automatically after a specified period of time has elapsed since the last modification to that folder

To delete items from a public folder either individually or in bulk

- 1 Use the following command:

```
ommaintbb
```

where the available options are outlined in the table.

Table 4: Options for the Public Folder Maintenance Command

Option	Description
-a	Delete all public folders.
-m	Delete items from the public folder by the name <"Folder Name">
-e	Delete items added to the public folder more than <number of> days ago.
-A	Age items in that public folder.
-R	Perform the delete action (-A or -e) to all subfolders of this folder.

Assigning E-mail Addresses to Public Folders

If you want users to e-mail items to public folders (instead of or in addition to the drag-and-drop method), you can assign e-mail addresses to those folders.

To use a plug-in to create a public folder and assign an e-mail address to it, see "Creating a Public Folder and Optionally Assigning it an E-mail Address" on page 95.

To assign an e-mail address to a public folder

- 1 At the omaddent command, add an e-mail entry to the system directory for that folder. Assuming the folder is called "Top Level", the command is:

```
omaddent -e "S=+BB/CN=Top Level/OU1=mailnode/DDT1=BB-NAME/DDV1=Top Level/IA=top.level@domain.com"
```

If the public folder name contains non-ASCII characters, such as Japanese characters or German umlauts, use DDV1-TX instead of DDV1. In this scenario, the command is:

```
omaddent -e "S=+BB/CN=Top Level/OU1=mailnode/DDT1=BB-NAME/DDV1-
TX=Ümläutfolder/IA=top.level@domain.com"
```

- 2 To add an entry for a lower-level folder, for example Top Level>Second Level, the command is:

```
omaddent -e "S=+BB/CN=Second Level/OU1=mailnode/DDT1=BB-NAME/DDV1=Top
Level>Second Level/IA=second@domain.com"
```

where the folder separator is a ">" character.

Synchronizing Public Folders

Public folder synchronization is the process of automatically updating public folders and their contents from one system to another. It ensures that when you add an item to a public folder, the same item is also added to all equivalent public folders in the network.

Synchronization is accomplished using synchronization agreements. These define the rules of each exchange. Each agreement defines whether items are imported or exported and the public folders to which the agreement applies. All items within the hierarchy of the public folder are included in the agreement.

Synchronization is performed by exchanging mail messages between two public folder servers (BB servers). Each message adds one item to a public folder. The "sending" server is the public folder system that exports the BB server, the "receiving" server is the one that imports.

Alert

Before synchronizing public folders on two Scalix servers, you must have set up routes between the two. For more on how to establish routes between servers, see the Routing Mail section in the *Scalix Setup and Configuration Guide*.

The items on Server A are master items, because they were originally created on Server A. The same items on Server B are secondary items, because they are copies of the master. Whether an item is a master or a secondary is important when deleting or modifying items.

In cases of three or more public folder setups, one must be appointed as the master and all others must synchronize with that one.

Creating Folder Synchronization Agreements

Matching agreements must exist on the exporting and importing systems before items can be exchanged. Typically, a number of agreements are specified on each system, with each agreement specifying the exchange for several public folders.

Note

The deletion of public folders is not replicated across servers during synchronization. If you delete the Sales public folder on Server A, the Sales public folder on Server B is not deleted. You have to remove it manually. For the contents of public folders, deletion of items from the master server replicates, but deletion of items from the secondary does not.

Use the following guidelines when setting up synchronization agreements:

- Activate the importing synchronization agreement before activating the remote exporting agreement. This prevents exported items from arriving at the importing system before it can accept them.

- With a two-way import/export agreement, activate the corresponding agreement on the remote system at the same time
- If the primary mailnode on a system changes, all agreements (both import and export) must reflect the new mailnode name
- Use the wildcard character (*) when specifying the subjects of top-level public folders to import or export. This avoids adding individual agreements for each folder. Indiscriminate use can lead to significantly increased network traffic.

Wildcard characters represent zero or more characters. One or more wildcard characters can be placed anywhere in the subject string. If using a multibyte character set, wildcards can be placed only at the beginning and end of the subject string. Also, the output from the Scalix commands displays multibyte characters as asterisks, so users cannot distinguish between a subject containing wildcards and one containing multibyte characters.

Synchronization Prerequisites

The following minimum-level access capabilities are required to import items:

- The originator of the message (the exporting server) has use access on the importing server
- The originator of the message (the exporting server) has read access to the public folder area and attach and delete access to the folder being synchronized
- If the top-level public folder does not already exist, then the originator of the message must have attach and delete access to the public folder area

Synchronization and Permissions

After a synchronization:

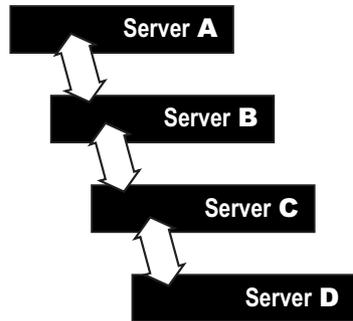
- Synchronization messages (type OMSYNC) are automatically given the capabilities of the admin and default groups in addition to any permissions explicitly granted to the originator/recipient address (O/R address) pattern of the originator. An O/R address is an attribute list that distinguishes a user or distribution list from another and defines the user's point of access to the message handling system or the distribution list's location. Examples of O/R attributes are the code C for country and S for surname.
- The minimum access permissions required to export items are the combined permissions of the standard groups local, default and admin plus any permissions explicitly granted to the O/R address pattern of the originator (OMSYNC +BB/local_primary_mailnode) must give read access to the public folder area and the public folders being synchronized.
- The public folder permissions themselves are not exported when public folders are synchronized. New top-level public folders created as a result of a synchronization agreement using the default settings. New subfolders created from synchronization agreements inherit their permissions from their parent.

Synchronization Topologies

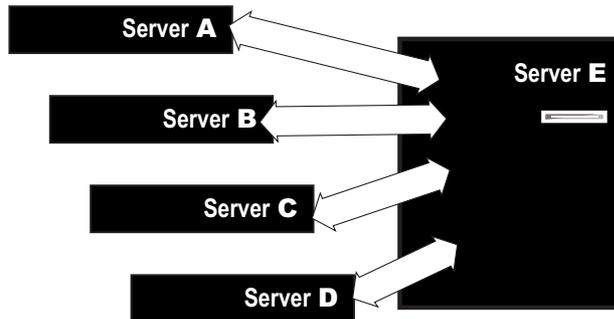
Public folders can be synchronized two ways:

- Chains – Each server passes new items to the next in the chain
- Hubs – Every server receives updates from one central server

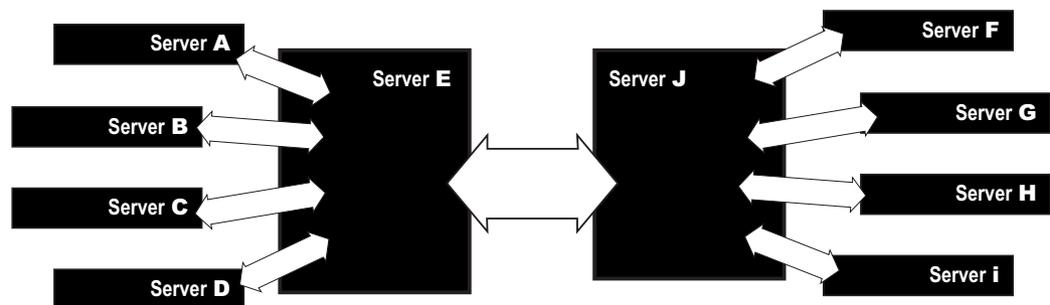
In a chain, a user adds an item to a public folder on Server A. This item is replicated to the equivalent folder on Server B, and then to Servers C and D.



In a hub, all changes are communicated to Server E, which propagates them to the other servers.



A hub can be extended to a linked hub (Server J).



Other Synchronization Topologies

There are a number of other synchronization topologies. Some are complex to administer, can cause network congestion, and might not give the required results. For example, grids (where all systems are updated by each other) and loops (linked chains) can result in duplication of synchronization messages and lead to a loss of synchronization.

A Sample Synchronization Agreement

The basic commands used for synchronization are `omaddbbsa`, `omdelbbsa`, `ommodbbsa`, and `omlistbbsa`.

Because there are many ways to set up a synchronization agreement, no one procedure works for every situation. This is an example of the most basic, two-way synchronization agreement.

To run a simple, two-way public folder synchronization agreement

- 1 Set up an import (-i) agreement on one server and an export (-e) agreement on the other by running the following commands, each on its own server. Although not shown here, you can create combination import/export agreements.

On Server A: `omaddbbsa -i y -m "OMSYNC +BB/serverB,mailnode" -s "BB subject"`

On Server B: `omaddbbsa -e y -m "OMSYNC +BB/serverA,mailnode" -s "BB subject"`

To do this the other way around:

On Server A: `omaddbbsa -e y -m "OMSYNC +BB/serverA,mailnode" -s "BB subject"`

On Server B: `omaddbbsa -i y -m "OMSYNC +BB/serverB,mailnode" -s "BB subject"`

- 2 In the `/var/opt/scalix/<nn>/s/sys/general.cfg` file, change the default interval from one hour to a smaller time period such as one minute. The following example shows one minute.

```
BBS_CUST_CHECK_TIME=1
```

- 3 Enable auditing to see the messages transfer between computers, and restart the synchronization service:

```
omconfaud bbs 15
omoff -d 0 -w bbs; omon bbs
```

- 4 To check that mail is flowing correctly, review the messages in the `/var/opt/scalix/<nn>/s/logs/audit` folder.
- 5 Repeat as needed until all folders have synchronization agreements.

Forwarding Public Folder Items

If you have Scalix public folders co-existing with a legacy system, such as Microsoft Exchange or Lotus Notes, you can configure Scalix to forward any public folder postings to the legacy system's public folders. This sends a copy of every message posted to Scalix to the similarly-named folder on Microsoft Exchange or Lotus Notes.

This forwarding arrangement creates a directory entry associated with the public folder and creates an SMTP address to receive inbound mail. After creating that directory entry, you must provide a “forward to external address” option in the Scalix public folder synchronization mechanism.

Alert

Migrate Microsoft Exchange public folder data to Scalix before enabling auto-forwarding. If you do not, you see duplicate messages in Scalix folders.

Note

This procedure provides functionality equivalent to the Microsoft Exchange public folder forwarding rule. That is, only new public folder messages are synchronized. Modified and deleted messages are not.

To forward public folder postings to a legacy system

- 1 Run the following command:

```
omaddbbsa -f <Forwarding Address> -s <Public Folder Name>
```

Posting to Public Folders by E-mail

You can enable a public folder to receive mail with an Internet address so that users from outside can post to it.

To post to a public folder by e-mail

- 1 Run the following command:

```
omaddent -e "S=+BB/CN=ABC/OU1=sxhost1/DDT1=BB-NAME/DDV1=KCI/IA=abc-post@yourcompany.com"
```

where ABC is the name of the public folder and sxhost1 is the mailnode. This enables people to send to abcpost@yourcompany.com and it goes directly into the folder.

If the public folder name contains non-ASCII characters, such as Japanese characters or German umlauts, use DDV1-TX instead of DDV1.

Commands

The following table lists commands associated with public folders. See also Table 3, “Commands for Setting Permissions on Public Folders,” on page 118.

Table 5: Public Folder Commands

Command	Description
omaddbb	Add a top-level public folder. Example: omaddbb -s “Public 2” to add a public folder called Public 2 The public folder has no owner when you add it using the command line.
omdelbb	Delete a top-level public folder. Example: omdelbb -m “Public 2” to delete a public folder called Public 2.
omlistbbs	List top-level public folders.

Table 5: Public Folder Commands

Command	Description
ommaintbb	Maintain top-level public folders by deleting items, for example when they are a number of days old (-e option). Example: ommaintbb -a -e 30 to delete items added more than 30 days ago from all public folders.
ommodbb	Modify a top-level public folder, such as its name or expiry date.
omshowbb	Show details of a top-level public folder, such as owner, expiry date, and size. Example: omshowbb -m "Public 1" to show information about a public folder called Public 1.
omaddbbsa	Add a public folder synchronization agreement. See earlier examples.
omdelbbsa	Delete a public folder synchronization agreement.
omlistbbsa	List public folder synchronization agreements.
ommodbbsa	Modify a public folder synchronization agreement.

Using Access Control Lists

This chapter describes Access Control Lists (ACLs) that control user access to Scalix resources, such as public folders, directories, scripts, and services.

The following topics are detailed:

- “About Access Control Lists” on page 127
- “Creating Access Control Lists” on page 127
- “Commands” on page 130
- “ACL Address Patterns” on page 131
- “Combining Users and Permissions” on page 133

About Access Control Lists

You can create ACLs to limit permissions for services, scripts, public folders, and directories. ACLs list users and the permissions they have for any given resource.

While ACLs for services, scripts, and directories are created and removed using commands, such as `omaddacl` and `omdelacl`, ACLs for public folders and directories are created and deleted automatically when a folder or directory is either created or deleted.

In Scalix ACLs, users can be listed by standard groupings or originator recipient (O/R) addresses. The standard groupings are local administrators (`admin`), local users (`local`), and everyone/default (`default`). Additionally, specific users can be added to a list by their O/R address or grouped more efficiently using “wildcards” in place of specific address attributes. An O/R address is an attribute list that distinguishes a user or distribution list from another and defines the user’s point of access to the message handling system or the distribution list’s location. Examples of O/R attributes are the code `C` for country and `S` for surname. Each entry in an ACL refers either to a standard group or to an O/R address pattern.

Every resource has configuration permission, that is, the permission to modify the ACL. This permission is always given to the standard group “local administrators” (and the root user) when the ACL is created. It can be changed later.

The ACL configuration file is named `acl.cfg` and is in the following location:

```
/var/opt/scalix/<nn>/s/sys/acl.cfg
```

The ACLs themselves are located in folders under:

```
/var/opt/scalix/<nn>/s/acl
```

Creating Access Control Lists

The methods for creating service, script, public folder, and directory ACLs differ in subtle ways. There are a few commands that apply to all, as follows.

You can create an ACL using the command:

```
omaddacl -t <type> -l <name>
```

where

- <type> is the kind of resource, such as service, script, public folder, or directory
- <name> is the name you give to this list

The following table lists the resource “types” available. For the command, you use the type shown, for example service or bulletin, or the abbreviation, for example bb. These resource types are defined in the acl.cfg file.

Table 1: ACL Resource Types

Resource	Type	Abbreviations	Value
Services	service	svc	s
Request Server Scripts	request	req	r
Public Folders	bulletin	bb	b
Directories	directory	dir	d
Print Servers	printer	prt	p

The name of an ACL depends on its resource type. The following table lists how ACL names are determined. Names can be enclosed in quotes, to allow spaces for example.

Table 2: ACL Naming Conventions

Resource	Name Determined By...
Services	The queue name of the service.
Request Server Scripts	The file name of the request as listed in the <i>/opt/scalix/req</i> folder.
Public Folders	The temporary or absolute reference number of the public folder as listed by the <i>omlistbbs</i> command. (Use 0 for the public folder area itself.)
Directories	The name of the Directory as listed by the <i>omlistdirs</i> command.
Print Servers	

Service ACLs

You can add a user to a service ACL using the command:

```
omaddacln -t service -l <queue_name>
```

Directory ACLs

You can add a user to a directory ACL using the command:

```
omaddacln -t directory -l <directory_name>
```

Public Folder ACLs

Public folder ACLs are handled differently. In Microsoft Outlook, most public folder access settings can be handled through the Microsoft Outlook client. Elsewhere, they can be set on the command line.

Whether in Microsoft Outlook or another mail client, ACLs have “implicit” permissions unless otherwise specified. That is, they inherit their permissions from the parent folder unless stated otherwise by creating new “explicit” permissions. Explicit permissions added later overwrite the implicit permissions.

When you delete a public folder’s permissions, its ACL changes from explicit to implicit and the ACL settings change from those in the ACL file to those of its parent.

You can add a user to a public folder ACL using the command:

```
omaddacln -t bulletin -l <BB_ref>
```

The following table lists the levels of access that can be given to users or groups of users.

Table 3: Public Folder Permissions

Permis- sion	Short- hand	Description
Owner	O (see note)	Grants all permissions in the folder. This user can create, read, modify, and delete all items, including e-mail messages, appointments, contacts, tasks, posted items, and documents and files. Also can create subfolders. The folder owner also can change permission levels that others have for the folder. (Does not apply to delegates.)
Contact	C	Grants the user folder contact status. Folder contacts receive automated notifications from the folder.
Create	c	Grants the user permission to post items in the folder.
Read	r	Grants the user permission to open any item in the folder.
Folder	f	Grants the user permission to see the folder.
Edit All	E	Grants the user permission to edit any public folders, whether his own or owned by somebody else.
Edit Own	e	Grants the user permission to edit only his own public folders.
Delete All	D	Grants the user permission to delete any public folders, whether his own or owned by somebody else.
Delete Own	d	Grants the user permission to delete only his own public folders.
Visible	v	Makes the folder visible.

Note: The shorthand O, C, and so on are only used for setting the UAL_FLDR_ACL_DEFAULT option in the general.cfg file. The command omaddacln only accepts the full words or those defined in the acl.cfg file. For more on the UAL_FLDR_ACL_DEFAULT setting, see the chapter “Configuration Options” on page 169.

Note that if an item attached to a public folder is itself a public folder, access to it is determined by its own ACL, and not the ACL of the parent folder.

Default ACLs

The following table lists the default ACLs for a top-level public folder.

Table 4: Default Public Folder ACLs

User	Permission
Scalix Administrators	Create, read, edit own, delete all, owner, contact, visible.
Local	None.
Default	Create, read, edit own, delete own, visible.

You can change the default level of access that “other users” are granted by setting the general configuration option `UAL_FLDR_ACL_DEFAULT`. When you create a nested public folder, it has a default ACL that is copied from its parent public folder.

Commands

The following table lists commands associated with ACLs.

Table 5: ACL Commands

Command	Description
<code>omaddacl</code>	Add an Access Control List.
<code>omaddacln</code>	Add permissions for users to an Access Control List.
<code>omchkacln</code>	Check permissions of a user in an Access Control List.
<code>omdelacl</code>	Delete an Access Control List.
<code>omdelacln</code>	Delete permissions for users from an Access Control List.
<code>ommodacln</code>	Modify permissions for users in an Access Control List. Permissions can be removed using the <code>ommodacln</code> command and a dash (-) in front of the permission you want to remove.
<code>omshowacl</code>	Show the contents of an Access Control List.

ACL Address Patterns

You can use originator/recipient addresses (O/R addresses) to identify individual users in ACLs. The following rules apply when specifying O/R address patterns in ACLs:

- The O/R address attributes by which a user is identified in an ACL are restricted to the mnemonic address form and are hierarchically ordered.

Table 6: Some O/R Address Attributes

Attribute Abbreviation	Attribute
C=	Country Name
A=	Administration Domain Name
P=	Private Domain Name
O=	Organization Name
OUn=1	Organizational Unit Name 1
OUn=2	Organizational Unit Name 2
OUn=3	Organizational Unit Name 3
OUn=4	Organizational Unit Name 4
G, S, I, Q, CN	Personal Name G — Given or first name S — Surname I — Initials Q — Generation qualifier, such as Jr. CN — Common name

- An attribute value must be fully specified, partly represented with a wildcard, wholly represented with a wildcard, or left blank.

If an attribute value contains a wildcard, either wholly represent all less-significant attributes with a wildcard or leave them blank.

If an Organizational Unit Name is left blank, leave all less significant Organizational Unit Names blank.

The Organization Name, Organizational Unit Name, and Personal Name attributes are specified in printable strings, teletex strings, or both. If both forms are specified, and one form of the attribute value is represented by a wildcard, then the other form must be represented also with a wildcard to the same extent.

Matching Addresses to O/R Address Patterns in ACLs

The following rules are used when matching the O/R address of a user to an O/R address pattern in an ACL entry:

- Match characters regardless of whether they are uppercase or lowercase
- Ignore address attributes that are not used by the mnemonic address form
- If an address pattern specifies both printable and teletex strings for an attribute, and the address being matched contains one form only, then the other form in the address pattern is ignored

Match each attribute:

- A specified attribute matches if each character compares one-for-one
- An attribute partly represented with a wildcard matches if each character in the specified part of the attribute compares one-for-one
- A blank attribute matches if the attribute is also blank in the address of the user
- An attribute wholly represented by a wildcard matches anything
- If the address of the user matches an address pattern, the user is granted the capabilities specified for that address pattern

Examples of O/R Address Patterns in ACLs

The O/R address for a user named “John Doe” is:

```
G=John/S=Doe/CN=John Doe
OU1=paris/OU2=sales/OU3=mis
O=pinewood/P=forester/A=atlas/C=fr
```

It matches the following address patterns:

```
*/CN=*/OU1=paris/OU2=*/OU3=*/O=pinewood/P=forester/A=atlas/C=fr
*/CN=*/OU1=*/OU2=*/OU3=*/OU4=*/O=*/P=forester/A=atlas/C=fr
*/CN=*/OU1=*/OU2=*/OU3=*/OU4=*/O=*/P=for*/A=atlas/C=fr
G=John/S=Doe/CN=John Doe/OU1=*/OU2=*/OU3=*/OU4=*/O=*/P=*/A=*/C=*
```

The address for “John Doe” does not match the following valid address patterns:

```
*/CN=*/OU1=paris/OU2=*/O=pinewood/P=forester/A=atlas/C=fr
*/CN=*/OU1=paris/OU2=sales/OU3=mis/P=forester/A=atlas/C=fr
G-TX=John/S-TX=Doe/CN-TX=*/OU1=*/OU2=*/OU3=*/OU4=*/O=*/P=*/A=*/C=*
*/OU1=*/OU2=*/OU3=*/OU4=*/O=*/P=for*/A=atlas/C=fr
```

The first address pattern does not specify an OU3. The address for John Doe does have an OU3 equal to mis. Similarly, the Organization Name in the second address pattern is blank. In the third address pattern, only the teletex string version of the Personal Name is specified rather than the printable string version. In the fourth address pattern, the Common Name is blank.

The following address patterns are not valid:

```
*/CN=*/OU1=paris/OU2=sales/OU3=mis/O=*/P=forester/A=atlas/C=fr
*/CN=*/OU1=paris/OU3=mis/O=pinewood/P=forester/A=atlas/C=fr
*/CN=*/OU1=paris/OU2=sales/OU3=mis/O=*pinewood/P=forester/A=atlas/C=fr
```

In the first address pattern, the Organization Name is represented with a wildcard. Because of the lesser significance of the Organization Unit Names, these need to be also represented with wildcards. In the second address pattern, OU2 is blank. Therefore, OU3 must also be blank. In the third address pattern, the wildcard character is incorrectly positioned in the Organization Name. The wildcard character must be at the end of the partial value.

Combining Users and Permissions

If a user is a member of more than one group, the permissions given to each group are combined for that user. The following example shows a Directory ACL.

Table 7: Combining Users and Permissions

User	Permission
John Doe/ny,hq,mis	update
/ny,	modifyself
/,*,*/**/*	read
Local Administrators	config
Local Users	none

The omshowacl command outputs data in positional format.

The local user John Doe is explicitly given update permission. The user is also part of the group */*,*,*/**/* and so has read permission.

If John Doe is an Administrator for this system, then John Doe also has config permission.

Note that John Doe/ny,hq,mis does not match */ny,* because a wildcard has not been specified for the third Organizational Unit Name.

When a user attempts to use a resource, Scalix searches the ACL entries of the resource as follows:

- 1 The group entries in the following order:
 - Default
 - Local users
 - Local administrators
- 2 The address entries for an address pattern match.

This search order is used for all ACL entries. Because the group entries are checked in ascending order, a local administrator has the combined permissions of a default user and a local user, and a local user also has the permissions of a default user. If the group entries give sufficient permissions, the address entries are not searched. If Scalix does not find sufficient permissions within the group entries, it starts checking the address entries. If Scalix does not find an address match in the address entries, permission is denied.

Working with Scalix Directories

This chapter explains Scalix's internal directories. For information about how to integrate with external directories, such as Microsoft Active Directory or the Lightweight Directory Access Protocol (LDAP), see those chapters in the *Scalix Setup and Configuration Guide*.

Contents

This chapter includes the following information:

- “Directory Overview” on page 135
- “Shared Directories” on page 136
- “Commands” on page 137
- “Listing Fields in the SYSTEM Directory” on page 138
- “Creating a New Directory” on page 139
- “Adding and Modifying a Directory Entry” on page 139
- “Searching a Directory” on page 139
- “Using the Client Directory Access Server” on page 141

Directory Overview

Directories are where user and other data is stored. They can be used several ways, including in the background when you send or receive mail and in the background when you schedule a meeting with free/busy times and to add entries. Actions that you can perform on directories include adding a phone number for a user to the directory using a command and searching it.

Scalix directories are made up of entries that identify users or entities and their attributes.

There are two types of directories in Scalix:

- **Shared directories** – Can be accessed by a number of users
- **Personal directories** – Can only be used by a specific user

Scalix's internal services and gateways as well as its external clients use directories to resolve incomplete addresses and help route e-mail. Clients can also use directories to obtain additional information, such as telephone numbers, job titles, or postal addresses of users.

Scalix must have a default shared directory, which most often is either provided by an LDAP or Microsoft Active Directory. The Scalix router uses this directory when it resolves addresses. This directory also contains the master list of all users in the network.

You can add other shared and personal directories to Scalix to fulfill the requirements of specific users or groups. Access to shared directories is controlled through the use of Access Control Lists.

The attributes that make up directory entries are defined in an attribute definition file. This file contains internal attribute tags, syntaxes, and lengths of all attributes defined for use on the Scalix system. You can customize Scalix directories by adding fields that are automatically generated each time you add an entry to the directory.

There can be any number of Scalix directories. Each one is in a database structure in a separate directory under `/var/opt/scalix/<nn>/s/dir`. Scalix provides a number of diagnostic utilities for monitoring the use and integrity of directory databases.

The Scalix directory system is not only used for the storage and retrieval of names and addresses, but also contains Public Distribution Lists (PDLs). When you create a group, such as sales, and its e-mail address sales@yourcompany.com, a PDL is created. Each e-mail sent to sales@yourcompany.com is sent to all users who are a member of the group. In that way, a PDL is created. You can manage access to PDLs using Access Control Lists. Also, using the Scalix LDAP server, you can access a Scalix directory using the LDAP protocol.

The internal attribute tags defined in the attribute definition file are mapped to language dependent tags and descriptions in the localized attribute file. The localized attribute file provides local language display of attribute tags and descriptions.

Shared Directories

One function of the Scalix directory system is the storage and retrieval of names and addresses. This function is shared across the SYSTEM, USERLIST, and FREEBUSY directories:

- The **SYSTEM** directory is the default directory for name and address storage and retrieval. Clients access this directory when a user enters a full or partial name in the “To” field when creating an e-mail, and the client returns a list of possible names. In addition, the system accesses this directory to verify recipient mailnodes if additional information is needed to route a message.
- The **USERLIST** directory verifies local mailnode and Scalix recipient information. This directory contains information about all the local addresses and valid recipients on the Scalix server. Each time you add a mailnode or local recipient, an entry is automatically added in the USERLIST directory. A user entry includes items such as name, mailnode, Scalix user ID, Linux user ID, privileges, and Scalix password (including when the password was last changed).

You can access the USERLIST directory like other Scalix directories. Because the USERLIST directory is “hidden”, you must specify `-t h` (type=hidden) if you want to search the directory. For example, the command `“omsearch -d USERLIST -t h -e s=*”` displays a list of resources and users.

This directory is hidden. The `omlistdirs` command does not display this directory.

Alert

Scalix recommends that you do not manually edit the USERLIST directory. Use commands, such as `ommodu` and `ommodmn`, to modify recipient and mailnode information.

- The **FREEBUSY** directory allows users to share calendar information. It is created automatically when you install Scalix. The local calendar information of each user is periodically added to the shared FREEBUSY directory on the local Scalix server. All users who want to share calendar information need to have an entry in this directory.

When a user attempts to schedule an event involving more than one user in the client calendar application, Scalix queries the appropriate FREEBUSY directories on the Scalix

server to determine the availability of users and other resources, such as a meeting room.

A directory contains addressing information and can store additional information, such as a telephone number, office location, and company name.

You can add customized attributes and these are entered or displayed using a TAG=value pair. The TAG identifies the type of attribute, and implicitly defines the syntax and size of the value that the attribute can have.

The `/var/opt/scalix/<nn>/s/sys/dir.attrs` file defines attribute types and the `/var/opt/scalix/<nn>/s/nls/<language>/diratt.loc` file (one for each language installed on the Scalix server) provides language dependent tags and descriptions for each attribute type. New attribute types are defined by editing these files. You can display attribute types available on Scalix by entering the `omshowatt` command.

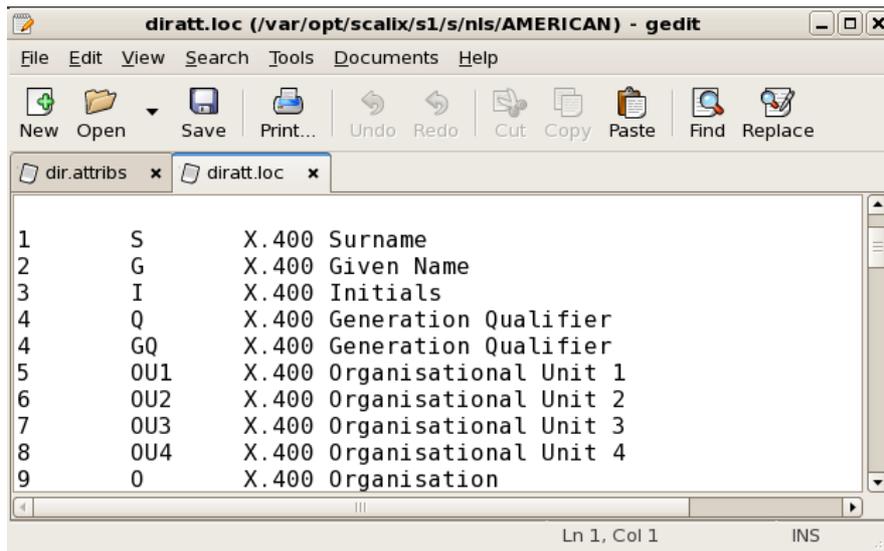


Figure 1: diratt.loc File

Directory entries are added, deleted, and modified using the `omaddent`, `omdelete`, and `ommodent` commands.

Commands

Use the following commands to manage Scalix directories.

Table 1: Commands for Working with Scalix Directories

Command	Description
<code>omaddent</code>	Add one or more entries to a directory.
<code>omdelent</code>	Delete one or more entries from a directory.
<code>omdiropt</code>	Optimize a directory.
<code>omdoptall</code>	Optimize all directories.
<code>omfmtent</code>	Format directory and address attributes.

Table 1: Commands for Working with Scalix Directories

Command	Description
omlistdirs	List directories, such as SYSTEM and FREEBUSY. The USERLIST directory is hidden.
ommoddir	Modify a directory.
ommodent	Modify a directory entry.
omremdir	Delete a directory.
omsearch	Search a directory.
omshowatt	Show a list of available attribute types in the SYSTEM directory.

Listing Fields in the SYSTEM Directory

To view the fields defined for the SYSTEM directory, enter this command:

```
omshowatt
```

The following information appears.

Table 2: Some Fields in the SYSTEM Directory

Field Names	Data Types	Lengths	Descriptive Names
S	KX	40	X.400 Surname
C	X	3	X.400 Country Code
DIT-RDN		U/L	DIT Relative Distinguished Name
DIT-RDN-ID	KPS	40	DIT RDN Global Identifier
DIT-PARENT-ID	KV	40	DIT DN Parent Identifier
DIT-OWNER	KV	U/L	DIT node owners
DIT-SEARCH-REF	KV	U/L	DIT search referrals
DIT-MODIFY-REF		U/L	DIT modify referral
FULL-NAME		64	Personal Full Name
LAST-NAME	K	64	Personal Last Name
MIDDLE-NAME	V	20	Personal Middle Name
FIRST-NAME	K	20	Personal First Name
ALIAS	KMSV	20	Personal Aliases
...			

Creating a New Directory

To create a new directory, enter:

```
omnewdir -d <directory_name> -t s
```

where you substitute the name of the directory for `directory_name`. Adding the `s` parameter at the end of the command means the directory is shared, while adding the `p` parameter at the end instead creates a “private” directory that is only accessible by the user who creates the directory.

New directories have default attributes.

Example

```
omnewdir -d PINEWOOD -t s -p secret
```

creates a directory called PINEWOOD that is shared and has a password of secret.

Adding and Modifying a Directory Entry

You can add an entry to a directory and modify an entry.

To add an entry to the SYSTEM directory

- 1 Use the `omaddent` command, for example:

```
omaddent -e "s=lastname/g=firstname/ou1=mailnode of unix gateway/  
ou2=value/ou3=value/cn=display name/ia=user@domain.com"
```

To modify an entry (field named Job Title with an associated value)

- 1 Use the `ommodent` command, for example:

```
ommodent -e s=lastname -n Job-Title="Accountant"
```

(This job title does not appear in Scalix Management Console.)

To modify an entry (phone number for Barbara Benson)

- 1 Use the `ommodent` command, for example:

```
ommodent -e "G=Barbara/S=Benson" -n "PHONE-1=613 555-3333"
```

where PHONE-1 corresponds to the **Work Phone** field in Scalix Management Console.

Searching a Directory

An entry in a directory is retrieved using a search filter. Use the `omsearch` command to search a directory.

To search the directory (for users by last name)

- 1 Enter the following command to search for all entries in the SYSTEM directory containing a surname of Smith:

```
omsearch -e S=smith
```

which returns, for example, the following information

```
S=Smith/G=Janet/OU1=scalix1/CN=Janet Smith/INTERNET-ADDR="Janet
Smith" <Janet.Smith@scalixtester.com>/ENTRY-TYPE=1/UL-
AUTHID=Janet.Smith/UL-CAPS=6/UL-CLASS=Full/UL-IL=AMERI-
CAN/CNTRY=US/PARENT-DL=192
```

A search filter is made up of “filter items” and other filters. A filter item is an attribute tag, an attribute value, and an operator. For example, S=ExampleEntry. The following table lists operators.

Table 3: Operators for Directory Searching

Operator	Description
=	Equal to the value of the filter item.
-	Approximately equal to the value of the filter item (supported with filter items using ASCII string type syntaxes).
>	Greater than or equal to the value of the filter item (supported with filter items using integer type syntaxes; for example <code>INTEGER</code> and <code>DATE</code>).
<	Less than or equal to the value of the filter item (supported with filter items using integer type syntaxes; for example <code>INTEGER</code> and <code>DATE</code>).
&	AND
	OR
!	NOT

Use parentheses () to nest filters within other filters. For example, to search the default directory to find all entries that have a surname of “Wolf”, and a given name of “Mike” or “Mikey” but not “OU1=sales”, the following filter is used:

```
omsearch -e "S=wolf & (G=Mike | G=Mikey) &! OU1=sales"
```

where OU1 is the name of the Scalix server, not a group name. (The command is a non-working example.) Wildcards (*) can also be used in filter items with string type syntaxes to represent whole or partial attribute values (this applies to string syntaxes only).

To list all surnames, enter:

```
omsearch -e s=*
```

Or enter the following to search for entries containing a specific string of characters:

```
omsearch -e s=*wo*/ou1=*sal*
```

To display only a specific attribute value, use the -m parameter. Enter:

```
omsearch -e s=* -m OU1=
```

Using the Client Directory Access Server

The Client Directory Access (CDA) server builds access tables for Scalix directories to provide sorted lists of directory entries.

Microsoft Outlook requires sorted entries in the Address Books. This enables “typedown” functionality when selecting addresses in the interface. The CDA Server is used to provide the sorted lists of directory entries.

The commands `omaddcda`, `ommodcda`, `omdelcda`, and `omshowcda`, are used to add, modify, delete, and show directories are configured for processing by the CDA server, respectively. The `omexeccda` command forces the immediate processing of a directory without waiting for the next periodic rebuild of its access tables.

Options you set in the `general.cfg` file determine how the CDA server operates. See the chapter “Configuration Options” on page 169 for more information.

The CDA server periodically checks its configuration settings (by default, once every five minutes in `/var/opt/scalix/<nn>/s/sys/cda.cfg`) and if the processing of a directory is required, the CDA accesses the directory, extracts the required information, sorts the entries (on surname, given name, and initials by default), and stores the entries in access tables within the `~/cda` directory.

As the access tables for a directory are created periodically, modifications to a directory are not immediately reflected in the access tables. Changes to directory entries become visible to a client as follows:

- Added entry – The new entry is visible only after the CDA server (or `omexeccda`) rebuilds the access tables and the client closes and opens the directory
- Deleted entry – The substitute text `<Deleted Entry>` appears until the CDA server (or `omexeccda`) rebuilds the access tables and the client closes and opens the directory. Then neither the entry nor the substitute text appears in the directory.
- Modified entry – The change is immediately visible, but the sort order can be incorrect until the CDA server (or `omexeccda`) rebuilds the access tables and the client closes and opens the directory

To force the server to process a directory immediately, you can use the `omexeccda` command.

You can configure the time interval between directory processing by the CDA server. The interval is configured by the `omaddcda` and `ommodcda` commands. By default, the interval is 24 hours. The practical minimum interval depends on the time taken for the CDA server to build the access tables. This in turn depends on a number of factors, such as system size, system resources, system loading, and directory size. If the interval is set too low, the CDA server ends up continuously processing the directory. To verify the amount of time a directory takes to process, use the command `omshowcda -d Dir_name`.

To optimize the rebuilding of the access tables, configure the CDA server to check the directory change log. Do this by setting the option `CDA_USE_CHANGE_LOG=TRUE` in the `general.cfg` file. See the chapter “Configuration Options” on page 169 for more information.

For a Microsoft Outlook user, PDL directory entries can appear as non-existent if the user does not have the required privileges defined by the Access Control List (ACL) for the PDL. For example, when accessing the Address Book, any PDL for which the user does not have read privileges is replaced by the text “`<Deleted Entry>`”.

Starting the Client Directory Access Server

To start the CDA server

1 Enter:

```
omon -s cda
```

Commands

The following table lists commands associated with the CDA.

Table 4: Client Directory Access Commands

Command	Description
omaddcda	Add a directory to the CDA server configuration. You can specify the directories to be processed, configure the interval at which the directories are to be reprocessed, the fields to be used to sort directory entries, and how often the CDA server re-reads its configuration details.
omdelcda	Delete a directory from the CDA server configuration.
omexeccda	Force the CDA server to process a directory immediately.
ommodcda	Modify the CDA server configuration for a directory.
omshowcda	Show the CDA server configuration for a directory.

Handling Undeliverable Mail

This chapter covers creation of a redirect account to hold undeliverable messages and how to designate a user account for notification when no redirect account has been created.

Contents

This chapter includes the following information:

- “Introduction” on page 143
- “Creating a Redirect Account” on page 144
- “Designating a User to Receive Non-Delivery Notice” on page 144

Introduction

You can create a redirect or “catch-all” user account to receive all e-mail not delivered to other, more specific addresses.

The format for configuring the redirect account is:

```
CATCH PATTERN RECIPIENT
```

where PATTERN can be:

- user*
for any unknown address starting with user
- @yourdomain.com
for any unknown address in yourdomain.com
- user*@yourdomain.com
for any unknown address starting with user and in yourdomain.com

and RECIPIENT is:

- The Simple Mail Transfer Protocol (SMTP) address for the catch-all account

When no redirect account exists, notification of non-delivery is sent to sxdadmin by default. You can view the user account used for such notification and change it.

Creating a Redirect Account

A catch-all/redirect account is for accepting e-mail sent to unknown users instead of non-delivery of mail.

The catch-all address can be sent to a Scalix or a UNIX user but it is subject to any relay rules if the catch-all address is outside the local domain.

To create a redirect account

- 1 Open the smtpd.cfg configuration file at

```
/var/opt/scalix/<nn>/s/sys/smtpd.cfg
```
- 2 Create a mailbox to receive redirected mail. To create that mailbox, add one of the following three lines:
 - Any unmatched user beginning with a known-string in any domain:

```
CATCH user* catchall@yourdomain.com
```
 - Any unmatched user in a known domain:

```
CATCH @domain.com catchall@yourdomain.com
```
 - Any unmatched user beginning with a known-string in a known domain:

```
CATCH user*@yourdomain.com catchall@yourdomain.com
```
- 3 Stop and restart the SMTP relay by entering the following commands:

```
omoff -d0 smtpd
omon smtpd
```

Designating a User to Receive Non-Delivery Notice

By default, if you do not set up a redirect account, non-deliverable mail is bounced and non-delivery reports are sent to sxadmin. You can view the user account designated to receive notice, and you can change it. The account designated to receive the mail is called the error notification user (enu).

To view the user account that receives notice of undeliverable mail

- 1 Enter the following command:

```
omshowenu
```

which displays the user account currently defined as the error notification user. By default, this is the sxadmin user.

To change the user account to receive notice of undeliverable mail

- 1 Use the following command:

```
omconfenu -n name[/mailnode]
```

where you substitute a user account name for name, for example

```
omconfenu -n "Jane Rogers"
```

Changing Hostname and IP Address

This chapter covers the procedure for changing a Scalix computer's hostname or Internet protocol (IP) address after installation.

Contents

This chapter includes the following information:

- “Introduction” on page 145
- “Changing a Hostname” on page 145
- “Changing an IP Address” on page 146

Introduction

The hostname is the name and domain of the Scalix server, for example scalix1.yourcompany.com

We do not recommend changing it after Scalix has been installed, but you can if you need to.

The method for changing a hostname varies with the Linux distribution. The approach is to change the `/etc/hosts` file so that the server resolves its own IP and changes the files that the distribution uses to store the hostname, for example, `/etc/default/hostname`, `/etc/sysconfig/network` or similar.

Changing a Hostname

A general procedure is provided.

To change a hostname

- 1 Run the following command:

```
sxmodfqdn -o <oldfqdn> -n <newfqdn>
```

for example

```
sxmodfqdn -o scalix1.yourcompany.com scalix2.yourcompany.com
```

- 2 Change the hostname configuration by opening the file:

```
/etc/opt/scalix/instance.cfg
```

and changing the old hostname to the new one in the lines:

```
OMNAME=<change old hostname to new one>  
OMHOSTNAME=<change old hostname to new one>
```

- 3 Change the old hostname to the new one in the following files:

```
/var/opt/scalix/<nn>/caa/scalix.res/config/ubermanager.properties
```

```
/var/opt/scalix/<nn>/platform/platform.properties  
/var/opt/scalix/<nn>/webmail/swa.properties  
/var/opt/scalix/<nn>/res/config/res.properties  
/var/opt/scalix/<nn>/tomcat/conf/server.xml  
/var/opt/scalix/<nn>/mobile/mobile.properties
```

And in all the files found in these directories:

```
~/tomcat/connector/ajp  
~t/tomcat/connector/jk
```

- 4 Restart the server.
- 5 Check the `/etc/hosts` file and change it if required.
- 6 Change all hostname references on Apache VirtualHost declarations or any other servers that communicate via hostname identifiers.

Changing an IP Address

Scalix bases most of its calls on fully qualified domain names rather than IP addresses. So the primary step in changing an IP address is updating the operating system's Domain Name System (DNS) tab. There is one additional change needed to update the PostgreSQL database white list.

To change a Scalix server's IP address

- 1 Change the IP address in the operating system's DNS tab. For example, in Red Hat click **System > Administration > Network**.
- 2 Run the following script to specify the new IP address. This is a space-separated list of all IP addresses allowed to access the database. Because it overrides (it is not additive), you must re-type all IP addresses accessing the database, including any additional machines running Scalix Web Access, the Search and Index Service, and so on.

```
./sxpsql-whitelist <IP address 1> <IP address 2> <IP address 3> etc
```

- 3 In addition, change the IP address in the following file:

```
/var/opt/scalix/<nn>/sis/sis.properties
```

- 4 Restart Tomcat and the PostgreSQL database:

```
/etc/init.d/scalix-postgres restart  
/etc/init.d/scalix-tomcat restart
```

Recovering Deleted Items

This chapter outlines how to recover items that have been deleted by users from the Deleted Items folder.

Contents

This chapter includes the following information:

- “Introduction” on page 147
- “Recovering Deleted Items” on page 148
- “Changing the Default Hold Period” on page 149
- “Disabling the Recovery Folder Feature” on page 149
- “Emptying Recovery Folders” on page 150

Introduction

If a user hard-deletes an important e-mail or a calendar item auto-expires from the Deleted Items folder, you can recover it. For a configurable period of time, the Scalix Recovered Items folder keeps e-mails removed from the Deleted Items folder. The default is seven days, and you can change it.

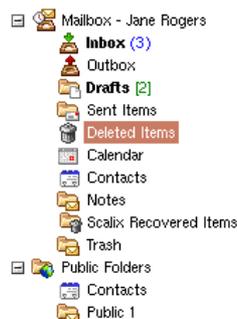


Figure 1: Deleted Items and Scalix Recovered Items Folders in Scalix Web Access

The recovery folder, which is created automatically during Premium user account creation, normally is not visible to users. It can be made visible as a regular mailbox folder in the client application, such as Scalix Web Access or Thunderbird, to recover an item that has been deleted. When visible, the items in the recovery folder are not modifiable until they are copied or moved to the live mailbox. Once the message is recovered, the recovery folder can be hidden from view again.

Recovery folders can be used for Premium user accounts except in Scalix Community Edition. You cannot turn on recovery folders for Standard users, and they cannot see the Scalix Recovered Items folder.

Items cannot be recovered through the SmartCache interface in Microsoft Outlook. If needed, use another client, such as Microsoft Outlook without SmartCache, Scalix Web Access, or an Internet Message Access Protocol (IMAP) client to recover lost messages.

Items within the recovery folder are not included in a user's mailbox limits.

There is a point where messages and calendar items do not exist even in the recovery folder. There are two ways this can happen:

- At client log-off, the system tidies the Deleted Items and recovery folders, removing items that exceed the configured expiry period. The expiry period is configurable.
- The recovery folder can be emptied manually using the `omtidy` or `omtidyallu` commands. It is treated as a separate area (identified by the letter "r"). This area `r` (the recovery folder) can be tidied by using an age or the recovery folder expiry period.

When the item is not found in the recovery folder, an option is to restore it from any backup that you performed.

Recovering Deleted Items

If a user deletes an item that he or she later needs to recover, make the recovery folder temporarily visible so that the user can retrieve the item and return it to the live mailbox. Then make the recovery folder invisible again. You manage this in Scalix Management Console or by commands.

To make a recovery folder visible using Scalix Management Console

- 1 In Scalix Management Console, access the user's account.
- 2 At the bottom right of the window, click **Show Recovery Folder**. The button is displayed for a Premium user account (except Scalix Community Edition). The user can now access the **Scalix Recovered Items** folder in their e-mail application, such as Scalix Web Access or Thunderbird. They can be required to close, then open their application for the folder to become visible.
- 3 When done, hide the folder again by clicking **Hide Recovery Folder** in Scalix Management Console.

To make a recovery folder visible using commands

- 1 At the Scalix server, run the following command with the recovery option:

```
ommodu -o <username> --recovery Y
```

for example

```
ommodu -o "Jane Rogers" --recovery y
```

The Premium user can now access the **Scalix Recovered Items** folder in their e-mail application, such as Scalix Web Access or Thunderbird. They can be required to close, then open their application for the folder to become visible.

- 2 When the user has finished recovering the item, hide the folder:

```
ommodu -o <username> --recovery N
```

Changing the Default Hold Period

By default, Scalix holds items in a recovery folder for seven days. When no value is specified, seven days applies.

To change the default hold period

- 1 Go to the following file:

```
/var/opt/scalix/<nn>/s/sys/general.cfg
```

- 2 Change or add the following value:

```
RECOVERY_FOLDER_EXPIRY_TIME=<time_period>
```

where <time_period> is the amount of time that deleted items remain in the **Scalix Recovered Items** folder before being removed from the system.

Sample settings for this option are:

- 4d12h (4 days and 12 hours)
- 240h (240 hours)

- 3 Restart the client.

Note

To set the value at the client level instead of the global level, use the `/var/opt/scalix/<nn>/sys/client.cfg` file instead.

Disabling the Recovery Folder Feature

If the recovery folder expiry time is explicitly configured to zero, the recovery feature is disabled. This means deleted items are not moved to the recovery folder and users do not have the option of retrieving messages that they have deleted by mistake.

To turn off the recovery folder feature

- 1 Open the following file:

```
/var/opt/scalix/<nn>/s/sys/general.cfg
```

- 2 Change or add the following value:

```
RECOVERY_FOLDER_EXPIRY_TIME=0
```

Emptying Recovery Folders

You can empty recovery folders, deleting all items in them. But once this is done, none of the items can be restored.

The recovery folder can be emptied manually using the `omtidyu` or `omtidyallu` commands, for individual or all user accounts. When using these commands, the recovery folder is treated as a separate area (identified by the letter “r”). This area r (the recovery folder) can be tidied by using either an age or the recovery folder expiry period.

To empty a recovery folder

- 1 Run one of the following commands:

```
omtidyu -B -u "Richard Hall" -d -T r -a 2
```

which tidies the recovery folder for user Richard Hall when items are more than two days old.

```
omtidyallu -d -T r -a c
```

which tidies all recovery folders using configured expiry times, including resources (such as a boardroom) that have e-mail accounts.

```
omtidyallu -d -T r -a 0
```

which clears all recovery folders of all items because the age (-a) specified was zero.

Setting Message Delivery Rules on the Router

This chapter describes how to use the service router to set message delivery rules.

Contents

This chapter includes the following information:

- “About Message Delivery Rules” on page 151
- “About the Service Router” on page 151
- “Commands” on page 152
- “Configuring Message Delivery Rules” on page 153
- “Examples of Message Delivery Rules” on page 161
- “Listing Deferred Mail and Forcing Delivery” on page 164

About Message Delivery Rules

You can set message delivery rules for any given route so that special routing instructions are handled at the server level. Some reasons to use router rules are:

- Rejecting mail from unknown or certain known senders before it reaches users
- Deferring delivery of low priority mail until off-peak hours to preserve bandwidth
- Blocking highly sensitive messages or preventing them from leaving the company
- Preventing delivery status notification messages from going out to the Internet or locally to other servers
- Filtering on the basis of sensitivity levels

These rules are set in the Service Router, which detects them and acts appropriately. The Service Router is a service in Scalix.

About the Service Router

All messages arriving on the system or generated by the system pass through the Service Router, which determines which services are used to deliver a message to its next “hop”. The next hop can be a Scalix interface or gateway, the local delivery service, or any number of other queues. For this reason, the Service Router is a good place to set rules that determine how, when, where, and whether messages are delivered.

When the router receives a message, it performs several tasks, including:

- Checking file types
- Updating the recipient list to match the latest routing information
- Checking and applying rules or filters for each route
- Adding routes for recipients
- Checking that message are not looping
- Checking that the sender has permission to use each delivery service
- Attaching messages to each delivery service queue

Messages are passed to the Service Router through its input queue, which is named ROUTER. The service name is router and the process name is service.router.

If a message is addressed to several recipients, several services can be required to deliver the message to its next hop.

Deferred Mail Manager

If the action of a service router rule is to defer delivery of a message, it submits the message to the Deferred Mail Manager queue.

The Deferred Mail Manager process (named defer.manager) monitors the Deferred Mail Manager queue, and picks up any new messages submitted to it by the Service Router. These messages and the deferral period defined in their rules are stored in a deferred message list located at `/var/opt/scalix/<nn>/s/msglists/DEFER.SR`

When the deferral period is reached, the Deferred Mail Manager delivers the messages. The Deferred Mail Manager does not resubmit messages to the Service Router, but routes the messages itself.

Commands

Use these commands to add, delete, modify, and list routes.

Table 1: Routing Commands

Command	Description
omaddrt	Add a route.
omdelrt	Delete a route.
ommodrt	Modify a route.
omshowrt	List routes and show how an address is routed.

Configuring Message Delivery Rules

A router rule is a text file that you create. There are no restrictions on the file name. Rules can be combined to create rule sets, which consist of a series of text lines.

Some guidelines for writing rules are:

- Lines that are blank or start with a hash character (#) are comment lines
- When an argument contains white space, enclose the argument in double quotation marks ("")
- When an argument contains a double quotation mark (") or a backslash character (/), precede the character with a backslash character
- Each rule in a rule set must be defined on a single line
- A rule contains a number of attributes specified as TAG=value pairs, which define the criteria to be matched in a message

Although some rules within a rule set are associated with the sender of a message (for example the OMLIMIT-EXCEEDED rule), the rules apply only to messages sent by that user to recipients associated with routes that have the same rule set.

Default Rules

There are two reserved rule set names: ALL-ROUTES and ALL-ROUTES.VIR. The files are found in the `/var/opt/scalix/<nn>/s/rules` folder.

- **ALL-ROUTES** – It applies to all routes, except routes for which you configure a specific rule set. This file is used by Scalix Management Console. It partially reflects the maximum mailbox size and message displayed when limits are reached, as set in Scalix Management Console.

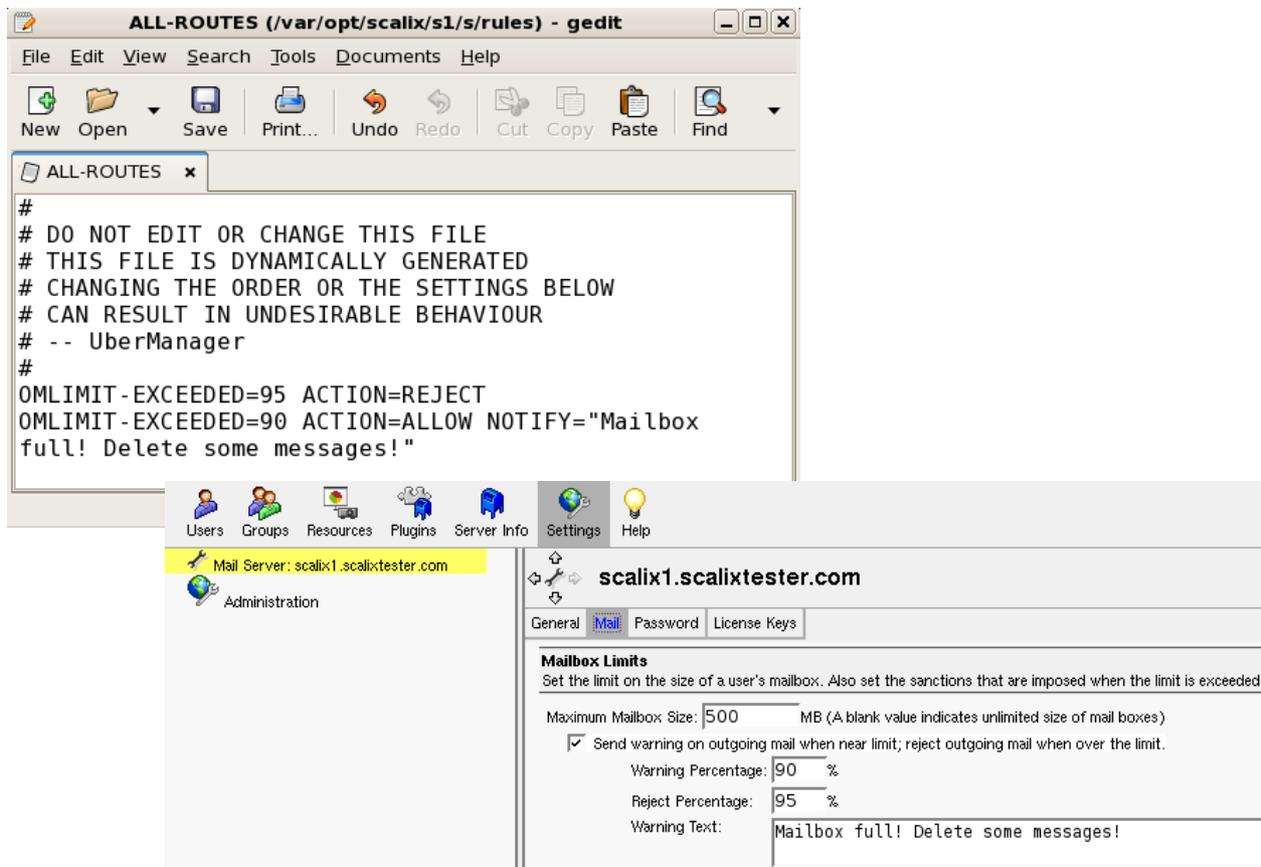


Figure 1: ALL-ROUTES File and the Same Settings in Scalix Management Console

- **ALL-ROUTES.VIR** – This rule set enables virus protection for the Scalix system. Scalix executes this rule set before others.

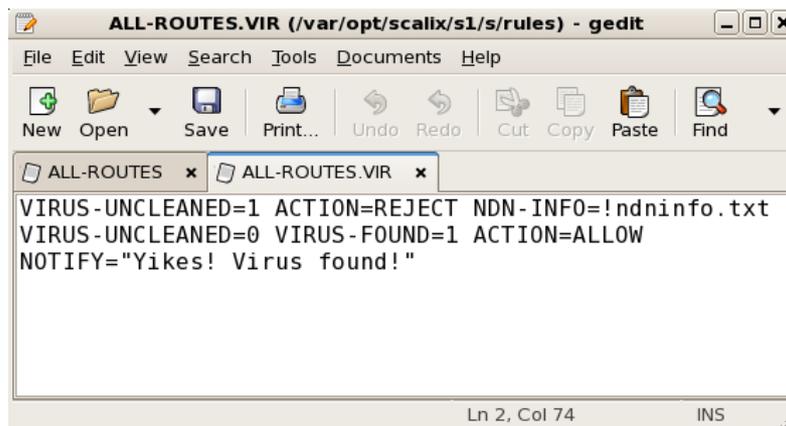


Figure 2: ALL-ROUTES.VIR File for Anti-Virus Settings

Note

Rule sets apply to a message only if you associate the recipient of a message with a route for which you configure a rule set.

Creating a Message Delivery Rule

You create a text file to create a rule.

To configure a Service Router rule

- 1 Create a text file with the rule inside it, using the following format:

```
<Message_Delivery_Attribute> <Action>
```

For example:

```
TYPE=ACK ACTION=DISCARD
```

Use the tables that follow this section for the attribute and action. Examples are also provided later in the chapter.

- 2 Store the text file in the following directory:

```
/var/opt/scalix/<nn>/s/rules
```

For example, a rule with a file name of “ack-discard” is stored as:

```
/var/opt/scalix/<nn>/s/rules/ack-discard
```

- 3 Associate the rule or rule set with the route using either the `omaddrt` command (for new routes) or `ommodrt` (for existing routes):

```
ommodrt -m <route_name> -d <file_name>
```

For example, to associate a rule set named “ack-discard” with an existing route named “remote,sales”, enter the following command:

```
ommodrt -m "remote,sales" -d ack-discard
```

- 4 Restart the service router:

```
omoff -d 0 -w sr
```

```
omon -w sr
```

Note

When you associate a rule set with a Scalix command, Scalix checks the contents of the rule set and reports syntax errors. If you change any rules in a rule set, it is recommended to run the `ommodrt` command to verify that the syntax of the rule is correct.

Rule Attributes

Rules must have attributes, such as the type of message to filter, the period during which the rule applies, or the action to take.

Any files specified as input to rule set attributes must be stored in the `~/rules` folder.

The following table lists the three categories of rule set attributes, and the attributes are explained in the following sections.

Table 2: Message Delivery Rule Attributes

Category	Description
message_filter	Defines the part of the message that the router checks when processing it for rules. When no message filter attributes are defined, then all message filter attributes are considered a match.
day_time	Defines the period during which the Deferred Mail Manager performs the specified action. These attributes apply only when the DEFER action is defined in the rule.
action_info	Defines the action to be performed or the information to be supplied when the values of the message_filter and day_time attributes are matched.

Message Filter Attributes

These attributes define the parts of a message that cause action to be performed. They are optional and if none are specified, the Service Router assumes a match for all attributes.

The following table lists the message_filter attributes.

Table 3: Message Filter Rule Attributes

Attribute	Description
BCC-COUNT	The number of blind carbon copy (BCC) addressees that can be contained in a message. This is matched when the number of BCC addresses in the message is greater than or equal to the value specified for this tag. For example, <code>BCC-COUNT=10</code> causes all messages that have 10 or more BCC addresses to be deferred or rejected, depending on the defined action.
DL-COUNT	The number of addressees that can be contained in the primary distribution list (DL) of a message. This is matched when the number of addresses in the distribution list is greater than or equal to the value specified for this tag. For example, <code>DL-COUNT=100</code> causes all messages that have 100 or more addresses in the primary distribution list to be deferred or rejected, depending on the defined action. A distribution list can contain one or more Public Distribution Lists (PDLs). Each PDL is initially counted as one address by the Service Router. When it is expanded by the local delivery service and passed back to the Service Router, each individual address in the PDL adds to the number of addresses in the primary distribution list and so can cause the message to be deferred or rejected.

Table 3: Message Filter Rule Attributes

Attribute	Description
OMLIMIT-EXCEEDED	<p>A percentage indicating how full a message store component is in relation to its configured limit. A number of message store size limits can be configured for users: overall message store, Inbox, pending tray, and so on. See the MAN page for omlimit for more information.</p> <p>Any NOTIFY action associated with this attribute is executed when the sender of a message has not already been notified within the last day. You can change the default value of 1 day by configuring the <code>OMLIMIT_MIN_WARN_INTERVAL</code> option in the <code>general.cfg</code> file.</p> <p>This filter is matched when the sender has a message store component that is at the specified percentage of its configured limit. For example, a value of 100 matches all messages from senders who had exceeded a limit by any amount; a value of 110 matches all messages from users who had exceeded a limit by 10 percent or more. A value less than 100 can be used to match messages from senders who are near to, but not yet at, one of their limits. For example, a value of 90 matches messages from senders who were at 90 percent or more of a limit.</p>
ORIGINATOR	<p><code>pattern</code> A Scalix address pattern to match against the originator of the message.</p> <p><code>!filename[:charset]</code> A separate file containing one or more Scalix address patterns to match against the originator of the message. The optional <code>charset</code> attribute specifies that the text of the file uses a character set other than IA5. The appropriate character set conversion is performed.</p> <p>Address patterns must observe the format and rules for Access Control List (ACL) address patterns.</p>
PRIORITY	<p>HIGH = An urgent message MEDIUM = A normal message LOW = A non-urgent message</p>
RECIPIENT-SERVICE-LEVEL	<p>The service level of the recipient of a message. Service levels are assigned to users solely to enable receipt and delivery rules to be constructed. A value of 0 checks for those recipients for which a service level has not been created.</p>
SENDER-SERVICE-LEVEL	<p>The service level of the sender of a message. Service levels are assigned to users solely to enable receipt and delivery rules to be constructed. A value of 0 checks for those senders for which a service level has not been sent.</p>
SENSITIVITY	<p>0 = Normal 1 = Personal 2 = Private 3 = Company confidential</p>
SIZE	<p>The size of a message in KBs, matched when the message size is greater than or equal to the value specified for this tag.</p>

Table 3: Message Filter Rule Attributes

Attribute	Description
SUBJECT	<p><code>pattern</code> The string of text to match against the subject of the message. Wildcard characters (*) can be used. The entire subject line of the message is compared with the pattern for a match. This comparison is case sensitive.</p> <p><code>!filename[:charset]</code> A separate file containing the string of text to match against the subject of the message. The optional <code>charset</code> attribute specifies that the text of the file uses a character set other than IA5. The appropriate character set conversion is performed. The entire subject line of the message is compared with the specified string of text for a match. This comparison is case sensitive.</p> <p><code>@script[:charset]</code> A separate script or program containing predefined protocol syntax to communicate with the Service Router and the Deferred Mail Manager to match the contents of the subject of a message. <code>script</code> must be a readable and executable file. The optional <code>charset</code> attribute specifies that the script (or program) uses a character set other than IA5 for the display of the subject. The appropriate character set conversion is performed, and the script (or program) checks for the contents of the subject in the display character set. The script returns a status of matched, or not matched, based on the predefined protocols syntax. For a sample script, see "Sample Script for SUBJECT Attribute" on page 162.</p>
TYPE=ACK	Specifies that the type of message is an acknowledgement (ACK), which is used to block delivery status notifications from going out to the Internet or locally to other servers.
VIRUS-FOUND	<p>Specifies whether a message contains a virus. A value of 0 indicates that a virus was not found in the message; a value of 1 indicates that a virus was found.</p> <p>Include this attribute in a rule to enable virus scanning, but not virus cleaning.</p> <p>This attribute can only be used in the ALL-ROUTES.VIR rule set and applies to all routes. It cannot be applied selectively to specified routes.</p>
VIRUS-UNCLEANED	Specifies whether a message that contains a virus can be cleaned. A value of 0 indicates that the message was checked and was successfully cleaned of any viruses that were found. A value of 1 indicates that the message contained a virus that cannot be cleaned. Include this attribute in a rule to enable virus cleaning. This attribute can only be used in the ALL-ROUTES.VIR rule set and applies to all routes. It cannot be applied selectively to specified routes.

Day/Time Attributes

These attributes define the period during which the Deferred Mail Manager is to defer messages when all other rule attributes are matched and ACTION=DEFER is specified. See the section “Listing Deferred Mail and Forcing Delivery” on page 164 for more information.

The following table lists the day_time attributes.

Table 4: Day and Time Attributes

Attribute	Description
DAY	The day of the week on which to defer messages. This attribute is specified with an integer where 0=Sunday, 1=Monday, 2=Tuesday, and so on. You can specify a range of days (for example, 1-5 for Monday through Friday). When no value is specified, all week is assumed.
TIME	<p>The time of day the DEFER action is to be performed. This attribute is the local time specified in HH:MM or HH format, using the 24-hour clock (00:00 or 00 is midnight). This attribute must be specified.</p> <p>You can specify a duration of time during which deferred messages can be delivered using the following syntax:</p> <pre>time_interval</pre> <p>Controls the start and stop times during which actions are to be performed specified in HH:MM-HH:MM or HH-HH format.</p> <p>You also can specify a time at which to begin storing a batch of deferred messages and an interval of time during which to deliver the deferred messages using the following syntax:</p> <pre>batch_spec</pre> <p>Controls the time to start batching messages and the interval during which to deliver the batch of deferred messages specified in HH:MM@HH:MM or HH@HH format.</p>

Action/Information Attributes

These attributes define the action to be taken or the information to be provided when the message_filter and date_time attributes are matched.

The following table lists the action_info attributes.

Table 5: Action Attributes

Attribute	Description
ACTION	<p>An ACTION attribute must be specified for a rule. For actions that do not automatically return a non-delivery notification, you can specify a message to be returned to the user with the NOTIFY tag.</p> <p>ALLOW = Route the message immediately</p> <p>DEFER = Defer delivery of the message during the period specified by the day and time attributes</p> <p>DISCARD = Discard the message without returning a non-delivery notification to the originator</p> <p>REJECT = Do not route the message and return a non-delivery notification to the originator</p> <p>RETURN = Do not route the message and return a non-delivery notification and the original message to the originator</p>

Table 5: Action Attributes

Attribute	Description
NAME	The name of a rule within a rule set. This name is used in any notification message generated and written to the Scalix Event Log and is useful in determining which rule is being applied when a message is routed. This tag is optional.
NDN-INFO	<p>Enables you to replace the standard text string in the supplementary information field with the specified text when non-delivery notification (NDN) is required. This tag is optional. The value is one of:</p> <p><code>text</code> The text to be included in a non-delivery notification.</p> <p><code>!filename[:charset]</code> A separate file containing the text to be included in a non-delivery notification. The optional <code>charset</code> attribute specifies that the text of the file uses a character set other than IA5. The text is converted to IA5.</p>
NOTIFY	<p>Enables you to include supplementary text in the standard notification message returned to the originator when the defined action has been performed on the message. This tag is optional. When it is specified, the supplementary text is imported as a text part and attached in front of the standard notification message text. This tag is one of:</p> <p><code>No value</code> The standard notification message text containing details of the rule set applied and the recipients affected is used if <code>NOTIFY</code> is specified with no value.</p> <p><code>text</code> The supplementary text to be included in a message to the originator. The maximum size of <code>text</code> is 255 bytes.</p> <p><code>!filename[:charset]</code> A separate file containing the supplementary text to be included in a message to the originator. The optional <code>charset</code> attribute specifies that the text of the file uses a character set other than IA5. The appropriate character set conversion is performed. There is no restriction on the size of text contained in <code>filename</code>.</p> <p><code>NOTIFY</code> is typically used with the <code>ACTION=DEFER</code> or <code>ACTION=DISCARD</code> attributes, because non-delivery notification is not returned to the originator of the message.</p>

Examples of Message Delivery Rules

Some sample rules are:

- Deferring messages based on originator

Delivery of all low priority messages sent from the “lab” mailnode is deferred between 11 a.m. and 6 p.m. That is, the messages are delivered after 6 p.m. and before 11 a.m.

```
PRIORITY=LOW ORIGINATOR="*/CN=*/lab" ACTION=DEFER TIME=11:00-18:00
```

- Delivering messages based on subject

Messages with a subject starting with the text “PUBLIC:”, of normal priority and of a size 1 MB or greater are not routed, and a non-delivery notification is returned to the sender. Any other messages are routed without delay according to the normal Service Router routing process.

```
PRIORITY=MEDIUM SIZE=1000 SUBJECT="PUBLIC:*" ACTION=REJECT
```

- Delivering messages based on priority

High priority messages are delivered Sunday through Saturday without delay according to the normal Service Router routing process. Any medium priority messages are submitted to the Deferred Mail Manager for deferral between 9 a.m. and 5 p.m., Monday through Friday. Any low priority messages are submitted to the Deferred Mail Manager for deferral between 6 a.m. and 9 p.m., Monday through Friday.

```
PRIORITY=HIGH ACTION=ALLOW
```

```
PRIORITY=MEDIUM ACTION=DEFER TIME=09:00-17:00 DAY=1-5
```

```
PRIORITY=LOW ACTION=DEFER TIME=06:00-21:00 DAY=1-5
```

- Rejecting or deferring message delivery based on size

Any messages of a size 1 MB or greater are rejected, and a non-delivery report is sent to the message originator. The delivery of any messages 100 KBs in size (but less than 1 MB) is deferred between 10 p.m. and 6 a.m.

```
NAME=Reject_1Mb SIZE=1000 ACTION=REJECT
```

```
NAME=Defer_100Kb SIZE=100 ACTION=DEFER TIME=22:00-06:00
```

- Providing supplementary text for a non-delivery notification

Messages over 1 MB in size are rejected, and a non-delivery notification containing the text “Message too large” is returned to the sender.

```
SIZE=1000 ACTION=REJECT NDN-INFO="Message too large"
```

- Notifying deferred message delivery

The delivery of low priority messages is deferred 9 a.m. to 6 p.m. on Friday. A notice of deferred delivery is sent to the sender, with the text contained as a separate file in the same `~/rules` folder:

```
PRIORITY=LOW ACTION=DEFER DAY=5 TIME=09:00-18:00 NOTIFY="!delaynote"
```

The text of the deferred delivery confirmation can be:

```
Item 2 (delaynote)
```

To speed the delivery of normal and urgent messages during normal office hours (9am-6pm) on Fridays, any low priority messages are not delivered during these hours.

- Deferring delivery of a batch of messages

Low priority messages received from 8 a.m. are held in a batch and delivered at 1-hour intervals, that is, at 9 a.m., 10 a.m., 11 a.m., and so on.

```
PRIORITY=LOW ACTION=DEFER TIME=8:00@1:00
```

Sample Script for SUBJECT Attribute

Here is an example of a script that can be used with the SUBJECT tag. It can be found at `/opt/scalix/examples/general/subject.map`

You can copy this script into the `/var/opt/scalix/<nn>/s/rules` folder and modify it as required. You must use the protocol syntax as defined in the comments at the top of the supplied script. You must ensure that the script is readable and executable.

```
#!/bin/sh

#####
#           Scalix Server Router Subject Mapping Protocols           #
#####
#
# PROTOCOLS SYNTAX:
# The following table outlines the possible commands sent by
# Scalix Server and the expected replies sent by the Mapper. Note:
# 1) each command/reply must end with a new line (\n) character
# 2) the Mapper must NOT buffer its output, each reply must be
#    flushed
# 3) the Mapper must reply to each command
# COMMAND          REPLY          REPLY COMMENTS
# =====
# <start>          220<SP><text>    Mapper must output this when
#                  starts up
# HELO<SP><text>    250<SP><text>    Mapper accepts scalix session
# SUBJECT:<text>    251<SP><text>    Subject does not match requirement
# SUBJECT:<text>    252<SP><text>    Subject matches requirement
# QUIT<SP><text>    221<SP><text>    Mapper terminates session
# <others>         500<SP><text>    Unexpected command/syntax
#####
# handle "<start>"
# return ready status
rep="220 Subject Mapper Ready"
echo "$rep"
# loop to process commands
Quit="FALSE"
while read cmd
do
    case "$cmd" in
        "HELO"*)
            # handle "HELO<SP><text>"
```

```

        # return ok status
        rep="250 ok"
        ;;
    "SUBJECT:PUBLIC:*")
        # handle "SUBJECT:<text>"
        # subject matches requirement, strip off "SUBJECT:"
        subject='echo $cmd | sed -e "s/SUBJECT:/"'
        rep="252 $subject"
        ;;
    "SUBJECT:*")
        # handle "SUBJECT:<text>"
        # subject does not match requirement, return reason
        rep="251 Subject Does Not Match"
        ;;
    "QUIT*")
        # handle "QUIT<SP><text>"
        # return status, set flag to exit loop
        rep="221 Subject Mapper Close"; Quit="TRUE"
        ;;
    *)
        # handle "<others>"
        # return error status
        rep="500 Unrecognized Command or Syntax Error"
        ;;
esac

# must reply to each command
echo "$rep"
if [ "$Quit" != "TRUE" ]
then
    continue
else
    break
fi
done
exit 0

#####
# End of script
#####

```

Listing Deferred Mail and Forcing Delivery

For any mail that has been deferred for later delivery, you can view a list and force delivery.

To view a list of deferred messages

1 Enter this command:

```
omstat -d
```

To force delivery of deferred messages

1 Enter this command:

```
omresub
```

for example

```
omresub -d "Jane Rogers"
```

to send all deferred mail for user Jane Rogers

and

```
omresub -d ALL
```

to send all deferred messages for users and the Server Router.

Working with the Scalix Search and Index Service

This chapter explains use of the Scalix Search and Index Service component, including how to rebuild the index, how to configure it, and the document types it handles.

Contents

This chapter includes the following information:

- “Introduction” on page 165
- “Document Types Handled” on page 166
- “Creating Users’ Indexes” on page 166
- “Disabling Indexing” on page 167
- “Re-Creating the Index” on page 167
- “Localizing the Scalix Search and Index Service” on page 168
- “Identifying an Individual Subdirectory (SIS URL)” on page 168

Introduction

The Scalix Search and Index Service (SIS) is a set of flat files that enable indexing and subsequent searches for e-mail messages, calendar items, and more. It consists of subdirectories designated for all individual users, who are identified by Scalix Search and Index Service URLs.

By default, Scalix Search and Index Service indexes every 10 minutes or after 200 new items have been added to the index, whichever comes first. This means that new messages or calendar items do not appear in search results until after that interval has elapsed. The interval can be changed, even to the point of real-time indexing, but higher-frequency indexing can drain system resources.

The Scalix Search and Index Service can be localized to many languages, but can only use one language at a time.

It has plug-in capabilities, so you can write your own message analyzers. For more on that, see the chapter “Using Plug-ins” on page 89 and contact Scalix professional services for assistance.

The index does not need to be backed up because it can be re-created at any time.

Document Types Handled

The Scalix search index parses the following document types:

- Microsoft Word, PowerPoint, and Excel
- PDF
- HTML

Creating Users' Indexes

When new user accounts are added to the system, they get an index by default that populates automatically as e-mails arrive. In these cases, no action is needed.

When existing user accounts are upgraded to version 11.x from a previous version, only messages that arrive after the upgrade are automatically indexed. This is because previous versions of Scalix did not include the service. To add messages that predate the update to the index, you run the `sxmindex` command. For more information on creating indexes for existing users when upgrading to Scalix 11, see the upgrade chapter in the *Scalix Installation Guide*.

To index messages for a user

- 1 Log in to a client as the user, and perform a search. Or at the Scalix computer, log in as the administrator and run the following command:

```
sxmindex <user_name>
```

for example

```
sxmindex "Jane Rogers"
```

or

```
sxmindex jane.rogers@yourcompany.com
```

To index messages for all users

- 1 At the Scalix computer, log in as the administrator and run the following command:

```
sxmindex
```

In response, the messages are processed for all user accounts and public folders (bulletin boards), which are listed along with the number of messages processed, for example:

```
sxadmin /scalix1: 20  
Jane Rogers /scalix1: 13  
Johnnie Kameamea /scalix1: 55  
+Bulletin Boards: 2
```

Disabling Indexing

You can disable indexing on a per-user basis, but if you do, that user's search function does not work.

To turn indexing off and on

- 1 To disable indexing, run the following command:

```
ommodu -o <user_name> --index none
```

- 2 To re-enable indexing, run the following commands to give the user a URL and to index past messages:

```
ommodu -o <user_name> --index auto
sxmkindex <user_name>
```

If you ever see a message “No SIS URL for this user”, it means you need to turn on indexing for the user. Use the first command.

Re-Creating the Index

The index can require manual re-creation if it becomes corrupted, out of synchronization, or out of date. This process can put a heavy load on the servers, so it is best undertaken during off hours.

To re-create the search index

- 1 Restart the Tomcat service:

```
/etc/init.d/scalix-tomcat restart
```

- 2 Run one of the following commands.

To re-create all indexes at once:

```
sxmkindex
```

To re-create indexes in recovery mode, which removes deleted messages:

```
sxmkindex -r 00:00:00
```

To re-create one user at a time:

```
sxmkindex <user_name> -r 0
```

where <user_name> is the user's common name, for example

```
sxmkindex "Jane Rogers" -r 0
```

After entering a command, allow the indexes to create, which can take some time depending on the number of users and the size of their mailboxes.

Localizing the Scalix Search and Index Service

The Scalix Search and Index Service can be configured to process text for any language. To work with different languages, it uses stemming rules for that specific language, which break down words by removing suffixes and endings just as they do with the English language. For example, a search for the English word “singing” matches the word “sing”.

To localize the service, see the localization chapter in the *Scalix Setup and Configuration Guide*.

Identifying an Individual Subdirectory (SIS URL)

If needed, you can identify a user’s Scalix Search and Index Service (SIS) URL, which is the subdirectory of the index that belongs to that user.

To identify which subdirectory belongs to a particular user

- 1 Run the following command:

```
omshowu -n <user_name>
```

for example

```
omshowu -n “Jane Rogers”
```

The response provides detailed information about the user account, including the SIS URL:

```
SIS URL : sidx://scalix1.yourdomain.com/02400000358ab874-622.1.61.271
```

Configuration Options

This chapter describes options in configuration files to customize Scalix. If you do not need to customize any configuration options, skip this chapter.

Contents

This chapter includes the following information:

- “About Configuration Files” on page 169
- “System-Wide Configuration Options” on page 170
- “Client-Specific Configuration Options” on page 223
- “User-Specific Configuration Options” on page 234
- “Language-Specific Configuration Options” on page 245

About Configuration Files

The configuration files contain options that affect the behavior of the Scalix system. You can modify system-wide, client-specific, and user-specific options.

Scalix includes a number of hard-coded default options. You can change these options by placing TAG=value pairs in one or more of the following configuration files listed in the following table. The files are located in the following folder:

```
/var/opt/scalix/<nn>/s/sys/
```

where nn varies with Scalix installation.

Table 1: Configuration Files

File	Description
general.cfg	System-wide configuration affecting the server.
client.cfg/<fqdn>	Client-specific configuration.
user.cfg/<scalix-uid>	Per-user configuration.
domain.cfg/<domainname>	Domain-specific configuration.
lang.cfg/<language>	Language-specific configuration.

Any values that contain underscores (_) or spaces are specified within double quotes, for example:

```
SAMPLE_OPTION="one_two three"
```

Some options can be set in more than one configuration file. In this case, user-specific options generally override client-specific options, and client-specific options override general options.

Options for the configuration files, except domain-specific configuration, are outlined in the rest of this chapter.

System-Wide Configuration Options

Global configuration is done in the following file:

```
/var/opt/scalix/<nn>/s/sys/general.cfg
```

The parameters are outlined in the table. After making your changes, restart the service router and archiver for the changes to take effect. The commands to restart the service router are:

```
omoff -d 0 -w sr  
omon -w sr
```

Table 2: System-Wide Options

Parameter	Description
<p>ARCHIVE=TRUE</p>	<p>Enables archiving of all messages that traverse the Scalix server. Messages are archived to a <code>~scalix/archive</code> folder.</p> <p>This parameter can include the following options.</p> <p><code>arch:/path/</code> This archives messages to the folder you specify. Within this directory, the archiver automatically creates subfolders based on the date that messages traverse the Scalix server. For example, if a message arrives at 2:55 on June 10th, 2004, the message is archived to: <code>/path/2004-06-10/14:55+0000.12345.1</code> where +0000 is the local time zone offset from GMT 12345 is the PID of the archiver .1 indicates the number of messages that arrived during that second. The archiver process operates as the user "scalix". If you want the archiver to archive messages to the <code>/home</code> folder, configure the permissions for the <code>/home</code> folder to allow the "scalix" user write access to the folder.</p> <p><code>inet:host.example.com inet:host.example.com:2000</code> This allows connection to the host on port 25 or on a port you specify (<code>host.example.com:2000</code>). This creates an SMTP session and enables you to use third-party archiving systems.</p> <p><code>ARCHIVE=bcc:archive@example.com</code> This forwards to a designated "bcc" mailbox created solely for archiving purposes a blind (bcc) copy of every message that is sent. You create this mailbox before adding this parameter. We recommend it be on a separate computer because archive files use significant memory space.</p> <p><code>file:/path/archive_file_name</code> This writes all messages to a single file. You cannot use this option with auxiliary processes.</p> <p><code>fork:/bin/archive_script.sh</code> The archiver forks the script and communicates with SMTP using stdin and stdout to the script.</p>
<p>ARCH_TNEF_ENCODE=TRUE</p>	<p>Sets the transport neutral encapsulation format (TNEF) as the message format for archived messages. TNEF refers to an e-mail attachment format used in Microsoft Outlook and Microsoft Exchange Server. By default, the archiver converts messages to MIME format and consequently loses some MAPI information (if applicable).</p>

Audit Log Options

Audit logs refer to user information. There are also event logs. You can set the audit log options in the general configuration file:

```
/var/opt/scalix/<nn>/s/sys/general.cfg
```

Table 3: Audit Log Options

Parameter	Description
AUD_88_NAMES=TRUE	Sets audit logging on for the X.400 1988 address attributes. By default, only the 1984 attributes are logged.
AUD_LOG_UX_NAME=FALSE	By default, users are identified in the Audit Log by their Scalix IDs. Set this option to <code>TRUE</code> if you want users to be identified by their Linux user names.

Auto Action Options

These options keep track of auto-actions performed on a recipient's incoming mail.

You can set these options in the general configuration file:

```
/var/opt/scalix/<nn>/s/sys/general.cfg
```

Table 4: Auto Action Options

Parameter	Description
AA_DEFAULT_LOGGING_ON=TRUE	Turns on logging of automatic actions for all users.
AA_GLOBAL_LOGGING_OFF=TRUE	Stops all logging of automatic actions even if configured in a client. <code>AA_GLOBAL_LOGGING_OFF</code> overrides <code>AA_DEFAULT_LOGGING_ON</code> when set.
AA_MAXCFG_LOG_SIZE= <i>size_in_bytes</i>	Sets, for all users, the maximum size of their automatic action log file. The maximum size is 65536 bytes.
FLT_ESC_NO_CONV=TRUE	If set to <code>TRUE</code> , a serious error is reported when the character set for a filter and that for a string being filtered are not of the same kind while filtering for automatic actions. If set to <code>FALSE</code> , this is reported as a failed match.

Client Directory Access Server Options

The Client Directory Access server builds access tables for Scalix directories to provide sorted lists of directory entries.

You can set these options in the general configuration file:

```
/var/opt/scalix/<nn>/s/sys/general.cfg
```

Table 5: Client Directory Access Server Options

Parameter	Description
CDA_CHECKTIME= <i>minutes</i>	Set the time interval, in minutes, at which the Client Directory Access (CDA) server checks its configuration for directories that need processing. The default is 5 minutes.
CDA_USE_CHANGE_LOG=TRUE	Set this option to optimize the rebuilding of directory access tables by the Client Directory Access server. By default, the Client Directory Access server rebuilds the access tables periodically. If set to <code>TRUE</code> , the Client Directory Access server first checks the change log for the directory, and only rebuilds the access tables if the change log shows that the directory has been modified. If the directory does not have a change log, the Client Directory Access server configures one.

Daemon Options

You can set these options in the general configuration file:

```
/var/opt/scalix/<nn>/s/sys/general.cfg
```

Table 6: Daemon Options

Parameter	Description
DADM_DAEMON_TIME_TO_EXIT= <i>seconds</i>	The number of seconds Scalix waits for a daemon to exit before sending a SIGKILL signal to stop the daemon process. The default is 30 seconds; if daemon processes are being stopped too quickly, increase this number. Use this option with caution because the SIGKILL signal does not allow the daemon process to tidy up before it stops.

Directory Options

You can set these options in the general configuration file:

`/var/opt/scalix/<nn>/s/sys/general.cfg`

Table 7: Directory Options

Parameter	Description
CU_LOG_OLD_DIR_CMDS=TRUE	If set, the old directory commands <code>omadddir</code> and <code>ommoddir</code> are used when logging changes to the directory update file (<code>om_record</code>), instead of the new <code>omadent</code> , <code>omdelent</code> , and <code>ommodent</code> commands.
DA_IGNORE_INDEXES= <i>attribute,attribute,...</i>	Under normal circumstances, Scalix fails to locate a match for any Scalix attribute that is keyed but for which the index does not exist. Use this option to specify those Scalix attributes that are keyed but for which Scalix is to search sequentially, rather than attempt to use the indexes for the attributes. <code>attribute,attribute,...</code> is a comma-separated list of Scalix internal attribute names. Do not insert spaces after the commas. This option can be used for newly keyed attributes for which the indexes have not yet been built.
DIR_IA_UNIQUECHECK_OFF= <i>directory-list</i>	Use this option to specify those directories in which uniqueness checking of the Internet address attributes is turned off. The value of this option is a comma-separated list of Scalix directories or <code>ALL</code> .
DIR_IA_UNIQUECHECK_ON= <i>directory-list</i>	Use this option to specify those directories in which uniqueness checking of the Internet address attributes is turned on. The value of this option is a comma-separated list of Scalix directories or <code>ALL</code> .
VI_NON_SUPP_ATTS_UNIQUE= TRUE	By default, the combined values of the O/R address attributes (shown by an X in the <code>omshowatt</code> command) in a directory entry must be unique. If they are not, the entry cannot be added or modified. If set to <code>TRUE</code> , this rule is relaxed and the combined values of all attributes, other than supplementary attributes, are used to determine the uniqueness of the entry rather than just those of the O/R address attributes.
VI_SORTED_VISTA_DATABASE= FALSE	Determines whether the results from a directory search are sorted or in random order. If set to <code>FALSE</code> (the default), the results are returned in random order. If set to <code>TRUE</code> , results are sorted by key. If you set this option to <code>TRUE</code> , you must rebuild all the directories (using the <code>omoptall</code> command) for it to take effect.

Directory Relay Server Options

You can set these options in the general configuration file:

`/var/opt/scalix/<nn>/s/sys/general.cfg`

Table 8: Directory Relay Server Options

Parameter	Description
DRS_HOST_RETRY_TIMEOUT= <i>seconds</i>	If the remote directory access mechanism fails to contact a remote host, it does not retry the connection for the number of seconds specified by this option. If a subsequent request for the same host occurs within the specified period, an error is returned immediately. The default is 60 seconds.
DRS_MAX_CHILDREN= <i>number_of_child_processes</i>	Specifies the maximum number of processes that the directory relay server can support at once. Each process has a separate bind to the directory information base, and some X.500 implementations can support only a limited number of binds at once. So, specify the maximum number of processes with this in mind.
DRS_RESERVED_CHILDREN= <i>number_of_child_processes</i>	Defines the minimum number of child processes that the directory relay server maintains at once. Each child process has its own bind to the directory information base. The greater the minimum number of child processes, the better the performance of directory lookups, but each process consumes resources. You do not normally set this to a value lower than 3: one process each for local delivery and the Service Router, and one to handle requests from the UAL and omsearch. The default value is 3.

Directory Synchronization Options

You can set these options in the general configuration file:

`/var/opt/scalix/<nn>/s/sys/general.cfg`

Table 9: Directory Synchronization Options

Parameter	Description
DR_NO_MOD_STRIP_PDL=TRUE	<p>Determines the amount of information included for an entry in the directory change log when changes are made to public distribution list (PDL) members within the exporting directory using the following PDL commands:</p> <ul style="list-style-type: none"> • <code>omaddpdln</code> • <code>omdelpdln</code> • <code>ommodpdln</code> <p>When set to <code>TRUE</code>, the full PDL entry, including PDL members, is logged in the “from” entry in the <code>MODIFY</code> record. Otherwise, only the X.400 attributes in the PDL entry is logged to save disk space and improve directory synchronization performance.</p>
DS_ADD_UPDATE_LOCAL_ENTRY=TRUE	<p>Determines the behavior of a directory synchronization search. If the <code>ADD</code> operation returns a matching entry and <code>DS_ADD_UPDATE_LOCAL_ENTRY</code> is set to <code>TRUE</code>, a <code>MODIFY</code> operation is performed.</p> <p>During the <code>MODIFY</code> operation, the matched entry in the importing directory is modified with the corresponding entry in the exporting directory.</p> <p>If the <code>MODIFY</code> operation is successful, a <code>MODIFY</code> record is added to the directory change log.</p> <p>Using this option can modify entries in the importing directory that are genuinely different from those in the exporting directory.</p>
DS_CUST_IMP_ADD_UPDATE_LOCAL_ENTRY=TRUE	<p>Determines the result of a directory synchronization search. During directory synchronization, an entry in the exporting directory matches an entry in the importing directory when the search attributes are identical, even though other attributes of the entry are different.</p> <p>In this case, if this option is set to <code>TRUE</code>, the entry in the importing directory is overwritten by the corresponding entry in the exporting directory.</p> <p>If the option is set to <code>FALSE</code>, the entry in the exporting directory is treated as a duplicate of the corresponding entry in the importing directory, and so it is not exported.</p> <p>Using this option can have the effect of modifying entries in the importing directory that are genuinely different from those in the exporting directory.</p>
DS_CUST_MSGQ_TIMEOUT= <i>seconds</i>	<p>The number of seconds the directory synchronization server waits on an empty message queue before checking if any of its timers have expired. Defaults to 1800 seconds. Use in conjunction with <code>DS_CUST_PERIOD_TIMER_MINUTES</code> when testing directory synchronization.</p>
DS_CUST_PERIOD_TIMER_MINUTES=TRUE	<p>If set, the value of the period timer for Scalix-to-Scalix directory synchronization is in minutes. The default is for the value of the period timer to be in hours. Use in conjunction with <code>DS_CUST_SEND_REQ_NOW</code> when testing directory synchronization.</p>

Table 9: Directory Synchronization Options

Parameter	Description
DS_CUST_SEND_REQ_NOW=TRUE	If set, request messages are sent immediately. The first timer check is performed after a restart of the directory synchronization server if the period timer value (24 hours by default) is greater than the time from the current time to the start time. The default is to wait for the period timer to expire. Use in conjunction with DS_CUST_PERIOD_TIMER_MINUTES when testing directory synchronization.
DS_SEND_SOURCE_LID=TRUE	When set to TRUE (default), a unique identifier is propagated with each entry in each transaction during directory synchronization. The value of the identifier is that of the LOCAL-UNIQUE-ID attribute of the entry in the exporting directory. Setting this option to FALSE prevents this identifier being sent during directory synchronization.

IMAP Client Options

You can set these options in the general configuration file:

```
/var/opt/scalix/<nn>/s/sys/general.cfg
```

Table 10: IMAP Client Options

Parameter	Description
IMAP_AUTOMATIC_MDN=FALSE	Determines whether the IMAP4 server generates message disposition notification messages (MDNs) automatically. MDN is defined as a means by which a message can request that message processing by the recipient be acknowledged as well as a format to be used for such acknowledgements. It can be used to notify the sender of a message that the message was displayed, printed, or deleted without display, for example. RFC 2298 specifies that IMAP4 clients are to generate MDNs where requested, but some clients are unable to do this. Set this option to TRUE if you want the IMAP4 server to send MDNs automatically, without reference to the IMAP4 client.
IMAP_BB_FOLDER_PREFIX=#bb	Specifies the string that precedes all mailbox names for public folders. Use this option to enable users to distinguish easily between public folders and private folders. You can specify any ASCII character as a separator, although it is recommended not to choose 0 to 9, a to z, A to Z, +, comma, &, - (minus), tab, space, newline, %, or *. You must not use the same value for this option as for IMAP_FOLDER_PREFIX, or IMAP_FOLDER_SEPARATOR, or IMAP_BB_FOLDER_SEPARATOR. You must enter the character itself, rather than the ASCII code for it.

Table 10: IMAP Client Options

Parameter	Description
IMAP_CONNECTION_LIMIT=0	<p>Specifies the maximum number of concurrent IMAP connections that the server is to support.</p> <p>If left at 0 (the default value), the IMAP4 server continues to accept all connections until computer resources are exhausted. This can adversely affect Scalix performance and eventually prevent other users from accessing the Scalix server.</p>
IMAP_CONNRATE_LIMIT=0	<p>Specifies the maximum number of IMAP connection requests that the IMAP server is to accept in any one second.</p> <p>If left at 0 (the default), the IMAP server accepts connection requests at a rate that is limited only by computer resources. This can adversely affect Scalix performance and eventually prevent other users from accessing the Scalix server. If, for example, you set this value to 3, the IMAP server accepts up to 180 connection requests per minute, and computer resources are likely to be sufficient to allow normal Scalix operation.</p>
IMAP_DELETE_SUBFOLDERS=FALSE	<p>Determines whether the IMAP4 server permits the deletion of folders that contain subfolders.</p> <p>If set to <code>FALSE</code> (the default), the IMAP4 server does not allow a client to delete a folder that contains subfolders. This is in accordance with the IMAP4 protocol. Some non-conforming clients attempt to delete such folders, so you can set this option to <code>TRUE</code> if you want to allow such attempts to succeed (and possibly enhance the usability of these clients).</p>
IMAP_FOLDER_SEPARATOR=/ /	<p>Specifies the character used to separate private folder names in an IMAP mailbox specification. For example, with a separator of / and a folder named beta inside another folder named alpha, the corresponding IMAP mailbox name is alpha/beta.</p> <p>You can specify any ASCII character as a separator, although it is recommended not to choose 0 to 9, a to z, A to Z, +, comma, &, - (minus), tab, space, newline, %, or *. You must enter the character itself, rather than the ASCII code for it. You can need to use a folder separator that is different from the default (/) if you want to use this character in folder names. For example, if an existing Scalix user has a folder called Sales/Forecasts, this folder is not seen through the IMAP server because it cannot be distinguished from a folder called Forecasts within a folder called Sales.</p> <p>There is a separate option to set the separator for public folders; see <code>IMAP_BB_FOLDER_SEPARATOR</code>. See also the related options <code>IMAP_FOLDER_PREFIX</code> and <code>IMAP_BB_FOLDER_PREFIX</code>.</p>
IMAP_IDLE_TIMEOUT=30	<p>Specifies the number of minutes an IMAP connection can remain idle before the connection is closed by the IMAP server.</p> <p>Specify a value of 0 to disable idle time-outs.</p> <p>The IMAP protocol (RFC 2060) specifies a minimum time-out of 30 minutes (the default). Some clients can wait exactly 30 minutes between commands and so are liable to get logged out prematurely if this option is not set or is set to its default value. For these clients, it is sometimes useful to set the idle time-out to 31 minutes.</p>

Table 10: IMAP Client Options

Parameter	Description
IMAP_IGNORE_SERVERNAME=FALSE	<p>Determines whether the IMAP server uses the characters following the @ character in a user name as the server name for this user.</p> <p>When set to <code>FALSE</code> (the default), the name part of the user name (up to and including the @ character) is stripped off and the remainder is used as the server name to which the IMAP connection is relayed.</p> <p>Set this option to <code>TRUE</code> to prevent the IMAP connection being relayed to another server.</p>
IMAP_LOGFILE=~/.tmp/imap.%h	<p>Specifies the name of the file to which IMAP events are logged, provided that logging is turned on using the <code>IMAP_LOGLEVEL</code> option.</p> <p>When the file you specify already exists, new events are appended to it. Note that at certain log levels log files can contain sensitive information, such as passwords.</p> <p>You can use the following tokens in the log file name:</p> <ul style="list-style-type: none"> <code>%P</code> — Expands to the PID of the IMAP server process. One log file is created for each IMAP server process. <code>%h</code> — Expands to the name of the client host. One log file is created for each client host that connects to the IMAP server. <code>%u</code> — Expands to the Scalix UID. One log file is created for each Scalix user that connects to the IMAP server.
IMAP_LOGLEVEL=0	<p>Activates logging of IMAP commands and errors. The log file is specified by the <code>IMAP_LOGFILE</code> option.</p> <p>Set a value of <code>0</code> to disable logging, <code>1</code> to log basic commands/responses only, <code>2</code> to log unexpected UAL errors, and <code>8</code> to enable raw protocol logging. Note that, at log level <code>8</code>, passwords are recorded in the log files. To avoid this, you can set a lower log level in the system-wide or per-client configuration file, and then set the log level to <code>8</code> in the user-specific configuration file. This log level only takes effect after authentication, and so passwords are not recorded.</p> <p>If you require several kinds of logging information, add the numbers for the log levels you require.</p> <p>If the option <code>IMAP_UAL_TRACE_LEVEL</code> is not defined, then setting <code>IMAP_LOGLEVEL</code> to any value other than <code>0</code> enables UAL logging for the IMAP server.</p>
IMAP_MAILSTORE_HOST= <i>hostname</i>	<p>Specifies the fully qualified domain name of the Scalix host to which the IMAP server connects. Use this option when the IMAP4 server does not reside on the same computer as the Scalix system that contains the relevant message store.</p>
IMAP_MDNSENT_FLAG= <i>\$MdnSent</i>	<p>Determines the name of the flag that is set to indicate that a message disposition notification (MDN) has been sent for this message. (See also the option <code>IMAP_AUTOMATIC_MDN</code>.)</p> <p>The name of this flag has not been standardized, so different IMAP4 clients can use different flag names. Set this option to the name of the flag that your IMAP clients use.</p>

Table 10: IMAP Client Options

Parameter	Description
IMAP_MIN_SIZE_ESTIMATE=0	<p>Specifies if the client computes message sizes or estimates them. Some clients report the message size when they list messages in the user's Inbox. To do this, they must render the message, which can be time-consuming, and cause a decrease in performance.</p> <p>To prevent the client from rendering messages above a certain size, specify this size in kilobytes. For example, to prevent the IMAP client from rendering all messages above 5 kilobytes, set this value to 5. Messages less than about 5 kilobytes are rendered and have their size reported accurately. Messages larger than about 5 kilobytes have an estimate of their size reported.</p> <p>Note that some clients require the message size to be computed accurately. For these clients, you set this option to 0 or leave it undefined.</p>
IMAP_REMOTE_UAL_ENABLED=TRUE	<p>Specifies whether an IMAP client can use a remote User Access Layer (UAL) server. UAL is a proprietary Scalix protocol that enables communication between clients and the Scalix server. Local connections have better performance.</p> <p>If set to <code>TRUE</code>, users can specify the name of a remote computer on which a UAL server is running. The IMAP server then uses this remote UAL server. Users specify the use of a remote UAL server by connecting as <code>username@hostname</code>, where <code>hostname</code> is the name of the remote machine to which they want to connect.</p> <p>Set this option to <code>FALSE</code> to prevent users from connecting to a remote UAL server.</p>
IMAP_SEARCH_TIMEOUT=0	<p>Specifies the number of seconds to wait before abandoning a search request. Specify a value of 0 to prevent search requests from timing out.</p>
IMAP_UAL_TRACE_LEVEL=0	<p>Activates tracing of IMAP server information at the UAL server. The trace files are placed in the <code>~/tmp</code> folder. When this folder cannot be found, they are placed in the <code>/tmp</code> folder. <code>user-no</code> is the Scalix user number.</p> <p>If you require several different kinds of trace information, add the numbers for the levels you require and set the entry to the total.</p> <p>0 — No tracing. The default. 1 — Raw (unformatted) command/reply tracing (file name: <code>OMuser-noN.trc</code>). 2 — Symbolic command/reply tracing (file name: <code>OMuser-noC.trc</code>). 4 — Message Store file name mapping. No trace file. The subject of an item listed or displayed in the client is replaced by its corresponding Message Store file name. 8 — Full tracing of command/reply and file transfer data. This can be used to rerun a session (file name <code>OMuser-noU.log</code> and <code>OMuser-noU.fnnnn</code>). 16 — Raw (unformatted) command/reply tracing and file transfer data (<code>user-noN.trc</code>).</p> <p>This option is similar to the <code>UAL_TRACE_LEVEL</code> option. However, the <code>UAL_TRACE_LEVEL</code> option is user-specific, and causes information on all UAL clients to be traced. The <code>IMAP_UAL_TRACE_LEVEL</code> option is IMAP-specific (that is, its trace files contain information on all users of a particular computer), but it traces only IMAP information.</p>

Table 10: IMAP Client Options

Parameter	Description
IMAP_PUBLIC_FOLDERS=FALSE	When set to <code>FALSE</code> , public folders are inaccessible in IMAP clients, such as Thunderbird, as well as Scalix Web Access. This can be set per user, per domain, or for the whole server. Please note that you need to fix the “foldrs” spelling in the configuration file for this option to work.

Internationalization Options

You can set these options in the general configuration file:

```
/var/opt/scalix/<nn>/s/sys/general.cfg
```

Table 11: Internationalization Options

Parameter	Description
UXO_MIME_TEXTFILE_CHARSET= <cs1>,<cs2>,...	Where <cs1> and <cs2> are comma separated character sets that the text and HTML content is converted to, with the one with least potential loss count selected. Supports per domain text character set conversion, ahead of the steering file settings.

Internet Addressing Options

You can set these options in the general configuration file:

```
/var/opt/scalix/<nn>/s/sys/general.cfg
```

Table 12: Internet Addressing Options

Parameter	Description
INET_AUTOGEN_IA_ON_MODIFY= FALSE	Determines whether the commands <code>ommodmn</code> , <code>ommodu</code> , <code>ommodpd</code> , <code>ommodent</code> , and <code>omldapmodify</code> generate Internet addresses automatically, when automatic Internet address mapping is in operation. The default is <code>FALSE</code> .
INET_DISPLAY_IA_COMMENTS= TRUE	Determines whether the POP3 and IMAP4 interfaces display the comment, or display name, part of an Internet address in a message. The default is <code>TRUE</code> . Set the option to <code>FALSE</code> to prevent the comment part of the Internet address from being displayed.
INET_INLINE_FILE_MAX_SIZE= <i>bytes</i>	Determines which body parts of MIME messages generated by the Internet mail gateway are inline and which are attachments. Body parts whose size is greater than the value of this option are attachments, while other body parts are inline. 0 — All body parts to be inline -1 — All body parts to be attachments

Table 12: Internet Addressing Options

Parameter	Description
INET_INLINE_FNAME_ALLOWED=FALSE	Determines whether MIME messages generated by the Internet gateway or prepared for browsing by POP3 or IMAP4 clients can have <code>filename=</code> in inline body part <code>Content-Disposition</code> lines. If the option is set to <code>FALSE</code> (the default), inline body parts cannot have <code>filename=</code> in the <code>Content-Disposition</code> line even if a candidate file name exists. Set this option to <code>TRUE</code> to allow inline body parts to have <code>filename=</code> in the <code>Content-Disposition</code> line, if a candidate file name has been selected.
INET_NO_IA_IN_ORN=FALSE	Determines whether the incoming Internet mail gateway saves the Internet address of the sender, each recipient, and distribution list member in the Scalix message. When set to <code>FALSE</code> (the default), the addresses are saved in the message. Note that this option applies to the names of Internet mail users and not to the names of Scalix users.
INET_NO_IA_COMMENTS=FALSE	Determines whether comments present in Internet addresses are included without alteration in outgoing messages. The default is <code>FALSE</code> , causing such comments to be included.
INET_USE_AUTO_IAM=TRUE	Specifies whether Internet addresses are automatically created when configuring users, and mapped at the Internet mail gateway and the POP3 and IMAP interfaces.

Internet Mail Gateway Options

You can set these options in the general configuration file:

```
/var/opt/scalix/<nn>/s/sys/general.cfg
```

Table 13: Internet Mail Gateway Options

Parameter	Description
BRW_INLINE_PARTS=1	Specifies the number of parts in a multipart item that are marked as inline if there is no other information about the part. The default is 1.
BRW_ITEMSUB_IS_FNAME=TRUE	For those items that do not have an Original Filename specified, determines whether the Subject of the item is used to generate a file name for the item. Leave this option at its default (<code>TRUE</code>) to use the item Subject as the file name (provided the value of <code>BRW_T61_ITEMSUB_IS_FNAME</code> has not caused a file name to be generated). Encoding is determined by <code>BRW_MIME_FNAME_ENCODING</code> . Note that if <code>BRW_MIME_FNAME_ENCODING=D</code> then this takes precedence over <code>BRW_ITEMSUB_IS_FNAME</code> . Set the option to <code>FALSE</code> to prevent the Subject from being used to generate the file name (although a file name can still be generated using one of the other fields).

Table 13: Internet Mail Gateway Options

Parameter	Description
BRW_MIME_EXPLICIT_ASCII=FALSE	Specifies the character set to be US-ASCII for plain text content types. The MIME standards specify the default character set to be US-ASCII for text/plain content types, so you can leave this at its default (<code>FALSE</code>) unless your client cannot display such content unless the character set is explicitly defined.
BRW_MIME_FNAME_ENCODING=Q	Specifies the method for encoding MIME names and file names used in the POP3 and IMAP4 interfaces. The possible values are: D — Forces outgoing non-text file name to meet DOS file name conventions N — No encoding Q — Quoted-printable encoding; this is the default B — Base64 encoding
BRW_MIME_OMIT_DEF_CTENC_HDR=T, Y, F, or N	If set to <code>T</code> for <code>TRUE</code> or <code>Y</code> for <code>YES</code> , the Content-Encoding header is omitted if it is the default 7 bit. The default is <code>F</code> or <code>N</code> .
BRW_MIME_SPACE_OK_IN_FNAME=TRUE	Specifies that spaces are allowed in file names based on the T.61 subject of a body part.
BRW_MIME_SUBJ_BENC_NONASCII=T, Y, F, or N	When <code>BRW_MIME_SUBJECT_ENCODING</code> is set to <code>B</code> for base64 encoding, you can set this option (using either <code>T</code> for <code>TRUE</code> or <code>Y</code> for <code>YES</code>), to encode only non-ASCII characters in MIME subjects using base64. The default is <code>F</code> or <code>N</code> .
BRW_MIME_SUBJ_NO_SPACE_SEPS=FALSE	If set to <code>TRUE</code> or <code>YES</code> , a space separator between encoded and non-encoded data is not generated. This option can only be set when <code>BRW_MIME_SUBJECT_ENCODING=B</code> and <code>BRW_MIME_SUBJ_BENC_NONASCII=T</code> . The default is <code>FALSE</code> or <code>NO</code> . Note that setting this option generates messages in a form that is not strictly compatible with RFC 1522.
BRW_MIME_SUBJECT_CHARSET=NULL	Specifies the POP3 and IMAP4 MIME subject character set when it is different from the body part text. This option is for RFC 1557, which uses ISO-2022-KR in the body part text and EUC-KR (equivalent to KSC5601) in the subject.
BRW_MIME_SUBJECT_ENCODING=D, N, Q, or B	Specifies the method for encoding the message subjects of MIME messages retrieved from the POP3 and IMAP4 servers. The methods available are: D — Forces outgoing non-text file name to meet DOS file name conventions N — No encoding Q — Quoted-printable encoding; this is the default B — Base64 encoding
BRW_MIME_SUBJECT_FOLDING=T, Y, F, or N	If set to <code>T</code> or <code>Y</code> , folds subject headers according to RFC 1522 rules (at 76 bytes after encoding). Multibyte characters are sometimes folded at slightly less, to avoid splitting characters and to handle escape sequences correctly. The default is <code>F</code> or <code>N</code> .

Table 13: Internet Mail Gateway Options

Parameter	Description
BRW_MIME_TEXTFILE_ENCODING= 7, 8, ?, N, Q, or B	<p>Specifies the method for encoding the message texts of MIME messages retrieved from the POP3 and IMAP4 servers. The methods available are:</p> <ul style="list-style-type: none"> 7 — “7bit encoding” where if every line of text meets the RFC rules and only contains seven-bit data, then this method is used 8 — “8bit encoding” where if every line of text meets the RFC rules and contains at least some eight-bit data, then this method is used ? — Use the relevant mapping in the mime.types file (the default) N — No encoding Q — Quoted-printable encoding; this is the default B — Base64 encoding <p>More than one choice is allowed, separated by a comma. Example: 7,Q,B Select the choice based on actual content data.</p>
BRW_NAME_MAPPING=FALSE	<p>If set, the originator’s name and address are mapped to the keyed <code>INTERNET-ADDR</code> attribute (number 167) in the directory entry for that user. The directory entry must contain the user name and domain name in the format expected by Sendmail. Routing set up within Scalix and Sendmail must correspond to the addresses used in mappings.</p> <p>Note that mappings occur only when there is an exact match between the name and address in the message and the directory entry attribute <code>INTERNET-ADDR</code>.</p> <p>You can specify which directory to use for name/address mappings using the <code>UX_NAME_MAPPING_DIR</code> option.</p> <p>You can specify a directory entry attribute to use other than <code>INTERNET-ADDR</code> using the <code>UX_NAME_MAPPING_ATTRIB</code> option.</p> <p>The default is <code>FALSE</code>.</p>
BRW_NO_RETAIN_IF_CONVERTED= FALSE or <i>filetype</i>	<p>Determines if a message containing an alternative file type read through the POP3 or IMAP4 server retains the original format file along with the converted plain text version.</p> <p>By default, this option is set to <code>FALSE</code>; alternative file types are retained along with the converted plain text version.</p> <p>If set to <code>TRUE</code>, the alternative file is discarded after it has been converted into a text file. The resultant MIME message is created using just the converted text file.</p> <p><i>filetype</i> is a file type (or a comma-separated list of file types) configured in Scalix to be discarded. For example, to discard an original RTF file after conversion to plain text, set this option to <code>BRW_NO_RETAIN_IF_CONVERTED=2130</code>.</p>
BRW_T61_ITEMSUB_IS_FNAME=F	<p>If set to <code>T</code>, the T61 item subject is used for the file name when browsing POP3 and IMAP4 mail messages. The encoding is determined by the setting of <code>BRW_MIME_FNAME_ENCODING</code>; if <code>BRW_MIME_FNAME_ENCODING</code> is set to <code>D</code>, it takes precedence over this option. The default is <code>F</code>.</p>
INET_USE_X400_ATTS_FOR_LOOKUP =TRUE	<p>Determines whether name mapping, using directory lookup, at the outgoing Internet mail gateway uses only X.400 attributes.</p> <p>When this option is <code>TRUE</code> (the default), the outgoing Internet mail gateway only uses X.400 attributes when it performs directory lookup to map O/R addresses to Internet addresses.</p>

Table 13: Internet Mail Gateway Options

Parameter	Description
MAX_MIME_BROWSERS=25	Specifies the maximum number of MIME browsers that the MIME browser controller can have in its pool. The default is 25 browsers. Specify a higher value to provide a faster response to IMAP4 and POP3 connection requests. Specify a lower value to conserve system resources.
MIME_CACHE_TARGET_SIZE=1	Specifies the target size in megabytes of the MIME cache (<i>/var/opt/scalix/<nn>/s/temp/mime_cache</i>). The cache can grow larger than this if everything in the cache is being used, but unused items are deleted to keep the size under control. The default is 1.
MIN_MIME_BROWSERS=0	Specifies the minimum number of MIME browsers that the MIME browser controller can have in its pool. The default is 0 browsers. When the MIME browser controller starts, it starts the number of browsers specified by this option.
UX_MIME_SUBJECT_CHARSET= <i>client_character_set</i>	Specifies the character set to be used for the incoming and outgoing MIME subject, when it is different from the body part text. <i>client-character-set</i> is the name of any client character set configured in Scalix. For example, KSC5601 for the Korean language, as per RFC 1557, which uses ISO-2022-KR in the body part text and EUC-KR (equivalent to KSC5601) in the subject. Note that the Scalix server set name is KS5601 and not EUC-KR.
UX_NAME_MAPPING_ATTRIB= <i>attribute_tag</i>	Specifies a directory entry attribute to use other than <code>INTERNET-ADDR</code> . <i>attribute_tag</i> is the internal (numeric) form of the Scalix attribute.
UX_NAME_MAPPING_DIR= <i>directory_name</i>	If set, the directory you specify here is used to map the originator or recipient's name and address to an Internet address specified in the <code>INTERNET-ADDR</code> attribute of the user's directory entry, as the message passes through the Internet mail gateway. The directory must be a shared directory. If this option is not set, the default system directory is used. See also the <code>UX_NAME_MAPPING_DIR_PASSWD</code> option.
UX_NAME_MAPPING_DIR_PASSWD= <i>password</i>	If you set the <code>UX_NAME_MAPPING_DIR</code> option, you can specify a directory password using this option.
UX_NO_ROUTE_CHECK=TRUE	If set, the Internet mail gateway does not check O/R addresses in the incoming messages. Normally, the Internet mail gateway checks if valid routes are configured for O/R addresses in the ARPA heading information of each incoming message.
UX_PRE_5_20_COMPATIBILITY_MODE=TRUE	When set to <code>TRUE</code> (the default), this option causes Scalix to create a <code>WINMAIL.DAT</code> attachment for outgoing messages that contain MAPI properties, and to not decode <code>WINMAIL.DAT</code> attachments for incoming messages.
UX_USE_ARPA_SENDER=TRUE	If set, the incoming Internet mail gateway constructs the Scalix "From" address of incoming messages from the value of the Sender: token in the ARPA header rather than from the SMTP <code>Mail From</code> command.

Table 13: Internet Mail Gateway Options

Parameter	Description
UXI_AUTO_REPLY_BULK_MAIL=FALSE	<p>Specifies whether the incoming Internet mail gateway allows auto-replies to bulk mailing list messages.</p> <p>Bulk mailing list messages are those that contain one of the following lines in the ARPA header:</p> <p>Precedence: bulk Precedence: list Precedence: junk</p> <p>When set to <code>FALSE</code> (the default), bulk mailing list messages are treated similar to auto-forwarded messages, and do not allow auto-replies.</p> <p>Set this option to <code>TRUE</code> to allow auto-replies to bulk mailing list messages.</p>
UXI_DDATYPE_HPMEXT=TRUE	<p>A domain-defined attribute (DDA) is used when address mapping is required to some component of the Originator/Recipient (O/R) name. For example, if you do not map G for given name, S for surname, C for country, and so on for your e-mail system, then you need to use a DDA for mapping.</p> <p>If set, then messages coming in through the Internet mail gateway that have their Internet mail addresses copied into the DDA of the Scalix addresses use a DDA with a type of <code>HPMEXT1</code> rather than the default <code>RFC-822</code>.</p>
UXI_DO_1327_SENDER_MAP=TRUE	<p>When set, the ARPA Sender of an Internet message displays as the Creator of the message. Any replies to this message are therefore sent to the Sender. This is the behavior described in RFC 1327. Note that this cannot be the required behavior; for example, it means that Replies to a mailing list can be directed to the Creator, rather than to the subscribers.</p>
UXI_KEEP_ARPA_ADDRESS=TRUE	<p>If set, the Internet mail gateway preserves the ARPA address of an incoming message even when the header contains an ARPA-encoded Scalix address. Normally, the Internet mail gateway checks the ARPA heading information of each incoming message and, when there is an ARPA encoding of a Scalix address, the ARPA address is discarded and the Scalix address used instead.</p>
UXI_KEEP_MIME_ARPA_HEADER=TRUE	<p>If set, the Internet mail gateway includes the ARPA header of an incoming MIME message in the Scalix message.</p>
UXI_KEEP_UUENC_ARPA_HEADER=TRUE	<p>If set, the Internet mail gateway includes the ARPA header of an incoming UUENCODE message in the Scalix message. UUENCODE refers to binary-to-text encoding and is associated with UNIX and the UUCP mail system.</p>
UXI_MIME_CS_AUTODETECT= <i>boolean</i>	<p>Scalix can scan incoming MIME and UNIX message formats, to check whether they have been labeled with an incorrect character set and are actually another character set type that Scalix can recognize with a higher degree of certainty.</p> <p>When this option is not defined, auto-detection is done when the character set information is not supplied. This is the default.</p> <p>When <code>FALSE</code>, no auto-detection is done, even when character set information is not supplied. This can increase Internet gateway performance</p> <p>When set to <code>TRUE</code>, auto-detection is always attempted, even when character set information is supplied.</p>

Table 13: Internet Mail Gateway Options

Parameter	Description
UXI_NAME_MAPPING=TRUE	<p>If set, the originator's name and address are mapped to the keyed <code>INTERNET-ADDR</code> attribute (number 167) in the directory entry for that user. The directory entry must contain the user name and domain name in the appropriate format. Routing set up within Scalix and Sendmail must correspond to the addresses used in mappings.</p> <p>Mappings occur only when there is an exact match between the name and address in the message and the directory entry attribute <code>INTERNET-ADDR</code>. You can specify which directory to use for name/address mappings using the <code>UX_NAME_MAPPING_DIR</code> option.</p> <p>You can specify a directory entry attribute to use other than <code>INTERNET-ADDR</code> using the <code>UX_NAME_MAPPING_ATTRIB</code> option.</p>
UXI_NO_CONVERT_REPORTS=FALSE	<p>When set to <code>FALSE</code>, Internet acknowledgements and acknowledgement requests are converted to their Scalix equivalents. If you set this option to <code>TRUE</code>, they are not converted, but are passed into Scalix as messages.</p>
UXI_NO_INET_OBJFILES=FALSE	<p>When set to <code>FALSE</code>, the contents of Internet headers are preserved in object files. Certain clients, such as the IMAP4 and POP3 clients, can make use of these object files.</p> <p>If set to <code>TRUE</code>, Scalix does not create these object files, and the header information is lost.</p>
UXI_NO_UUDECODE_STRING= <i>text string</i>	<p>If set, UUENCODEd parts of messages that are not of a recognized format, such as MIME or RFC1154, are not decoded when the message body contains a text string that matches the one you specify here. If this option is not set, or no text string is supplied for it, such messages have their UUENCODEd parts decoded into separate binary attachments. UUENCODE refers to binary-to-text encoding and is associated with UNIX and the UUCP mail system.</p>
UXI_PASSIVE_RECIPS_MAPI_ENABLED=FALSE	<p>Determines whether passive recipients (that is, those recipients for which the Internet mail gateway does not have responsibility) appear to Microsoft Outlook users with the "Send In RTF" flag set.</p> <p>When this option is set to <code>FALSE</code> (the default), then such recipients are assumed not to be MAPI-enabled, and the "Send In RTF" flag is not set. Set this option to <code>TRUE</code> to have the "Send In RTF" flag set for these recipients.</p>
UXI_PRESERVE_MAPI_MSG_CLASS=FALSE	<p>Specifies whether the MAPI message class of certain incoming messages is converted.</p> <p>To interoperate with Microsoft Exchange, the Internet mail gateway must convert the MAPI message class of certain messages received from the Microsoft Exchange Internet mail connector for the Scalix MAPI service providers. The default is <code>FALSE</code>.</p> <p>See also the <code>UXO_PRESERVE_MAPI_MSG_CLASS</code> option.</p>
UXI_SUPPRESS_ARPA_HEADER=TRUE	<p>Suppresses, at a system level, the generation of the ARPA header for incoming messages from the Internet mail gateway.</p> <p>Note that MIME-encoded messages have ARPA headers suppressed by default. To enable MIME-encoded messages to have ARPA headers, you must set <code>UXI_KEEP_MIME_ARPA_HEADER=TRUE</code>.</p>

Table 13: Internet Mail Gateway Options

Parameter	Description
UXI_TREAT_AS_MIME_SUBJECT= T or Y	If set to T for TRUE or Y for YES , incoming messages from the Internet mail gateway's UUENCODE or SHAR route (in other words, messages in which the ARPA headers did not contain a <code>Mime-Version: 1.0</code> tag) but which have MIME-conformant subjects, have their subjects decoded as if they came via the MIME route, and are subject to all other settings for MIME subjects.
UXI_UNIX_MAIL_CHARSET= <i>character_set</i>	Specifies the non-Latin character set used in messages coming in through the Internet mail gateway. For Latin character sets, Scalix assumes the same character set is being used as was used for outgoing messages; that is, the character set to which ISO8859/1 text was converted to in the <i>unixout.str</i> or <i>mimeout.str</i> file. If the <code>UXI_UNIX_MAIL_CHARSET</code> option is set, the file <i>~/sys/unixin.str</i> or <i>mimein.str</i> can be used to specify conversions from this character set to a suitable interchange character set.
UXI_UUDECODE_ARPA_TOKEN= <i>string</i>	Specifies the token which, if present in the ARPA header of an incoming Internet mail message, results in any UUENCODEd parts in the message being decoded. The default is to decode UUENCODEd parts in all messages. To prevent any messages containing UUENCODEd message parts from being decoded (except those that conform to RFC 1154), specify a null ("") string.
UXO_ADD_DELIM=TRUE	Specifies that a leading / is inserted in front of an O/R address that is being used within Internet mail. The / is inserted only if the O/R address is format 2 (attribute format) and is enclosed in inverted commas. (This is done when attributes in the O/R address contain characters that have a special meaning to Internet mail.) Inserting the / ensures that Sendmail identifies the message as a message for Scalix.

Table 13: Internet Mail Gateway Options

Parameter	Description
<p>UXO_CHECK_TYPES_OF_DDA= <i>DDA_type</i></p>	<p>Specifies the DDA types that are acceptable as valid Internet addresses, to enable the UAL client interface and the Internet mail gateway to route the message to the correct destination for the recipient. A domain-defined attribute (DDA) is used when address mapping is required to some component of the Originator/Recipient (O/R) name. For example, if you do not map G for given name, S for surname, C for country, and so on for your e-mail system, then you need to use a DDA for mapping. The User Access Layer (UAL) refers to a proprietary Scalix protocol that enables communication between clients and the Scalix server.</p> <p><i>DDA_type</i> is one of the following:</p> <p>One or more valid DDA types, for example: RFC-822 HPMEXT1 HPMEXT2 HPMEXT3 HPMEXT4</p> <p>You can specify up to 10 DDA types, separated with commas. For example: RFC-822, HPMEXT1, HPMEXT2, HPMEXT3, HPMEXT4</p> <p>FALSE No DDA type checking is performed. This behavior is as for Scalix systems before B.05.10.</p> <p>If your Scalix directory contains DDAs with no type specified and they are not valid Internet addresses, you are recommended to set this option to: UXO_CHECK_TYPES_OF_DDA=RFC-822, HPMEXT1, HPMEXT2, HPMEXT3, HPMEXT4</p> <p>If this option is not present, the default setting is: UXO_CHECK_TYPES_OF_DDA=, RFC-822, HPMEXT1, HPMEXT2, HPMEXT3, HPMEXT4 The leading comma means that DDAs with no type specified are also acceptable as valid Internet addresses.</p>
<p>UXO_ITEMSUB_IS_FNAME=FALSE</p>	<p>If set to TRUE, the item subject is used for the file name in outgoing MIME Internet mail messages, if no original file name is present and if UXO_T61_ITEMSUB_IS_FNAME has not caused a file name to be generated. The encoding is determined by the setting for UXO_MIME_FNAME_ENCODING; if UXO_MIME_FNAME_ENCODING is set to D, it takes precedence over this option. The default is FALSE; this setting prevents a file name from being generated from the item subject for the Content-Disposition header.</p> <p>See also: UXO_MIME_FNAME_ENCODING UXO_T61_ITEMSUB_IS_FNAME INET_INLINE_FNAME_ALLOWED</p>

Table 13: Internet Mail Gateway Options

Parameter	Description
UXO_MIME_FNAME_ENCODING= D, N, Q, or B	Specifies how MIME names and file names are encoded at the outgoing Internet mail gateway. The options are: D — Forces outgoing non-text file name to meet DOS file name conventions N — No encoding Q — Quoted-printable encoding; this is the default B — Base64 encoding
UXO_MIME_OMIT_DEF_CTENC_HDR= T or Y	If set to T for TRUE or Y for YES, the Content-Encoding header is omitted if it is the default 7 bit.
UXO_MIME_SPACE_OK_IN_FNAME= TRUE	Specifies that spaces are allowed in file names based on the T.61 subject of a body part.
UXO_MIME_SUBJ_NO_SPACE_SEPS= TRUE	If set to TRUE or YES, a space separator between encoded and non-encoded data is not generated. This option can only be set when UXO_MIME_SUBJECT_ENCODING=B and UXO_MIME_SUBJ_BENC_NONASCII=T. Note that setting this option generates messages in a form that is not strictly compatible with RFC 1522.
UXO_MIME_SUBJECT_BENC_ NONASCII=T	When UXO_MIME_SUBJECT_ENCODING is set to B for base64 encoding, you can set this option (using either T for TRUE or Y for YES), to encode only non-ASCII characters in MIME subjects using base64.
UXO_MIME_SUBJECT_ENCODING= N, Q, or B	Specifies the method for encoding MIME subjects of outgoing messages. The methods available are: N — No encoding Q — Quoted-printable encoding; this is the default B — Base64 encoding If UXO_MIME_FNAME_ENCODING is not set, this option is used for file name encoding, as well.
UXO_MIME_SUBJECT_FOLDING=T or Y	Folds subject headers according to RFC 1522 rules (at 76 bytes after encoding). Multibyte characters are sometimes folded at slightly less, to avoid splitting characters and to handle escape sequences correctly. Enter either T for TRUE or Y for YES to set this option.
UXO_MIME_TEXTFILE_ENCODING= 7, 8, N, Q, or B	Specifies the method for encoding message text of outgoing MIME messages. The methods available are: 7 — “7bit encoding” where if every line of text meets the RFC rules and only contains seven-bit data, then this method is used 8 — “8bit encoding” where if every line of text meets the RFC rules and contains at least some eight-bit data, then this method is used N — No encoding Q — Quoted-printable encoding; this is the default B — Base64 encoding More than one choice is allowed, separated by a comma. Example: 7,Q,B Select the choice based on actual content data.

Table 13: Internet Mail Gateway Options

Parameter	Description
UXO_NAME_MAPPING=TRUE	<p>If set, the recipient's name and address are mapped to the keyed <code>INTERNET-ADDR</code> attribute (number 167) in the directory entry for that user. The directory entry must contain the user name and domain name in the format expected by Sendmail. Routing set up within Scalix and Sendmail must correspond to the addresses used in mappings.</p> <p>If the recipient already has an Internet mail name and address configured in the DDA fields in the message or in the entry retrieved from the directory, this is used in preference to the <code>INTERNET_ADDR</code> attribute value.</p> <p>You can specify which directory to use for name/address mappings using the <code>UX_NAME_MAPPING_DIR</code> option.</p> <p>You can specify a directory entry attribute to use other than <code>INTERNET-ADDR</code> using the <code>UX_NAME_MAPPING_ATTRIB</code> option.</p>
UXO_NO_RETAIN_IF_CONVERTED=FALSE or <i>filetype</i>	<p>Determines if a message containing an alternative file type sent through the Internet mail gateway retains the original format file along with the converted plain text version.</p> <p>By default, this option is set to <code>FALSE</code>; alternative file types are retained along with the converted plain text version.</p> <p>If set to <code>TRUE</code>, the alternative file is discarded after it has been converted into a text file. The resultant MIME message is created using just the converted text file.</p> <p><i>filetype</i> is a file type (or a comma-separated list of file types) configured in Scalix to be discarded. For example, to discard an original RTF file after conversion to plain text, this option is set to</p> <p><code>UXO_NO_RETAIN_IF_CONVERTED=2130</code></p>
UXO_PRESERVE_MAPI_MSG_CLASS=FALSE	<p>Specifies whether the MAPI message class of certain outgoing messages is converted.</p> <p>To interoperate with Microsoft Exchange, the Internet mail gateway must convert the MAPI message class of certain messages destined for the Microsoft Exchange Internet mail connector for the Scalix MAPI service providers.</p> <p>The default is <code>FALSE</code>.</p> <p>See also the <code>UXI_PRESERVE_MAPI_MSG_CLASS</code> option.</p>
UXO_SHAR_ARGS= <i>arguments</i>	<p>Specifies the arguments used by the shell archive (SHAR) program when it is started by the Internet mail gateway. The default arguments are <code>-bc</code>. See also <code>UXO_SHAR_COMMAND</code>.</p>
UXO_SHAR_COMMAND= <i>command</i>	<p>Specifies the program used by the Internet mail gateway to create a shell archive package. The default is <code>shar</code>. See also <code>UXO_SHAR_ARGS</code>.</p>
UXO_T61_ITEMSUB_IS_FNAME=T	<p>If set, the T61 item subject is used for the file name in outgoing MIME Internet mail messages. The encoding is determined by the setting for <code>UXO_MIME_FNAME_ENCODING</code>; if <code>UXO_MIME_FNAME_ENCODING</code> is set to <code>D</code>, it takes precedence over this option.</p>
UXO_TREAT_AS_MIME_SUBJECT=T or Y	<p>If set to <code>T</code> for TRUE or <code>Y</code> for YES, messages going out via the Internet mail gateway's UUECODE or SHAR route that have MIME-conformant subjects have their subjects encoded as if going out via the MIME route, and are subject to all other settings for MIME subjects.</p>

Table 13: Internet Mail Gateway Options

Parameter	Description
UXO_USE_SENDER_DDA=TRUE	Specifies whether a domain-defined attribute (DDA) is used directly when mapping the sender address in the outgoing Internet mail gateway. If set to <code>TRUE</code> , the Internet mail gateway maps DDAs in the sender address in the same way as it does for DDAs in the recipient address; that is, any Internet address specified in the DDA is used directly. If this option is not present or is set to <code>FALSE</code> , the Internet mail gateway does not use the DDA directly when mapping the Internet address of the sender.

Item Structure Server Options

You can set these options in the general configuration file:

```
/var/opt/scalix/<nn>/s/sys/general.cfg
```

Table 14: Item Structure Server Options

Parameter	Description
ISL_DISABLE_LOGGING=TRUE	Disables logging by the item structure server of structural changes made to the Message Store. This option is set when the item structure database is not required, in order to save disk space. This option takes precedence over <code>ISL_LOG_IF_OFF=TRUE</code> .
ISL_LOG_IF_OFF=TRUE	Enables logging of structural changes made to the Message Store, when the item structure server daemon is not running. Logging is performed directly to the item structure server log files, which reduces performance. The <code>ISL_DISABLE_LOGGING=TRUE</code> option takes precedence over this one.

Local Delivery Service Options

You can set these options in the general configuration file:

`/var/opt/scalix/<nn>/s/sys/general.cfg`

Table 15: Local Delivery Service Options

Parameter	Description
LD_ADD_ACKS_AS_TO=	If set, the address returned in an acknowledgement that cannot be matched in the original distribution list of the message in the Outbox is added to the distribution list as a “To” record rather than as a “New Recipient” record.
LD_AUTOREPLY_CHECK_ON=TRUE	Each time a user configures auto-reply, Scalix creates a text file in the user’s <code>/g</code> folder under <code>~/user/</code> that contains a list of addresses to which automatic replies have been sent since the current auto-reply session was created. With this option set, the local delivery service checks users’ address list files against the address in each received message’s transaction file. If a match is found, an automatic reply is not generated. This prevents more than one automatic reply from being generated for each unique sender address.
LD_AUTOREPLY_EXPIRY_TIME= <i>no_of_days</i>	Specifies the number of days an address can be present in the auto-reply address list file before it is removed. If you specify two days, for example, a person receives an out-of-office notice every two days instead of every day or each time.
LD_MAX_NEST_LEVEL= <i>depth</i>	Specifies the maximum level of nesting allowed in a message before further nested parts are flattened by the local delivery service. A value of 0 means that all delivered messages are flattened. See <code>SR_MAX_NEST_LEVEL</code> for more information.
LD_READ_ACK_ON_AUTOPRINT= FALSE	If set, when a message is automatically printed, no “read” acknowledgement is returned to the originator. The default is to return a “read” acknowledgement when a message is automatically printed.
LD_TRACE_DISP_ACT=SHOW_ADMIN	Shows trace information on all messages received by anyone with Scalix administration permissions.

LDAP Server Options

You can set these options in the general configuration file:

```
/var/opt/scalix/<nn>/s/sys/general.cfg
```

Table 16: LDAP Server Options

Parameter	Description
LDAP_MB_CN_IS_GS_IN_FILTER=FALSE	<p>This option only has effect when the LDAP session is multibyte, and you have not created an explicit Scalix attribute <code>COMMONNAME</code>.</p> <p>When the LDAP client sends a search filter that contains the LDAP <code>COMMONNAME</code> attribute, the LDAP server uses a built-in parsing method to determine how to convert this to Scalix attributes. By default, it assumes that the <code>COMMONNAME</code> attribute contains the Scalix attributes <code>SURNAME</code>, <code>GIVENNAME</code> in that order.</p> <p>If your LDAP clients construct <code>COMMONNAME</code>s in the reverse order, you must set this option to <code>TRUE</code>.</p> <p>For example, if your LDAP client uses “<code>Japanese-surname Japanese-givenname</code>” as the <code>COMMONNAME</code>, leave this option at its default. The LDAP server correctly interprets this as <code>GIVENNAME=Japanese-givenname</code> and <code>SURNAME=Japanese-surname</code>.</p> <p>But if your LDAP client uses <code>Japanese-givenname Japanese-surname</code> as the <code>COMMONNAME</code>, the LDAP server interprets this as <code>GIVENNAME=Japanese-surname</code> and <code>SURNAME=Japanese-givenname</code> unless you set this option to <code>TRUE</code>.</p>
LDAP_MB_CN_IS_GS_IN_SYNTH_OUT=FALSE	<p>This option only has effect when the LDAP session is multibyte, and you have not created an explicit Scalix attribute <code>COMMONNAME</code>.</p> <p>When the LDAP server synthesizes the LDAP <code>COMMONNAME</code> attribute using the Scalix attributes <code>SURNAME</code> and <code>GIVENNAME</code>, it puts them in the order <code>SURNAME</code>, <code>GIVENNAME</code>.</p> <p>If you want <code>COMMONNAME</code>s to appear in the reverse order, you set this option to <code>TRUE</code>.</p> <p>For example, if set to <code>FALSE</code> (default), the name “<code>Japanese-givenname Japanese-surname</code>” is returned from the LDAP server as <code>Japanese-surname Japanese-givenname</code>.</p> <p>But if set to <code>TRUE</code>, the name is returned as <code>Japanese-givenname Japanese-surname</code>.</p>
LDAP_SEQUENTIAL_SEARCH=TRUE or FALSE	<p>If you do not set this option, the LDAP server does not, in general, issue sequential searches of the Scalix directories. Instead, it searches using the indexes of keyed attributes, to keep search time to a minimum.</p> <p>However, it issues sequential searches under certain circumstances, such as when the <code>DA_IGNORE_INDEXES</code> option is set to <code>TRUE</code>.</p> <p>Set this option to <code>TRUE</code> to have the LDAP server issue sequential searches. This enables you to search for attributes that are not keyed, but searches can take a long time.</p> <p>Set this option to <code>FALSE</code> to prevent the LDAP server from issuing sequential searches. This keeps search times to a minimum, but can prevent the LDAP server from finding all entries that match a given filter.</p>

Table 16: LDAP Server Options

Parameter	Description
OMLDAP_REMOVE_LEADING_WILDCARDS=TRUE	<p>If present and set to <code>TRUE</code>, leading wildcard characters (*) are stripped from substring filters when the LDAP server searches a Scalix directory for entries that match criteria specified by a search filter. This option causes filters of the form “(cn=*name*)” to be converted to the form “(cn=name*)”. That is, the LDAP server matches the filter “(cn=name*)” to all entries in the underlying Scalix directory whose <code>SURNAME</code> or <code>COMMON-NAME</code> attributes start with <i>name</i>. This causes fewer system resources to be used when searching.</p> <p>If not present or set to <code>FALSE</code>, the leading wildcards are not stripped, and the LDAP server searches for all <code>SURNAME</code> or <code>COMMON-NAME</code> attributes containing <i>name</i>.</p> <p>For example, if <code>OMLDAP_REMOVE_LEADING_WILDCARDS</code> is set to <code>TRUE</code>, then “(cn=Marion Brand*)” matches all entries whose <code>SURNAME</code> starts with “Brand” or whose <code>COMMON-NAME</code> starts with “Marion Brand”. If set to <code>FALSE</code>, “Ann-Marion Brandson” is a match.</p>

Non-Delivery Notification Options

You can set these options in the general configuration file:

```
/var/opt/scalix/<nn>/s/sys/general.cfg
```

Table 17: Non-Delivery Notification Options

Parameter	Description
NDN_EM_SERIOUS_ONLY=TRUE	Sends non-delivery notifications (NDNs) for serious errors to the error manager, meaning the user account designated to receive such information (sxadmin by default). Sends non-delivery notifications for simple addressing problems to the originator. If this option is not set, no notifications for simple addressing problems are sent to the error manager or the originator.
NDN_NO_ALTERNATES=TRUE	If this option is set and the original message contained an ambiguous O/R name, alternate names are not placed in a non-delivery notification.

Notification Server Options

You can set these options in the general configuration file:

```
/var/opt/scalix/<nn>/s/sys/general.cfg
```

Table 18: Notification Server Options

Parameter	Description
NS_INITIAL_MEM=bytes	<p>Specifies the initial memory size of the notification server.</p> <p>Use this option to increase the initial memory size from 65536 bytes (default). This default is suitable for up to approximately 1200 configured and active users. You can increase this value if a larger number of users are configured such that, just after startup, the shared memory segment is repeatedly enlarged.</p>

Offline Folder Synchronization Options (Microsoft Outlook Clients)

You can set these options in the general configuration file:

`/var/opt/scalix/<nn>/s/sys/general.cfg`

Table 19: Offline Folder Synchronization Options

Parameter	Description
OFS_ENABLED=TRUE	Specifies whether folder synchronization is enabled on the Scalix server. The default is <code>TRUE</code> . If set to <code>TRUE</code> , it can be overridden on a per-user basis by setting it to <code>FALSE</code> in the relevant user-specific configuration files.
OFS_LOG_AGE_LIMIT=days	When the age of a change log entry exceeds this value, it can be deleted when the change log file is compacted. Use this option to prevent change logs from growing too large when logging is activated but synchronization is not taking place for any reason. Take care when you set this value, because removal of any valid entries causes the entire folder to be resynchronized. A value you set in the <i>general.cfg</i> file can be overridden on a per-user basis by setting a lower value for this option in the relevant user-specific configuration file.
OFS_LOG_SIZE_LIMIT=kilobytes	Specifies the maximum size in kilobytes of the folder synchronization change log. Set a value between 20 and 10000 KB. The default is 100 KB. When the size of a change log exceeds this value, the older entries are deleted when the change log file is compacted. Use this option to prevent change logs from growing too large when logging is activated but synchronization is not taking place for any reason. Take care when you set this value, because removal of any valid entries causes the entire folder to be resynchronized. A value you set in the <i>general.cfg</i> file can be overridden on a per-user basis by setting a lower value for this option in the relevant user-specific configuration file.
OFS_WORK_FILE_DIR=temp-dir	Specifies the location of the temporary files created during folder synchronization. Normally (when this option is not set), these temporary files are stored in the <code>~/temp</code> folder. Specify a value for this option to cause all these files to be written to a different location. This allows you to use a high-speed (and possibly low-recovery) file system (for example, a RAM disk) to store these temporary files. The folder you specify must have: <ul style="list-style-type: none"> • Permissions of 771 • A group of <code>scalix</code> • An owner of <code>scalix</code> • A path length of 225 characters or less For example, to create a folder called <i>temp-ofs</i> , enter the following commands: <pre>mkdir \$(omrealpath '~/temp-ofs') chown scalix:scalix \$(omrealpath '~/temp-ofs') chmod 771 \$(omrealpath '~/temp-ofs')</pre>

Omscan Options

The `omscan` command is used to monitor and repair the Scalix Message Store, message queues, and message lists. It can be used to delete temporary files and view disk space used by each user.

For example:

```
omscan -U "Jane Rogers"
```

returns

```
(KB)                INBOX  OUTBOX  SENT  OTHERS  TRASH  TOTAL  RCVRY
Jane Rogers /scalix1/CN=Jane R  2906   1    1454   27      1   4389   1
```

You can set `omscan` options in the general configuration file:

```
/var/opt/scalix/<nn>/s/sys/general.cfg
```

Table 20: Omscan Options

Parameter	Description
<code>GS_DONT_SPLIT_FC=FALSE</code>	If set to <code>TRUE</code> , <code>omscan</code> reports a single value for the size of a user's filing cabinet and trash combined, instead of separate figures for the filing cabinet and trash. In the example shown, the <code>TRASH</code> column is eliminated and its value is added to the <code>OTHERS</code> value. To view the effect immediately, run <code>omscan</code> in active mode, meaning add the <code>-A</code> option to the <code>omscan</code> command. Otherwise, to view the results with the <code>omscan</code> command, you need to restart the <code>omscan</code> server using <code>omoff/omon</code> and wait until the next server cycle gets done.
<code>SCN_KEEP_DATA_ORPHANS=FALSE</code>	If set to <code>FALSE</code> , files reported as orphans by <code>omscan</code> are deleted and not moved to the <code>~/orphans</code> folder.
<code>SCN_ORPHAN_DELETE_DELAY=number_of_days</code>	Sets the age limit for orphan files before they are reported by <code>omscan</code> and moved to the <code>~/orphans</code> folder. The default is 1 day.
<code>SCN_PREV_ORPHAN_DELETE_DELAY=number_of_days</code>	The number of days before a file in the <code>~/orphans</code> folder is deleted by the next run of <code>omscan -d</code> . The default is 30 days.
<code>SCN_TEMP_DELETE_DELAY=number_of_days</code>	Sets the age limit for files in <code>~/temp</code> before they are deleted by <code>omscan</code> . The default is 7 days.
<code>SCN_TMP_DELETE_DELAY=number_of_days</code>	Sets the age limit for files in <code>~/tmp</code> before they are deleted by <code>omscan</code> . The default is 7 days.

POP Server Options

You can set these options in the general configuration file:

```
/var/opt/scalix/<nn>/s/sys/general.cfg
```

Table 21: POP Server Options

Parameter	Description
POP3_IGNORE_SERVERNAME= FALSE	<p>Determines whether the POP3 server uses the characters following the @ character as the server name for a user.</p> <p>When set to <code>FALSE</code> (the default), the name part (up to and including the @ character) is stripped off and the remainder is used as the server name to which the POP3 connection is relayed.</p> <p>Set this option to <code>TRUE</code> to prevent the POP3 connection being relayed to another server.</p>
POP3_MAILSTORE_HOST= <i>hostname</i>	<p>Specifies the fully qualified domain name of the Scalix host to which the POP server connects, for example <code>omsvr1.acme.company.com</code>. Use this option when the POP server does not reside on the same computer as the Scalix system that contains the relevant message store.</p>
POP3_MAX_THREADS= <i>integer</i>	<p>Restricts the number of threads that a single pop3.server process uses. By default, the value used is the maximum allowed from system resources (including system thread limits as well as limits in available file descriptors). Specify a value here to limit the number of threads used to a value less than the default.</p> <p>If you specify a value higher than the default, it has no effect.</p>
POP3_RECORD_EMPTY_SIGNON= FALSE	<p>Determines whether POP3 user logins are recorded for empty Inboxes.</p> <p>When a user with items in their Inbox logs in using POP3, the login is recorded, and the last login time for the user is updated. This causes the login to take longer than if the login is not recorded.</p> <p>When set to <code>FALSE</code> (the default), if a user with an empty Inbox logs in using POP3, the login is not recorded and is faster.</p> <p>When set to <code>TRUE</code>, user login is recorded even when the user's Inbox is empty. This causes slower login, but allows you to determine the last login time for users or to use <code>omstat -u</code> and <code>omstat -s</code> to report on POP3 users.</p>

Public Folder Server Options

Public folders are also referred to as bulletin boards (BBS) in Scalix. You can set options in the general configuration file:

```
/var/opt/scalix/<nn>/s/sys/general.cfg
```

Table 22: Public Folder Server Options

Parameter	Description
BBS_ALLOW_LOCAL_SYNC=FALSE	Specifies whether public folder synchronization can occur between public folders on the same computer. When set to <code>FALSE</code> (default) and an attempt is made to synchronize public folders on the same computer, a warning message in the log file results.
BBS_CUST_CHECK_TIME= <i>minutes</i>	Sets the amount of time a public folder server spends in “import” mode before checking if any of its synchronization timers have expired. The default is 5 minutes. A public folder server toggles between import and export mode. It stays in import mode for the specified amount of time before checking the synchronization timers, and then if the timers have expired, it changes to export mode. When done all the exports, it changes back to import mode.
BBS_DELETE_MASTER_BY_SYNC=FALSE	Specifies whether deletion of a slave item from a public folder is not propagated to its master item. Set this option to <code>TRUE</code> if you want deletion of a slave item to result in deletion of its master item. (<code>BBS_PROPAGATE_SLAVE_DELETION</code> must also be set to <code>TRUE</code> for this to happen.)
BBS_DELLOG_RETENTION_PERIOD= <i>hours</i>	Specifies the retention period, in hours, for delete log files. The default is 24 hours.
BBS_PROPAGATE_SLAVE_DELETION=FALSE	Specifies whether deletion of a slave item from a public folder is propagated to any other slave copies or to the master item. Set this option to <code>TRUE</code> if you want deletion of a slave item to result in deletion of all other slave copies of this item. (<code>BBS_DELETE_MASTER_BY_SYNC</code> must also be set to <code>TRUE</code> if you want deletion of a slave item to result in deletion of its master.)
BBS_SEND_OBJECT_FILES=TRUE	Specifies whether object files attached to messages or items are included when the message or item is exchanged during the public folder synchronization process. If set to <code>TRUE</code> , any object files attached to messages or items are included when the message is sent to another public folder server. This option affects object files attached to messages or basic items on the public folder; object files attached directly to public folders are not synchronized.
BBS_SYNC_MSG_PRIORITY= <i>priority</i>	Specifies the priority with which public folder synchronization messages are sent. If public folder synchronization messages are slowing other Scalix operations, you can use a lower priority for such messages. Alternatively, if public folder synchronization messages take too long, you can use a higher priority. 0 — Normal 1 — Non-urgent 2 — Urgent

Queue Options

You can set these options in the general configuration file:

`/var/opt/scalix/<nn>/s/sys/general.cfg`

Table 23: Queue Options

Parameter	Description
QM_DONT_READ_MSG_AT_START=FALSE	<p>When set to <code>TRUE</code>, this option specifies that all messages currently in the Scalix queues remain stationary when Scalix is restarted. New messages are processed normally.</p> <p>Set this option to <code>TRUE</code> if a major problem is encountered when the queue manager attempts to read queued messages from disk when Scalix starts up. This allows Scalix to start. Set the option back to <code>FALSE</code> and restart Scalix when the problem is resolved.</p>
QM_FAILURE_DELAY_SEC= <i>seconds</i>	<p>Specifies the number of seconds between message retry by the queue manager. When a message fails to be processed because the process that was handling the message died, the queue manager delays the message for this number of seconds before retrying the message.</p> <p>The default is 30 seconds.</p> <p>See also <code>QM_MAX_FAILURES</code>.</p>
QM_MAX_FAILURES= <i>integer</i>	<p>Sets the number of times the queue manager attempts to retry a message before giving up and putting the message in the POISON queue.</p> <p>A failure occurs when the process that received the message dies before informing the queue manager that it has successfully dealt with the message.</p> <p>A value between 1 and 4 is normally suitable. A value of 0 causes the queue manager to place the message in the POISON queue immediately on failure (that is, no retries). Too large a value can cause services to abort repeatedly.</p> <p>See also <code>QM_FAILURE_DELAY_SEC</code>.</p>
Q_TIME_OUT= <i>seconds</i>	<p>Sets the amount of time processes attempting to read a request from a Scalix queue wait before timing-out. Setting this value low ensures that processes remain swapped-in. The default is 30 seconds.</p>

Recovery Folder Options

The Scalix Recovered Items folder can be made visible if a user hard-deletes an important e-mail or calendar item auto-expires from the Deleted Items folder. The default retention period is seven days.

You can set these options in the general configuration file:

```
/var/opt/scalix/<nn>/s/sys/general.cfg
```

Table 24: Recovery Folder Options

Parameter	Description
RECOVERY_FOLDER_EXPIRY_TIME= <i>time_period</i>	Set the amount of time that deleted items remain in the Scalix Recovered Items folder before being removed from the system. The default is seven days (7d). Sample settings for this option are: 4d12h (4 days and 12 hours) or 240h (240 hours). To disable recovery folder saving and never have messages saved to it, set the value to 0. You can also set this value on a client level.

Search Server Options

You can set these options in the general configuration file:

```
/var/opt/scalix/<nn>/s/sys/general.cfg
```

Table 25: Search Server Options

Parameter	Description
SE_DEFAULT_DELAY= <i>number_of_seconds</i>	Specifies the delay in seconds between runs of a persistent (that is, automatically repeated) background search of the Message Store. The search server checks for a specified delay in the following sequence: If a delay is specified in the search request transaction file, that delay is used. If no delay is specified in the search request transaction file or it is set to zero, the delay specified in this SE_DEFAULT_DELAY option is used. If no delay is specified either in the search request transaction file or the SE_DEFAULT_DELAY option, a default delay of 300 seconds is used.
SE_MAX_CHILDREN= <i>max_number_of_child_processes</i>	Specifies the maximum number of child search processes that the search server can create. Each child process can execute only one search at a time. This option limits the number of background searches that can be performed simultaneously, but not the number of background searches that can be queued. The default number of child processes is 20.
SE_MAX_OVERDUE_TIME= <i>number_of_seconds</i>	Specifies the time after which an overdue persistent background search takes priority over one-off searches. The search server normally gives priority to one-off searches. When the time specified in this option is reached, the search server gives a persistent search priority over the one-off searches. This prevents persistent searches from being permanently blocked by a long queue of one-off searches. The default time is 300 seconds.

Service Router Options

See the “Setting Message Delivery Rules on the Router” chapter to create rules to control message delivery, for example defer delivery of low-priority messages.

Otherwise, you can set Service Router options in the general configuration file:

```
/var/opt/scalix/<nn>/s/sys/general.cfg
```

X.400 and X.500 refer to standards for e-mail messages, such as using C for country and G for given name.

Table 26: Service Router Options

Parameter	Description
NDN_MSGFLAGS_OVERRIDE_RULE_ACTION_RETURN=FALSE	By default, messages created as a result of the RETURN action for a message delivery rule set has the original message attached, even if the original message has a flag specifying that contents must not be included in non-delivery notifications. If set to TRUE and the return of contents is not requested, the original message is not attached.
RSL_BLANK_SUBJECT_BS_CHAR=FALSE	If the subject mapper is a shell script, a message subject containing a backslash causes problems as the script interprets these as escape characters. The Service Router and Deferred Mail Manager replace any backslashes with an empty space. If the subject mapper is not a shell script, a backslash can be preserved by setting this option to FALSE.
SR_CONVERT_ISO7_FROM_UNIX=TRUE	If set, all textual body parts of messages coming in through the Internet mail gateway are converted to the ISO8859/1 character set, assuming the body parts contain IA5 characters with ISO-7 extensions. This option is only active if the SR_ISO7_HOST and SR_ISO7_language options are also present.
SR_CONVERT_ISO7_FROM_X400=TRUE	If set, all textual body parts of messages coming in through the X.400 Interface are converted to the ISO8859/1 character set, assuming the body parts contain IA5 characters with ISO-7 extensions. This option is only active if the SR_ISO7_HOST and SR_ISO7_language options are also present.
SR_CONVERT_ISO7_LANG= <i>language</i>	If set, activates the option SR_ISO7_language for messages passing through the Service Router. Only one instance of this option can be used and the language string must match a string in the <code>~/sys/LangMap</code> file. See also UAL_ISO7_HOST.
SR_CONVERT_ONLY_IA5=TRUE	Used in conjunction with SR_CONVERT_ISO7_FROM_UNIX and SR_CONVERT_ISO7_FROM_X400. If set, only textual body parts with a character set of IA5 are assumed to contain ISO-7 extensions and be eligible for conversion as specified by the options SR_ISO7_HOST and SR_ISO7_language.
SR_DUMP_MSGS=BEFORE or AFTER	Puts a copy of each message processed by the Service Router on the Dump Server queue DUMP. If set to BEFORE, the message is copied before it is processed by the Service Router. If the set to AFTER, the message is copied after it is processed by the Service Router.

Table 26: Service Router Options

Parameter	Description
SR_EXPAND_PDL=TRUE	<p>Sets the Service Router to perform Public Distribution List (PDL) expansion. When this option is set, the active distribution list of any message that is addressed to a PDL is expanded. (Expanded means a PDL entry is replaced by the full list of the recipients that it represents.) When a PDL has been expanded, the message is re-submitted to the Service Router.</p> <p>The Service Router expands PDLs that cannot be routed regardless of whether this option is set or not. SR_NO_ROUTE_PDL stops expansion when a message cannot be routed.</p>
SR_FILTER_TYPES_OF_ATT=TRUE	<p>Causes the Service Router to remove WINMAIL.DAT attachments, used by some clients.</p>
SR_ISO7_language=ISO7_characters	<p>Specifies how text using the ISO-7 extensions is converted to the ISO8859/1 character set by the Service Router.</p> <p>ISO7_characters is a list of ISO8859/1 characters to which the 12 special "ISO-7" characters are mapped. The IA5 characters used as special ISO-7 characters are:</p> <pre># \$ @ [] ^ ' { } ~</pre> <p>The ISO8859/1 equivalents (ISO7_characters) must be specified in the same order. Ensure that the ISO8859/1 equivalents are entered into the file using the ISO8859/1 character set.</p> <p>The language must correspond to the language set in the SR_CONVERT_ISO7_LANG option and the SR_CONVERT_ISO7_LANG option must be present to activate this option. See also SR_CONVERT_ISO7_FROM_UNIX and SR_CONVERT_ISO7_FROM_X400. Also UAL_ISO7_language.</p>
SR_LD_BYPASS_LSERV=TRUE	<p>When set to TRUE (default setting), the Service Router can bypass the Local Delivery Service and route a local message directly to the queue of one of the following Scalix services:</p> <ul style="list-style-type: none"> Public Folder Server Directory Synchronization Server Error Manager Server Print Server Request Server <p>By minimizing traffic through the Local Delivery Service, this option can reduce the amount of time required for directory synchronization, and increase the speed of other local traffic.</p> <p>If an ACL is associated with the Local Delivery Service, set this option to FALSE to prevent the ACL being bypassed when a message is being routed directly to one of the Scalix services listed above.</p>
SR_MAX_HOP_COUNT=hop_count	<p>Specifies the number of hops that a message can make before it is assumed to be looping. The default is 100.</p>
SR_MAX_NEST_LEVEL=nest_level	<p>Specifies the maximum level of nesting allowed in a message before further nested parts are flattened by the Service Router. A value of zero means that all messages are flattened. See also LD_MAX_NEST_LEVEL.</p>

Table 26: Service Router Options

Parameter	Description
SR_NO_ROUTE_PDL=TRUE	Stops Public Distribution List (PDL) expansion by the Service Router when a message cannot be routed. (Normally, if a message cannot be routed when there is a PDL within the message's distribution list, the Service Router expands the PDL, or PDLs, and tries to route the message again before returning a non-delivery notification.)
SR_Q_TIME_OUT= <i>seconds</i>	Specifies the time, in seconds, between checking the Service Router queue for new messages and checking for deferred messages that are due for submittal to the Service Router. The default is 30 seconds.
SR_RESOLVE_MASK= <i>number_of_ORname_fields</i>	<p>Specifies the directory attributes that are retained in the recipient address when the address is automatically resubmitted by the Service Router following a delivery failure. These attributes are specified as internal or language dependant attribute tags separated by forward slashes (/). If a message cannot be routed or delivered using the full recipient address, you can resubmit the recipient names with a less fully specified address by specifying how many O/R Name fields are retained when the name is resubmitted.</p> <p>For example:</p> <p>S/G/I/Q — This will retain the Personal Name attributes Surname, GivenName, Initials, and Generation Qualifier, such as Jr.</p> <p>CN/OU1 — This will retain the Common Name and Organizational Unit 1 attributes</p>

Table 26: Service Router Options

Parameter	Description
SR_ROUTE_X400_TO_OMX400_n= <i>route_match</i>	<p>Allows messages to be rerouted from the X400 queue to the OMX400 queue for recipients whose address matches the specified values. The X400 queue is used for messages routed to non-Scalix X.400 systems; the OMX400 queue is used for messages routed to other Scalix systems. This option must be set on the Scalix system that contains the X.400 gateway where this rerouting is required.</p> <p><i>n</i> is a number between 1 and 8. This enables you to specify up to 8 unique instances of this option in the general configuration file.</p> <p><i>route_match</i> specifies the route to be matched, using a series of O/R address attributes and values, separated by forward slash characters (/). Attributes are specified as <i>TAG=value</i> pairings, where TAG is one of the following O/R address attributes:</p> <ul style="list-style-type: none"> TAG — O/R Address Attribute OU1 — Organizational Unit Name 1 OU2 — Organizational Unit Name 2 OU3 — Organizational Unit Name 3 OU4 — Organizational Unit Name 4 O — Organization Name P — Private Domain Name A — Administrative Domain Name C — Country OU1-TX — Teletex Organizational Unit Name 1 OU2-TX — Teletex Organizational Unit Name 2 OU3-TX — Teletex Organizational Unit Name 3 OU4-TX — Teletex Organizational Unit Name 4 O-TX — Teletex Organization Name <p>The <i>value</i> specified is not case sensitive, and wildcard characters (*) can be used. If an attribute is not specified, it is treated as if it were fully wildcarded; that is, any value for that attribute is matched. No hierarchical rules are applied regarding which attributes can be specified and wildcarded.</p>
SR_SYNC_P2_WITH_P1=TRUE	<p>Sets the Service Router to modify the original value of the O/R address in the P2 distribution list as well as the P1.</p>
SR_USEX500_DIR= TRUE or <i>X.500_Directory_Name</i>	<p>Specifies that an X.500 directory is used by the Service Router to resolve a DDN.</p> <p>If set to TRUE, the first X.500 directory found is used.</p> <p>If the name of an X.500 directory is specified, this directory is used by the Service Router.</p>

Table 26: Service Router Options

Parameter	Description
OMLIMIT_MIN_WARN_INTERVAL= <i>time_period</i>	<p>NOTIFY messages for the OMLIMIT-EXCEEDED sanction are only sent if the NOTIFY message has not been sent within the time specified by this setting.</p> <p>The default value for the OMLIMIT_MIN_WARN_INTERVAL option is one day (1d).</p> <p>Examples:</p> <p>1h40m20s — 1 hour, 40 minutes, and 20 seconds</p> <p>2d40 — 2 days and 40 seconds</p> <p>6000 — 6000 seconds/100 minutes</p> <p>If the “omlimit -e u” sanction is enabled, the OMLIMIT_MIN_WARN_INTERVAL option also manages the interval during which omlimit-related messages are sent to a user.</p>

UAL Client Interface Options

The User Access Layer (UAL) is a proprietary Scalix protocol that enables communication between clients and the Scalix server. You can set these options in the general configuration file:

```
/var/opt/scalix/<nn>/s/sys/general.cfg
```

Table 27: UAL Client Interface Options

Parameter	Description
UAKD_CONNRATE_LIMIT= <i>number_of_connections_per_</i> <i>second</i>	<p>Specifies the maximum number of client connection processes that can be started per second.</p> <p>Specify a value here in order to limit the rate at which client connections are attempted. This can prevent delays caused by connection processes waiting for server resources.</p>
UAKD_LISTEN_Q_SIZE= <i>number_of_connections</i>	<p>Specifies the number of TCP/IP socket connections that can be queued to the UAL server <code>listen.daemon</code> process during busy periods. This reduces the possibility of “UAL unable to connect” errors.</p> <p>The <i>number_of_connections</i> can be between zero and the operating system limit. The default is 20 connections.</p>
UAKD_NICE_VALUE= <i>-20<=value<=20</i>	<p>Increases or reduces the priority of TCP/IP socket connections to the UAL server <code>listen.daemon</code> process, over other activities performed by the Scalix Server.</p> <p><i>value</i> is a number between -20 and 20, where negative values increase the priority of client login. The default is -10.</p>

Table 27: UAL Client Interface Options

Parameter	Description
<p>UAKD_SERVER_PUSH_NOTIFS=TRUE</p>	<p>Determines whether the server-push mechanism is enabled. The server-push mechanism allows certain clients to receive notifications automatically, without having to poll for them.</p> <p>The default is <code>TRUE</code>, meaning enabled for automatic notification.</p> <p>Set this option to <code>FALSE</code> to disable the server-push mechanism, forcing clients to poll for notifications. Setting this option to <code>FALSE</code> can result in increased performance, but do not set the option to <code>FALSE</code> if:</p> <ul style="list-style-type: none"> • There are a significant number of Microsoft Outlook clients in use. This will cause a large increase in network traffic. • Any IMAP clients are in use. IMAP clients cannot receive notifications if this option is <code>FALSE</code>.
<p>UAL_5_40_PERF_CHANGES=TRUE</p>	<p>Switches on or off the performance changes to the UAL client interface that were introduced in Scalix release 5.40. The default is <code>TRUE</code>. Set this option to <code>FALSE</code> if you suspect that one or more of the performance enhancements is causing problems.</p>
<p>UAL_ALLOW_DISABLED_CLIENTS=FALSE</p>	<p>If set to <code>TRUE</code>, clients specified in the <code>UAL_DISABLED_CLIENTS</code> option are permitted to log in to the server. Such logins are logged with a Warning level. This option can be used to find out which users are using a particular client so that they can be warned before the client is actually disabled.</p>
<p>UAL_FLDR_ACL_DEFAULT = <i>permissions</i></p>	<p>Specifies the permissions that are granted to the default user when a public folder is created. These permissions apply to each user unless the ACL has an entry that is more specific to that user.</p> <p>Set the value of <i>permissions</i> to a string of up to six characters, selected from the following:</p> <ul style="list-style-type: none"> o — Owner C — Contact c — Create r — Read f — Folder E — Edit all e — Edit own D — Delete all d — Delete own v — Visible
<p>UAL_DEAD_TIMEOUT=<i>number_of_minutes</i></p>	<p>Specifies the amount of time that Scalix waits for the next UAL command of any type (as opposed to <code>UAL_IDLE_TIMEOUT</code>, which is triggered by active commands only) from a UAL client before assuming a time-out. Once the time-out period has been reached, Scalix assumes the connection to the client has been lost and logs out the user of the UAL client.</p> <p>If a time-out period is not specified, Scalix assumes the connection to the UAL client is good regardless of how long it has been waiting for another command.</p> <p>For serial connections, <code>UAL_DEAD_TIMEOUT</code> is overridden by <code>UAL_SERIAL_DEAD_TIMEOUT</code>. For local UAL clients, <code>UAL_DEAD_TIMEOUT</code> is overridden by <code>UAL_LOCAL_DEAD_TIMEOUT</code>.</p>

Table 27: UAL Client Interface Options

Parameter	Description
<code>UAL_DEF_MIME_MN_OVERRIDE=route</code>	<p>By default, a message generated using the Microsoft Outlook client with the "Send in RTF" flag unchecked is routed according to the default MIME mailnode entry in the Routing Table. Set this option if you want to use a different route for such messages.</p> <p>The route you specify must ultimately point to a MIME gateway. Specify a route as an O/R address pattern, in the format specified for the <code>-m</code> option in the <code>omaddr</code> MAN page. For example, <code>UAL_DEF_MIME_MN_OVERRIDE="internet,ux"</code>. If you specify the address pattern in this route as a teletex value, you must specify an appropriate display character set in the <code>UAL_DEF_MIME_MN_OVERRIDE_CS</code> option.</p>
<code>UAL_DEF_MIME_MN_OVERRIDE_CS=character-set</code>	<p>This option specifies the display character set for the address pattern you specify in the <code>UAL_DEF_MIME_MN_OVERRIDE</code> option, if you entered it as a teletex value. The default character set is ISO8859_1. This option has no effect if the <code>UAL_DEF_MIME_MN_OVERRIDE</code> option is not set.</p>
<code>UAL_DEF_TNEF_MN_OVERRIDE=route</code>	<p>By default, a message generated using the Microsoft Outlook client with the "Send in RTF" flag checked is routed according to the default TNEF mailnode entry in the Routing Table. Set this option if you want to use a different route for such messages.</p> <p>The route you specify must ultimately point to a TNEF gateway. Specify a route as an O/R address pattern, in the format specified for the <code>-m</code> option in the <code>omaddr</code> MAN page. For example, <code>UAL_DEF_TNEF_MN_OVERRIDE="internet,ux"</code>. If you specify the address pattern in this route as a teletex value, you must specify an appropriate display character set in the <code>UAL_DEF_TNEF_MN_OVERRIDE_CS</code> option.</p>
<code>UAL_DEF_TNEF_MN_OVERRIDE_CS=character-set</code>	<p>This option specifies the display character set for the address pattern you specify in the <code>UAL_DEF_TNEF_MN_OVERRIDE</code> option, if you entered it as a teletex value. The default character set is ISO8859_1. This option has no effect if the <code>UAL_DEF_TNEF_MN_OVERRIDE</code> option is not set.</p>
<code>UAL_DIR_LIST_SORT_ORDER=list_of_internal_attributes</code>	<p>Specifies the order in which directory attributes are sorted. The order is specified as a list of internal attribute names with each attribute separated by a <code>/</code>. The internal attribute names, which are numbers for the core Scalix attributes, are listed using the command <code>omshowatt -u</code></p>
<code>UAL_DIR_LIST_SORT_PROG=absolute_program_name</code>	<p>Specifies the program that sorts lists of directory entries for UAL clients. The value <i>absolute_program_name</i> must specify the full path name of the sorting program together with any parameters that are necessary. The default Scalix sort program is <code>/bin/sort -f</code>. This is used if <code>UAL_DIR_LIST_SORT_PROG</code> is not set.</p>
<code>UAL_DIR_MOD_FULL_NAME=TRUE</code>	<p>Specifies that full name checking is always done on the <code>UAL_CHKLIST</code>, <code>UAL_CHKNAM</code>, <code>UAL_DELENT</code>, and <code>UAL_MODENT</code> commands.</p>

Table 27: UAL Client Interface Options

Parameter	Description
UAL_DISABLE_BB=FALSE	Disables or enables public folder access. If set to <code>TRUE</code> , when the user attempts to perform an action involving public folders the client displays an error message stating that the user has insufficient access capabilities to perform the action. The default is <code>FALSE</code> .
UAL_DISABLED_CLIENTS= <i>strings</i>	Specifies those UAL clients that are not allowed to log in to the server. <i>strings</i> is a list of space-separated, quoted strings (use single quotes only). Each string is a client identity string as passed in the <code>UAL_INIT</code> command. Strings can contain wildcards. Login attempts by identified clients are refused, and logged at the Error logging level. See also <code>UAL_ALLOW_DISABLED_CLIENTS</code> .
UAL_DISABLE_NESTED_BBS=TRUE	Stops the UAL client interface from creating new nested public folders under top-level public folders.
UAL_DISALLOW_AUTO_PASSWORD=TRUE	If set, a client cannot log in to Scalix if the client has explicitly indicated that its password was obtained from a configuration file rather than having been entered interactively by a user. See also <code>UAL_DISALLOW_NON_USER_PASSWORD</code> . The user-specific setting of this option overrides the system-wide setting.
UAL_DISALLOW_NON_USER_PASSWORD=TRUE	If set, a client cannot log in to Scalix if the client has not explicitly indicated that its password was obtained interactively from a user. See also <code>UAL_DISALLOW_AUTO_PASSWORD</code> . Note that this option only works with clients that supply the “password origination status”. If a client does not support this element, then it is unable to log in even when the password is actually entered interactively by the user. The user-specific setting of this option overrides the system-wide setting.
UAL_DL_SIZE_LIMIT= <i>no_of_kilobytes</i>	Sets the distribution list (DL) area size limit in kilobytes. A value of zero (0) means no size limit. Once you configure a limit, you must then configure the sanctions to be applied to those users who exceed it. If you do not configure sanctions, users can exceed their limits without effect.
UAL_DO_LONG_INET_CHECK=FALSE	Specifies whether the POP3 and IMAP4 servers perform full checking of Internet addresses. The default value is <code>FALSE</code> , and this causes the POP3 and IMAP4 servers to only look to see if a name has a DDA of type RFC-822 when checking if there is an Internet version of the name. This allows greater efficiency in cases where the names are either in a DDA or held in a directory, because a check to see if the name is routable to a UNIX queue is omitted. Set this option to <code>TRUE</code> to cause the full range of address conversions to be applied (according to the <code>unixmap.in</code> and <code>unixin.rules</code> steering files).

Table 27: UAL Client Interface Options

Parameter	Description
UAL_FC_SIZE_LIMIT= <i>no_of_kilobytes</i>	<p>Sets the filing cabinet (FC) size limit in kilobytes. A value of zero (0) means no size limit.</p> <p>Once you configure a limit, you must then configure the sanctions to be applied to those users who exceed it. If you do not configure sanctions, users can exceed their limits without effect.</p>
UAL_FORCE_IA_IN_ORN=FALSE	<p>Determines whether the UAL is forced to put the Internet address, as configured in the <code>SYSTEM</code> directory, of all distribution list names in the message, doing additional directory lookups if necessary.</p> <p>Assuming that the <code>SYSTEM</code> directory is populated with Internet addresses, when this option is set to <code>FALSE</code> (the default), the UAL inserts the Internet addresses of distribution list entries in the message, where it can do so without additional directory lookups. When a message reaches the Internet mail gateway, or is browsed by a POP3 or IMAP4 client, any ORNs without an Internet address are looked up in the directory to retrieve the Internet address. So the directory lookup overhead is at the Internet mail gateway, the POP3, or the IMAP4 interfaces.</p> <p>Set this option to <code>TRUE</code> to switch the overhead to the time when the message is sent.</p>
UAL_FORCE_TRACE_LEVEL= <i>trace_level</i>	<p>Sets the UAL trace level on a system-wide basis, overriding any trace value supplied by a client or set in the <code>user.cfg</code> file. The <i>trace_level</i> can be any valid trace level, including 0 (zero), which switches off tracing.</p>
UAL_GIVE_GROUP5_INET_NAME_ STRICT=FALSE	<p>Determines whether the UAL server gives a Group 5 Internet name in all cases. When set to <code>FALSE</code> (the default), the UAL server gives a Group 5 Internet name in all cases where the address contains a DDA of type RFC-822. This occurs even for those addresses that are tunnelled through Scalix, and causes replies to be incorrectly routed through the default Internet mail gateway.</p> <p>Set the option to <code>TRUE</code> to cause the UAL server to only give a Group 5 Internet name when the address in the DDA is routable to the local Internet mail gateway. There are two circumstances under which setting this option to <code>TRUE</code> has no effect:</p> <ul style="list-style-type: none"> • If Scalix users and PDLs have Internet addresses configured. • If Internet addresses of external users are put into the Group 5 Internet address at the incoming Internet mail gateway. You can prevent this by setting the option <code>INET_NO_IA_IN_ORN</code> to <code>TRUE</code>.
UAL_IDLE_SHUTDELAY= <i>number_of_minutes</i>	<p>Specifies the additional delay in shutting down a UAL client connection that has timed out.</p> <p><code>UAL_IDLE_SHUTDELAY</code> is used with <code>UAL_IDLE_TIMEOUT</code>.</p> <p>For serial connections, <code>UAL_IDLE_SHUTDELAY</code> is overridden by <code>UAL_SERIAL_IDLE_SHUTDELAY</code>.</p> <p>For local UAL clients, <code>UAL_IDLE_SHUTDELAY</code> is overridden by <code>UAL_LOCAL_IDLE_SHUTDELAY</code>.</p>

Table 27: UAL Client Interface Options

Parameter	Description
<p><code>UAL_IDLE_TIMEOUT=</code> <i>number_of_minutes</i></p>	<p>Specifies the amount of time that Scalix waits for the next active UAL command from a UAL client before assuming a time-out (<code>PREPARE MESSAGE</code>, <code>ATTACH ITEM</code> are examples of active UAL commands, and <code>NEW MESSAGES</code> and <code>LIST ACK</code> are examples of passive UAL commands). Once the time-out period has been reached, Scalix assumes the connection to the client has been lost and logs out the user of the UAL client. (The logout can be delayed using <code>UAL_IDLE_SHUTDELAY</code>.)</p> <p>If a time-out period is not specified, Scalix assumes the connection to the UAL client is good regardless of how long it has been waiting for another command. <code>UAL_IDLE_TIMEOUT</code> is used with <code>UAL_IDLE_SHUTDELAY</code>. For example:</p> <p>If <code>UAL_IDLE_TIMEOUT</code> is set to 30 minutes and <code>UAL_IDLE_SHUTDELAY</code> is not set, the client is disconnected from the server 30 minutes after the last active UAL command was issued.</p> <p>If <code>UAL_IDLE_TIMEOUT</code> is set to 30 minutes and <code>UAL_IDLE_SHUTDELAY</code> is set to 10 minutes, 30 minutes after the last active UAL command is issued, the client displays a dialog box asking if the user wants to retain the connection. This dialog box is displayed for up to the 10 minutes specified by <code>UAL_IDLE_SHUTDELAY</code>.</p> <p>If the user responds within this time with a Yes, that is considered an active UAL command, and the <code>TIMEOUT</code> countdown restarts from the beginning.</p> <p>If the user responds with a No, the connection is closed.</p> <p>If the user does not respond within the 10 minutes, the connection is closed.</p> <p>For serial connections, <code>UAL_IDLE_TIMEOUT</code> is overridden by <code>UAL_SERIAL_IDLE_TIMEOUT</code>.</p> <p>For local UAL clients, <code>UAL_IDLE_TIMEOUT</code> is overridden by <code>UAL_LOCAL_IDLE_TIMEOUT</code>.</p>
<p><code>UAL_INTRAY_SIZE_LIMIT=</code> <i>no_of_kilobytes</i></p>	<p>Sets the Inbox size limit in kilobytes. A value of zero (0) means no size limit. Once you configure a limit, you must then configure the sanctions to be applied to those users who exceed it. If you do not configure sanctions, users can exceed their limits without effect.</p> <p>Set Message Store size limits using the <code>omlimit</code> command.</p>
<p><code>UAL_ISO7_FROM_HOST=</code><i>language</i></p>	<p>This option is the same as <code>UAL_ISO7_HOST</code> except that the character set conversion only occurs when text is passed from Scalix to the client and not when it is passed back to the server.</p>
<p><code>UAL_ISO7_HOST=</code><i>language</i></p>	<p>This option allows clients to interoperate with a Scalix Message Store containing IA5 text that uses the ISO-7 extensions.</p> <p>If set, activates the option <code>UAL_ISO7_language</code> for any clients using <i>language</i>. IA5 text with the ISO-7 extensions are converted to the ISO8859/1 character set when downloaded to or displayed by a client and conversely, the ISO8859/1 characters are mapped back into IA5 with ISO-7 extensions when entering the Scalix system from a client.</p> <p>Only one instance of this option can be used and the <i>language</i> string must match a string in the <code>~/sys/LangMap</code> file.</p> <p>See also <code>UAL_ISO7_FROM_HOST</code>, <code>UAL_ISO7_TO_HOST</code>, and <code>SR_ISO7_HOST</code>.</p>

Table 27: UAL Client Interface Options

Parameter	Description
<p><code>UAL_ISO7_language=ISO7_characters</code></p>	<p>Specifies how text using the ISO-7 extensions is converted to the ISO8859/1 character set.</p> <p><i>ISO7_characters</i> is a list of ISO8859/1 characters to which the 12 special “ISO-7” characters are mapped. The IA5 characters used as special ISO-7 characters are:</p> <pre># \$ @ [\] ^ ' { } ~</pre> <p>The ISO8859/1 equivalents (<i>ISO7_characters</i>) must be specified in the same order. Ensure that the ISO8859/1 equivalents are entered into the file using the ISO8859/1 character set.</p> <p>The <i>language</i> must correspond to the language set in the <code>UAL_ISO7_HOST</code> option and the <code>UAL_ISO7_HOST</code> option must be present to activate this option.</p> <p>See also</p> <p><code>SR_ISO7_language</code></p> <p><code>UAL_ISO7_TO_HOST=language</code></p> <p>This option is the same as <code>UAL_ISO7_HOST</code> except that the character set conversion only occurs when text is passed from the client to Scalix and not when it is passed back to the client.</p>
<p><code>UAL_KILL_REMOTE_SIGNON_2=TRUE</code></p>	<p>Allows the Scalix server to kill a current user session in order to allow the user to log in again.</p> <p>If a user session is terminated abnormally (for example, a user restarts their computer), the session can continue to exist on the server. This can prevent the user from logging in again. Setting this option to <code>TRUE</code> allows the Scalix server to kill the user’s oldest session, allowing the user to log in.</p> <p>The Scalix server permits 17 concurrent logins. If this option is set to <code>TRUE</code>, and the user tries to connect for the eighteenth time, the Scalix server kills the user’s oldest session, and then allows them to log in again. If the option is set to <code>FALSE</code>, the Scalix server does not permit the user to log in.</p> <p>Note that some clients can set a lower limit for the number of concurrent logins.</p>
<p><code>UAL_LIST_CACHE_SIZE=number_of_message_parts</code></p>	<p>Specifies the number of message parts that can be held in memory by a UAL process. This entry reduces I/O by forcing Scalix to keep the message in memory instead of creating and then opening one file for each message part and the message header. The default is 4, which equates to a header record and three body parts.</p>
<p><code>UAL_LOCAL_DEAD_TIMEOUT=number_of_minutes</code></p>	<p>Specifies the amount of time that Scalix waits for the next UAL command of any type (as opposed to <code>UAL_LOCAL_IDLE_TIMEOUT</code>, which is triggered by active commands only) from a local UAL client before assuming a time-out.</p> <p>Once the time-out period has been reached, Scalix assumes the connection to the client has been lost and logs off the user of the UAL client.</p> <p>If a time-out period is not specified, Scalix assumes the connection to the local UAL client is good regardless of how long it has been waiting for another command.</p> <p><code>UAL_LOCAL_DEAD_TIMEOUT</code> overrides <code>UAL_DEAD_TIMEOUT</code>. To remove a time-out for local UAL clients that was set using <code>UAL_DEAD_TIMEOUT</code>, set <code>UAL_LOCAL_DEAD_TIMEOUT</code> to 0.</p>

Table 27: UAL Client Interface Options

Parameter	Description
UAL_LOCAL_IDLE_SHUTDELAY= <i>number_of_minutes</i>	Specifies the additional delay in shutting down a local UAL client connection that has timed out. Use with UAL_LOCAL_IDLE_TIMEOUT.
UAL_LOCAL_IDLE_TIMEOUT= <i>number_of_minutes</i>	Specifies the amount of time that Scalix waits for the next active UAL command from a local UAL client before assuming a time-out (PREPARE MESSAGE, ATTACH ITEM are examples of active UAL commands, and NEW MESSAGES and LIST ACL are examples of passive UAL commands). Once the time-out period has been reached, Scalix assumes the serial connection to the client has been lost and logs out the user of the UAL client. (The logout can be delayed using UAL_LOCAL_IDLE_SHUTDELAY.) If a time-out period is not specified, Scalix assumes the connection to the UAL client is good regardless of how long it has been waiting for another command. Used with UAL_LOCAL_IDLE_SHUTDELAY. Overrides UAL_IDLE_TIMEOUT. To remove a time-out for local UAL clients that was set using UAL_IDLE_TIMEOUT, set UAL_LOCAL_IDLE_TIMEOUT to 0.
UAL_LOCAL_IGNORE_PASSWORD= TRUE	Removes the password entry stage from the login process. The login succeeds only if the user has logged in using their Scalix mailbox Linux login, and if the user is using a local UAL client.
UAL_MAP_ALIAS_AT_MAIL=FALSE	By default, recipient O/R addresses entered as aliases in a distribution list are displayed as those aliases to the recipients. Set this option to TRUE to cause aliases to be rewritten as their real O/R addresses when the message is submitted to Scalix (unless both sender and recipient are using Microsoft Outlook). This enables the user to use and see alias names when preparing a message, but the recipients of the message only see the real names in the distribution list, not the alias names. If both sender and recipient are using Microsoft Outlook, then setting this option to TRUE has no effect, and the recipients continue to see the alias names in the distribution list.
MAX_SIGNON_PER_USER= <i>number</i>	Specifies the number of simultaneous logins that a user can have. The default is 17.
UAL_MOD_BB_ITEMS=TRUE	Determines whether items attached to public folders can be modified. Set this option to FALSE to prevent modification of the items. In this case, users can still add or delete top-level items to public folders, depending on the public folder's ACL. When set to TRUE (the default), master items can be modified, although slave items cannot. Public folders can be accessed only by Premium users.
UAL_MSTORE_SIZE_LIMIT= <i>no_of_kilobytes</i>	Sets the overall Message Store size limit in kilobytes. A value of zero (0) means no size limit. Once you configure a limit, you must then configure the sanctions to be applied to those users who exceed it. If you do not configure sanctions, users can exceed their limits without effect.
UAL_NAMED_PIPE_BLOCK_SIZE= <i>block_size</i>	Sets the physical block size for TCP/IP named pipes client connections. The default is 1380 bytes.

Table 27: UAL Client Interface Options

Parameter	Description
UAL_NMP_DELAY= <i>number_of_milliseconds</i>	Specifies the time delay before returning a reply to a command from a UAL client using a TCP/IP named pipes connection. By default, there is no time delay, but this can mean the receiving client system can miss the reply when it is sent. To overcome this problem set the delay to between 10 and 100 milliseconds.
UAL_NO_AUTOGEN_IA=FALSE	Determines, for certain UAL clients, whether automatic Internet address mapping is enabled. This option only affects those UAL clients that use the UAL_ENTADD command to add directory entries. Set this option to TRUE to override automatic Internet address mapping for these UAL clients. The default is FALSE. See the option INET_USE_AUTO_IAM.
UAL_NO_DESIGNATE_SIGNON=TRUE	Removes the designate login feature.
UAL_NO_IA_IN_ORN=FALSE	Determines whether the UAL puts the Internet addresses of the sender, recipients, or distribution list names into the message. When set to FALSE (the default), Internet addresses are inserted into the message if they can be determined without additional directory lookups.
UAL_NO_REPLY_BLOCKING=TRUE	If set, multiple UAL client interface replies are not blocked before being sent to a UAL remote client. This is used to overcome data communication problems that result from large blocks being sent from the server.
UAL_NO_WB_EMPTY=TRUE	Stops a user's Trash (waste basket, or WB) from being emptied when the user has finished using a UAL client and logs out. If this option is set, use the omtidy or omtidyallu command to ensure Trash continues to be emptied regularly.
UAL_OUTTRAY_SIZE_LIMIT= <i>no_of_kilobytes</i>	Sets the Outbox size limit in kilobytes. A value of zero (0) means no size limit. Once you configure a limit, you must then configure the sanctions to be applied to those users who exceed it. If you do not configure sanctions, users can exceed their limits without effect. Set Message Store size limits using the omlimit command.
UAL_PASSWORD_AGED= IGNORE, WARN, or ERROR	This option determines the effect of an expired password on a user logging in to Scalix through a client. The default value is ERROR. If the user's password has expired, an error is generated when the user attempts to log in and the login fails. The login can only succeed when a valid new password is supplied. If the value is set to WARN and the user's password has expired, the user can log in using the expired password but a warning message is placed in their Inbox stating that their password has expired and needs to be changed immediately. (This message appears in the Inbox for the first login of the day.) If the value is set to IGNORE, any user password expiration condition is ignored, and a Scalix user is allowed to log in even though their password has expired.
UAL_PEND_SIZE_LIMIT= <i>no_of_kilobytes</i>	Sets the pending tray size limit in kilobytes. A value of zero (0) means no size limit. Once you configure a limit, you must then configure the sanctions to be applied to those users who exceed it. If you do not configure sanctions, users can exceed their limits without effect. Set Message Store size limits using the omlimit command.

Table 27: UAL Client Interface Options

Parameter	Description
UAL_POP3_HOSTNAME= <i>hostname</i>	Set the POP3 server or the IMAP4 server host name so that addresses display as name@hostname. By default, the name of the Scalix host is used.
UAL_POP3_LANG= <i>language</i>	Specifies the Scalix language to use for error messages returned by the POP3 or IMAP4 client. The default is C.
UAL_POP3_TIMEOUT= <i>no_of_seconds</i>	Specifies the number of seconds of inactivity allowed before connection to the POP3 server times out. The default is 600 seconds.
UAL_POP3_TRACE=TRUE	If set, information from the <code>in.pop3d</code> process is traced and placed in the <code>~Scalix/tmp</code> folder. You can set this option to <code>DETAIL</code> to generate more detailed logging. Set the option to <code>FALSE</code> to prevent logging.
UAL_PRINT_SERVER_ONLY=TRUE	If set, all printing by UAL clients goes through the print server. See also <code>UAL_PRINT_SPECIFICATION</code> .
UAL_PRINT_SPECIFICATION= <i>print_command</i>	If set, <i>print_command</i> overrides any printer specification supplied by a UAL client. The <i>print_command</i> can either be a Linux printer command line or a print server printer specification.
UAL_PWD_WARNING_DAYS= <i>days</i>	Activates the mechanism to generate advisory messages to users whose mailbox passwords are due to expire within the period specified by <i>days</i> . The warning message appears as a new message in the user's Inbox for the first login of the day. Use this option if clients are being used that do not recognize the <i>password expired</i> login error. These clients cannot login successfully once the user's password has expired.
UAL_SCK_DELAY= <i>number_of_milliseconds</i>	Specifies the time delay before returning a reply to a command from a UAL client using a TCP/IP sockets connection. By default, there is no time delay, but this can mean the receiving client system can miss the reply when it is sent. To overcome this problem set the delay to between 10 and 100 milliseconds.
UAL_SEND_OBJECT_FILES=TRUE	Determines whether an object file (created with the UAL <code>addobj</code> call) is mailed with the message to which it is attached. When set to <code>TRUE</code> , the UAL submits both the message and any attached object files (assuming that the object files do not have the <code>UAL_ADDOBJ_NOT_MAIL</code> flag set).
UAL_SERIAL_DEAD_TIMEOUT= <i>number_of_minutes</i>	Specifies the amount of time that Scalix waits for the next UAL command of any type (as opposed to <code>UAL_SERIAL_IDLE_TIMEOUT</code> , which is triggered by active commands only) from a UAL client using a serial connection before assuming a time-out. Once the time-out period has been reached, Scalix assumes the connection to the client has been lost and logs out the user of the UAL client. If a time-out period is not specified, Scalix assumes the serial connection to the UAL client is good regardless of how long it has been waiting for another command. <code>UAL_SERIAL_DEAD_TIMEOUT</code> overrides <code>UAL_DEAD_TIMEOUT</code> . To remove a time-out for UAL clients that was set using <code>UAL_DEAD_TIMEOUT</code> , set <code>UAL_SERIAL_DEAD_TIMEOUT</code> to 0. This removes the time-out for all UAL clients using a serial connection.

Table 27: UAL Client Interface Options

Parameter	Description
<p>UAL_SERIAL_IDLE_SHUTDELAY= <i>number_of_minutes</i></p>	<p>Specifies the additional delay in shutting down a UAL client serial connection that has timed out. Used with UAL_SERIAL_IDLE_TIMEOUT.</p>
<p>UAL_SERIAL_IDLE_TIMEOUT= <i>number_of_minutes</i></p>	<p>Specifies the amount of time that Scalix waits for the next active UAL command from a UAL client using a serial connection before assuming a time-out (PRE-PARE MESSAGE and ATTACH ITEM are examples of active UAL commands, and NEW MESSAGES and LIST ACL are examples of passive UAL commands). Once the time-out period has been reached, Scalix assumes the serial connection to the client has been lost and logs out the user of the UAL client. (The logout can be delayed using UAL_SERIAL_IDLE_SHUTDELAY.) If a time-out period is not specified, Scalix assumes the connection to the UAL client is good regardless of how long it has been waiting for another command. Used with UAL_SERIAL_IDLE_SHUTDELAY. UAL_SERIAL_IDLE_TIMEOUT overrides UAL_IDLE_TIMEOUT. To remove a time-out for UAL clients that was set using UAL_IDLE_TIMEOUT, set UAL_SERIAL_IDLE_TIMEOUT to 0. This removes the time-out for all UAL clients using a serial connection.</p>
<p>UAL_SET_ROC_ON_ND= TRUE or FALSE</p>	<p>Overrides client setting of “Return of contents on non-delivery”. Set to TRUE to request a return of contents for all non-delivered messages. Set to FALSE to prevent return of contents for all non-delivered messages.</p>
<p>UAL_SHOW_8BIT_T61_AS_1167= TRUE</p>	<p>If set, teletex body parts (file code 1736) are presented to clients as normal 8-bit text (file code 1167). This enables existing Western European clients to work with no loss of features when handling teletex body parts that contain 8-bit character sets.</p>
<p>UAL_SIGNON_ALIAS=YES or ONLY</p>	<p>Specifies whether aliases are used for login. Any UAL_SIGNON_ALIAS entries in the <i>user.cfg</i> file take precedence over the UAL_SIGNON_ALIAS entry in the <i>general.cfg</i> file. (This enables you to set a default use of aliases in <i>general.cfg</i> and then set overrides for specific users in <i>user.cfg</i>.) The YES value means aliases can be used for login, and users can also continue to use their personal name if they want to. The ONLY value means only aliases can be used for login, and the personal name cannot be used any more. Used with UAL_SIGNON_ALIAS_CONFIG and UAL_USE_SIGNON_ALIAS.</p>
<p>UAL_SIGNON_ALIAS_CONFIG= SYS or USER</p>	<p>Allows users to log in using an alias. The SYS value means that everyone can log in using an alias. The USER value means that alias login entries in the <i>user.cfg</i> file are used when they exist and take precedence over any alias login entries in the <i>general.cfg</i> file. UAL_SIGNON_ALIAS_CONFIG is used with UAL_SIGNON_ALIAS and UAL_USE_SIGNON_ALIAS.</p>

Table 27: UAL Client Interface Options

Parameter	Description
UAL_SINGLE_TEMP_DIR= <i>temp-directory</i>	<p>Specifies the location of temporary user files.</p> <p>Normally (when this option is not set), the temporary user files are stored in the directory files for each user. Specify a value for this option to cause all user temporary files to be written to a single directory. This allows you to use a high-speed (and possibly low-recovery) file system (for example, a RAM disk) to store these temporary files.</p> <p>The directory you specify must have:</p> <ul style="list-style-type: none"> • Permissions of 771 • An owner of <code>scalix</code> • A group of <code>scalix</code> • A path length of 225 characters or less <p>For example, to create a folder called <code>usr_tmp</code>, enter the following commands:</p> <pre>mkdir \$(omrealpath '~usr_tmp') chown scalix:scalix \$(omrealpath '~usr_tmp') chmod 771 \$(omrealpath '~usr_tmp')</pre>
UAL_SIZE_ERR_TO_USER=TRUE	Specifies that a UAL error message is generated when a user tries to create an item in their filing cabinet or distribution list area once it has exceeded the limit set by <code>omlimit</code> .
UAL_SIZE_MSG_TO_ENU=TRUE	Specifies that a message is sent to the Error Notification user when a user's Inbox, pending tray, or Trash exceeds the set warning limit, boundary limit, or maximum limit. See <code>UAL_SIZE_WARNING_BOUNDS</code> and <code>UAL_SIZE_WARNING_LIMIT</code> .
UAL_SIZE_MSG_TO_USER=TRUE	Specifies that a message is sent to the user when their Inbox, pending tray, or Trash exceeds the set warning limit, boundary limit, or maximum limit. See <code>UAL_SIZE_WARNING_BOUNDS</code> and <code>UAL_SIZE_WARNING_LIMIT</code> .
UAL_SIZE_ON_RECEIPT=FALSE	Specifies whether a user whose message store components exceed their configured limits is prevented from receiving messages. If set to <code>FALSE</code> (the default), users are not prevented from receiving messages even if the size of their message store component is greater than its configured limit.
UAL_SIZE_ON_SEND=FALSE	Specifies whether a user whose message store components exceed their configured limits is prevented from sending messages. If set to <code>TRUE</code> , then message delivery rules can be implemented that limit a user's ability to send messages. These rules utilize the <code>OMLIMIT-EXCEEDED</code> message attribute filter. If set to <code>FALSE</code> (the default), then rules based on the <code>OMLIMIT-EXCEEDED</code> filter have no effect.
UAL_SIZE_WARNING_BOUNDS= <i>percent_increase</i>	<p>Specifies the boundary levels for warnings between the warning limit and the maximum limit. For example, if set to 5, warnings are sent when the size of an Inbox, pending tray, or Trash increases by 5 percent or more since the last warning.</p> <p>To enable warning messages to be sent, you must have set at least one of these options: <code>UAL_SIZE_MSG_TO_ENU</code> and <code>UAL_SIZE_MSG_TO_USER</code>.</p>

Table 27: UAL Client Interface Options

Parameter	Description
UAL_SIZE_WARNING_LIMIT= <i>percentage_of_max_limit</i>	Specifies the percentage of the maximum limit, set on the size of the Inbox, pending tray, or Trash, to be reached for a warning message to be generated. For example, if set to 80, warnings are sent when the Inbox, pending tray, or Trash reaches 80 percent of its maximum limit. To enable warning messages to be sent, you must have set at least one of these options: UAL_SIZE_MSG_TO_ENU and UAL_SIZE_MSG_TO_USER.
UAL_SOCKET_BLOCK_SIZE= <i>block_size</i>	Sets the physical block size for sockets client connections. The default is 1380 bytes.
UAL_TTX_NAME_FORMAT_LANG= <i>attribute order</i>	Specifies the order in which personal name attributes are displayed for clients using the UAL client interface display program (<code>item.browse</code>). The four personal name attributes are represented with the following letters: S — Surname F — Given name I — Initials G — Generation qualifier, such as Jr. Enter the letters in the order you want the attributes to be displayed. The <i>LANG</i> part of the option specifies the language the format is used for. For example, to display native Japanese names in their natural form, specify the option like this: UAL_TTX_NAME_FORMAT_NIPPON=SF
UAL_TTX_NAME_SHOW_ALL=TRUE	Sets the UAL client interface display program (<code>item.browse</code>) to display all teletex O/R address attributes regardless of whether the correct client character set is configured. By default, these address attributes are not displayed unless a suitable client character set is configured.
UAL_TTX_NAME_SUBST=TRUE	Substitutes the teletex O/R address attributes with the corresponding printable string attributes before displaying the message. This option is for clients using the UAL client interface display program (<code>item.browse</code>).
UAL_USE_SIGNON_ALIAS= FALSE or TRUE	Specifies whether an alias is used after login. If set to FALSE, the UAL client reverts to using the user's personal name for the remaining time the user is logged in (the alias or personal name is used on the "Creator" part of a message). If set to TRUE, the alias is used for the remaining time the user is logged in. UAL_USE_SIGNON_ALIAS is used with UAL_SIGNON_ALIAS and UAL_SIGNON_ALIAS_CONFIG.
UAL_WB_SIZE_LIMIT= <i>no_of_kilobytes</i>	Sets the Trash (waste basket, or WB) size limit in kilobytes. A value of zero (0) means no size limit. Once you configure a limit, you must then configure the sanctions to be applied to those users who exceed it. If you do not configure sanctions, users can exceed their limits without effect. Set Message Store size limits using the <code>omlimit</code> command.

Table 27: UAL Client Interface Options

Parameter	Description
OMLIMIT_MIN_WARN_INTERVAL= <i>time_period</i>	<p>If the “<code>omlimit -e u</code>” sanction is enabled, the <code>OMLIMIT_MIN_WARN_INTERVAL</code> option also manages the interval during which <code>omlimit</code>-related messages are sent to a user. The default value for the <code>OMLIMIT_MIN_WARN_INTERVAL</code> option is one day (1d).</p> <p>Examples: <code>1h40m20s</code> — 1 hour, 40 minutes, and 20 seconds <code>2d40</code> — 2 days and 40 seconds <code>6000</code> — 6000 seconds/100 minutes</p> <p>The <code>OMLIMIT_MIN_WARN_INTERVAL</code> option also manages the interval between <code>OMLIMIT-EXCEEDED</code> notifications when the service router processes message delivery rule sets.</p>

Virus Protection Options

You can set these options in the general configuration file:

```
/var/opt/scalix/<nn>/s/sys/general.cfg
```

Table 28: Virus Protection Options

Parameter	Description
SR_VS_DO_VIRUS_SCAN=FALSE	<p>In the absence of the <code>ALL-ROUTES.VIR</code> rule set file, this option determines whether virus scanning is active. When the <code>ALL-ROUTES.VIR</code> file exists, it determines the virus scanning/cleaning action to be taken.</p> <p>If set to <code>TRUE</code>, the Service Router checks all message attachments for viruses. When a virus is found, the message is not routed, and Scalix generates a non-delivery notification.</p> <p>If set to <code>FALSE</code>, virus checking is disabled.</p> <p>Note that the performance of your Scalix system can be degraded if you enable virus checking and a large number of viruses are detected, because each virus detected causes Scalix to generate a non-delivery report.</p>
SR_VS_IGNORE_ITEM_TYPES= <i>filetype-no</i>	<p>Specifies the file types to exclude from virus scanning.</p> <p>By default, when virus scanning is enabled, either by setting the <code>SR_VS_DO_VIRUS_SCAN</code> option to <code>TRUE</code> or by creating the <code>ALL-ROUTES.VIR</code> rule set file, all file types are scanned for viruses. Use this option to prevent certain file types from being scanned.</p> <p><i>filetype-no</i> is a colon-separated list of numerical file codes, as specified in <code>/var/opt/scalix/<nn>/s/nls/<language>/filetype</code></p> <p>For example, set <code>SR_VS_IGNORE_ITEM_TYPES</code> to <code>1167</code> to prevent text files from being scanned.</p>
SR_VS_TEST_SCAN_SL= <i>string</i>	<p>Specifies the location of the test virus shared library. If this file is in its default location, you set this option to <code>/opt/scalix/version/lib/libom_testvs.sl</code> if you want to test your virus scanning configuration.</p>

Table 28: Virus Protection Options

Parameter	Description
SR_VIRUS_SCAN_TYPE= <i>string</i>	<p>Specifies whether virus checking operates in test mode. Set this option to “Test Scan” to cause the Service Router to check messages and generate a non-delivery notification if the first five characters of any attachment are VIRUS.</p> <p>If you set this option to “Test Scan”, you must also set the SR_VS_TEST_SCAN_SL option to the location of the test virus shared library.</p> <p>If you set this option to “Generic”, then <code>/var/opt/scalix/<nn>/s/sys/omvscan.cfg</code> determines the virus scanning engine to use. Also, you must copy <code>omvscan.map</code> to the <code>~/rules/</code> folder to enable virus scanning.</p>

Export Process Options

You can set these options in the general configuration file:

`/var/opt/scalix/<nn>/s/sys/general.cfg`

Table 29: Export Process Options

Parameter	Description
XP_START_IMPORT_DELAY= <i>seconds</i>	<p>If set, specifies the number of seconds that the <code>xport.in</code> process waits when invoked by the Service Router in recovery mode before starting to process messages and put them on the Service Router queue. The delay is observed to a resolution of 5 seconds. A value of zero (0) causes <code>xport.in</code> to start processing the messages immediately. The default is 60 seconds.</p>

Miscellaneous Options

You can set these options in the general configuration file:

`/var/opt/scalix/<nn>/s/sys/general.cfg`

Table 30: Miscellaneous Options

Parameter	Description
AK_ACK_MSG_PRI=2	<p>Determines the priority to use for acknowledgments if <code>AK_ACK_SAME_PRI</code> is not set or the priority of the message being acknowledged is not known. Valid values are:</p> <ul style="list-style-type: none"> 0 — Normal 1 — Non-urgent 2 — Urgent (default)
AK_ACK_SAME_PRI=TRUE	<p>If set to <code>TRUE</code>, this option causes the priority of an acknowledgment to be the same as that of the message being acknowledged where that can be determined. Otherwise, the value of <code>AK_ACK_MSG_PRI</code> is used. The default is <code>FALSE</code>.</p>

Table 30: Miscellaneous Options

Parameter	Description
CT_OLD_PENDING_SIZE_MODE=FALSE	<p>Determines whether items in the Message Store that are pending deletion are included in the reported size of the Message Store.</p> <p>If set to <code>TRUE</code>, then items that are pending deletion are included in the reported size. The size is not reduced until the items are actually deleted.</p> <p>Leave this option set to <code>FALSE</code> (the default) if you want the reported size of the Message Store to be reduced as soon as items are marked for deletion.</p> <p>This is useful, for example, when users have limits configured on their Message Store sizes, as follows. If set to <code>FALSE</code>, users see an immediate effect on their reported Message Store sizes when they delete items. If set to <code>TRUE</code>, the Message Store size does not change until the user logs out of Scalix (for multiple logins, the last user must log out).</p> <p>If you change the value of this option, run the <code>omscan -A -S</code> command to regularize the reported Message Store sizes.</p>
CT_OLD_SIZE_METHOD=FALSE	<p>Specifies how the size of containers in the Message Store is updated.</p> <p>If set to <code>FALSE</code> (the default), container sizes are written to the Container Access Monitor, so that all processes have access to them. This ensures that all processes use the same reported container sizes, and is particularly useful when Message Store size limits are configured.</p> <p>If set to <code>TRUE</code>, container sizes are stored within an individual process before being written to disk.</p>
DIA_NO_T61_SUBJECT=FALSE	<p>Determines whether the <code>omcontain</code> command attempts to display T61 subjects.</p> <p>When set to <code>FALSE</code> (the default), <code>omcontain</code> does not display T61 subjects.</p>
IM_MAKE_MSG_ID_GLOBAL_UNIQUE=TRUE	<p>Specifies that Scalix message IDs are to use the long format. Set the value to <code>FALSE</code> if you want message IDs to use the short format. Note, however, that this can cause message IDs not to be globally unique.</p> <p>If you change the value of this option, restart Scalix for the change to take effect.</p>
SMTPD_PWD_TRANSITION=FALSE	<p>Determines whether the SMTP relay generates simple authentication and security layer (SASL) passwords and stores them in the user list, where SASL is an authentication method.</p> <p>Set this option to <code>TRUE</code> to cause the SMTP relay to generate alternative SASL passwords when a PLAIN password authentication succeeds. These SASL passwords are then stored in the user list.</p> <p>Reset this option to <code>FALSE</code> (the default) when the user list contains all the SASL passwords.</p>
USRL_AUTO_GEN_AUTHID=G_I_S	<p>Specifies the method used to generate the name part of the authentication ID. If you want to use the OMID method instead, enter <code>DEFAULT</code> for this value.</p>

Client-Specific Configuration Options

A subset of the options used in the `general.cfg` file can be specified for individual Scalix clients. The options for each client are held in a file with the name of the client host's fully qualified domain name (FQDN), in the following folder:

```
/var/opt/scalix/<nn>/sys/client.cfg
```

For example, for a client on the host `north.sales.alpha.com`, the client configuration options file is named `/var/opt/scalix/<nn>/sys/client.cfg/north.sales.alpha.com`

The `client.cfg` folder can need to be created. Make the owner the user `scalix` with permissions of `555` (`dr-xr-xr-x`). Have client files within this folder be owned by the user `scalix` with permissions of `444` (`-r--r--r--`).

The following client options are outlined in this section: recovery folder, IMAP, and Microsoft Outlook.

Note

Scalix Connect for Microsoft Outlook can be used only by Premium users.

Recovery Folder Options

The Scalix Recovered Items folder can be made visible when a user deletes messages and wants to retrieve them. You can configure the options in the following folder:

```
/var/opt/scalix/<nn>/sys/client.cfg
```

Table 31: Recovery Folder Options

Parameter	Description
RECOVERY_FOLDER_EXPIRY_TIME= <i><time_period></i>	Sets the amount of time that deleted items remain in the Scalix Recovered Items folder before being removed from the system. The default is seven days (7d) Examples: 4d12h — 4 days and 12 hours 240h — 240 hours Use a value of 0 to have no items saved to recovery folders. You can also set this value at the global level.

IMAP Configuration Options

You can configure the options in the following folder:

```
/var/opt/scalix/<nn>/sys/client.cfg
```

See the descriptions in the “System-Wide Configuration Options” section for the following options:

- IMAP_AUTOMATIC_MDN=FALSE
- IMAP_BB_FOLDER_PREFIX=#bb
- IMAP_BB_FOLDER_SEPARATOR=/
- IMAP_DELETE_SUBFOLDERS=FALSE
- IMAP_FOLDER_PREFIX=
(not defined in this document)
- IMAP_FOLDER_SEPARATOR=/
- IMAP_IDLE_TIMEOUT=30
- IMAP_LOGFILE=~/.tmp/imap.%h
- IMAP_LOGLEVEL=0
- IMAP_MDSENT_FLAG=*\$MdnSent*
- IMAP_MIN_SIZE_ESTIMATE=0
- IMAP_REMOTE_UAL_ENABLED=TRUE
- IMAP_SEARCH_TIMEOUT=0
- IMAP_UAL_TRACE_LEVEL=0
- IMAP_X_NETSCAPE_URL=
(not defined in this document)

The following table lists the IMAP4 options that you can specify for individual clients.

Table 32: IMAP4 Options

Parameter	Description
<p><code>IMAP_CAPABILITIES=<i>capabilities-list</i></code></p>	<p>Lists the capabilities that the IMAP server advertises to the client. Each item in the list is separated by a space. Note that capabilities you specify here are added to those specified on a system-wide and per-user basis.</p> <p>The default list of capabilities is "IMAP4 IMAP4rev1 IDLE NAMESPACE AUTH=LOGIN"</p> <p>The capabilities that can be included in the list are:</p> <p>IMAP4 Support for the basic protocol as defined in RFC 1730. Note that the IMAP4 commands defined in RFC 1730 but absent in RFC 2060 are still supported even if this capability is not advertised.</p> <p>IMAP4rev1 Support for the basic protocol as defined in RFC 2060. The IMAP server always advertises this capability.</p> <p>CHILDREN Support for a means of indicating whether or not folders have child folders. This is not a standard extension.</p> <p>IDLE Support for the <code>IDLE</code> extension as defined in RFC 2177. This extension can provide a significant performance benefit for clients that can use it.</p> <p>LITERAL+ Support for non-synchronizing literals as defined in RFC 2088. Use this capability with caution because it leaves the server open to denial-of-service attacks.</p> <p>NAMESPACE Support for the <code>NAMESPACE</code> command as defined in RFC 2342. This command is used by certain clients to discover the namespace prefix for public folders so that these can be seen by the client user.</p>
<p><code>IMAP_MAILSTORE_HOST=<i>hostname</i></code></p>	<p>Specifies the fully qualified domain name of the Scalix host to which the IMAP server connects. Use this option when the IMAP4 server does not reside on the same computer as the relevant Scalix Message Store.</p>

Microsoft Outlook Configuration Options

Mail API (MAPI) is a programming interface from Microsoft that enables a client application to send and receive mail to and from a Microsoft Exchange Server or a Microsoft Mail (MS Mail) messaging system. Microsoft Outlook uses MAPI. The `mapi.cfg` file sets parameters for all Scalix MAPI client users and provides a way to customize some Microsoft Outlook client functionality. This file is in the `/var/opt/scalix/<nn>/s/nls/C/` directory on the Scalix server if you are using auto-upgrades.

After a user logs in to Microsoft Outlook for the first time, the `mapi.cfg` file is automatically downloaded to the local system from the Scalix server. The local `mapi.cfg` file is downloaded to the `C:\Documents and Settings\user\Local Settings\Application Data\Scalix\Scalix\MAPI\Profiles\profile_name\Scalix` folder.

The following tables outline the configurable parameters of the `mapi.cfg` file. See also “Offline Folder Synchronization Options (Microsoft Outlook Clients)” on page 244.

Alert

If you modify any of these parameters then install (manually or automatically) an updated version of the MAPI service provider, the `mapi.cfg` file is replaced and the changes are lost.

[AutoUpgrade] Parameters

Use this section to set auto-upgrade options for Microsoft Outlook. Here is an example:

```
# MAPI Client configuration file
20
[AutoUpgrade]
HTTPSetupPath=http://address/directory/Setup.exe
HTTPUpdateInstallMgr=1
HTTPUpgradeExemptList=username1;username2
MinimumScalixVersion=x.xx.xx.xx
ForwardInstallLogsTo=administrator@yourcompany.com
ForwardInstallLogsFrom=IT Team
ForwardInstallLogsSubject=Automatic-Upgrade Status
UseLocalTimeVSGMT=1
UpgradeIntervalTimeCheck=8
```

Table 33: Automatic Upgrade Options for Microsoft Outlook

Parameter	Description
<i>n</i>	The version number of the <code>mapi.cfg</code> file that is used to determine whether auto-upgrades occur. This number is used to determine whether <code>mapi.cfg</code> is downloaded to update other administrative settings. If the version number of the <code>mapi.cfg</code> file on the user system is greater than the version number of the <code>mapi.cfg</code> file on the server, Scalix does not upgrade Scalix Connect on the user system with the latest version of the MAPI service provider and/or update the <code>mapi.cfg</code> file. The version is 20 in the example shown.
<i>HTTPSetupPath</i>	The path to the shared folder that contains the source Scalix Connect installation files. The <i>HTTPSetupPath</i> must be a valid <code>http://</code> address. The format is <code>http://address/directory/Setup.exe</code> For example <code>http://scalix.yourcompany.com/folder/Setup.exe</code>

Table 33: Automatic Upgrade Options for Microsoft Outlook

Parameter	Description
HTTPUpdateInstallMgr	<p>This value is set to 1. Do not modify this value.</p> <p>Set this parameter to 1 to install the SXInstallMgr.exe file on user systems. When set to 0, the <i>SXInstallMgr.exe</i> file is not installed on local systems.</p>
HTTPUpgradeExemptList	<p>Allows you to specify users that you do not want to upgrade to the latest version of Scalix Connect.</p> <p>Example: HTTPUpgradeExemptList=username1;username2</p> <p>The code checks for inclusion of the logged-in Windows users name in HTTPUpgradeExemptList, so it is a simple substring match and the choice of separator is irrelevant.</p> <p>Once auto-upgrade is set up, the first user who logs in to a computer, starts Microsoft Outlook with a Scalix profile, and whose name is NOT on the exception list, is prompted to upgrade the connector. If another user logs in to the same computer with another user account and the connector has been upgraded, the second user is not prompted because the upgrade is per-computer.</p>
MinimumScalixVersion	<p>The version number of the Scalix Connect dynamic link libraries. In other words, the version of the .dll file that is part of the Scalix Connect release to which you want to upgrade. The Scalix Release Notes contain the version number.</p>
ForwardInstallLogsTo	<p>The administrator mailbox to which auto-upgrade results are sent.</p> <p>Enter <code>off</code> to disable error logging.</p> <p>Logs list users who have (or, by absence, have not) upgraded their Windows computers to the latest version of Scalix Connect. They are saved to a temporary location and then automatically sent from the user system to the e-mail address specified in the mapi.cfg file.</p>
ForwardInstallLogsFrom	<p>The text that displays in the From field of the auto-install log message.</p>
ForwardInstallLogsSubject	<p>The Subject line of the e-mail that includes the auto-upgrade results.</p>
UseLocalTimeVSGMT	<p>Specify whether you want to use local time or Greenwich Mean Time (GMT) to auto-upgrade users. Enter 1 to use local time, or 0 to use GMT.</p>
UpgradeIntervalTimeCheck	<p>The (metric) time at which Scalix polls client systems to verify whether they are using the latest version of Scalix Connect. For example, enter 8 to poll for auto-upgrade status information at 8 am, or enter 22 to poll for information at 10 pm. Entering a value of 24 or greater causes Scalix to poll for auto-upgrade information in intervals (by seconds). For example, if you want to poll client systems every hour, enter 3600.</p>

[Startup] Parameters

Use this section to set startup options for Microsoft Outlook.

Table 34: Startup Parameters for Microsoft Outlook

Parameter	Description
AddressBookDownloadReminderInterval	This option displays the number of days since you last downloaded a copy of the Address Book from the Scalix server. Scalix Connect also reads the value of <code>PreviousABDownloadDate</code> in the registry key of <code>HKEY_LOCAL_MACHINE\SOFTWARE\SCALIX\MAPI</code> . Scalix Connect calculates the difference between the two dates. If the difference is greater than the value displayed in the <code>AddressBookDownloadReminderInterval</code> option, Scalix Connect displays a reminder to users to download a copy of the Address Book from the Scalix server. To remind users to download Address Books monthly, set the value in the <code>AddressBookDownloadReminderInterval</code> option to 30.
AlwaysShowLogon	The <code>AlwaysShowLogon=1</code> option specifies that the user is always prompted for a password at startup. If you enabled password storing at login, you are not prompted for a password.

[Addressing] Parameters

Addressing parameters affect the interpretation of Scalix addresses on messages.

Table 35: Addressing Parameters for Microsoft Outlook

Parameter	Description
InternetToOM	On an incoming message, Scalix Connect converts a Scalix address that includes a domain defined attribute (DDA) type of RFC-822 to an address type of SMTP. Scalix Connect then uses the DDA for the revised address. For example, Scalix Connect replaces the Scalix address of a message such as <code>chris/linux/dd.RFC-822=cwolfe@pwd.scalix.com</code> with an SMTP address such as <code>cwolfe@pwd.scalix.com</code> . You can override this behavior and keep the address as a Scalix type by including the setting <code>InternetToOM=1</code> in this section.
HPMEXTToSMTP	You can extend the conversion of Scalix addresses to SMTP addresses that include a DDA type of the form <code>HPMEXTn</code> by including the setting <code>HPMEXTToSMTP=1</code> in this section. The <code>InternetToOM=1</code> option takes precedence over the <code>HPMEXTToSMTP=1</code> option.

[Display] Parameters

The options in the [Display] section specify the following:

- The maximum number of items within a container
- Which attributes are displayed
- The maximum line length in plain text messages
- How Internet addresses are formatted

Settings in the [Display] section affect the presentation of Scalix addresses, for example, the displayed part of an address but not the underlying message address or type.

Table 36: Display Parameters for Microsoft Outlook

Parameter	Description
MaxContainerSize	<p>The maximum number of messages that are listed on opening a folder can be configured using this setting. This setting can take an integer value between 20 and 32767. The default value is 32767. If the configured limit is exceeded, then a warning message is displayed.</p> <p>Archiving (or auto-archiving) a folder that contains more than <code>MaxContainerSize</code> items causes the container-limit warning message to be displayed. Scalix Connect archives those items within the limit of 32767.</p>
ShowMailnodes	<p>Either the mailnode attributes or custom attributes can be displayed, but not both. You can set only one of the following options for attribute display. The format of each option is described in the following sections.</p> <p>The <code>ShowMailnodes=1</code> option specifies that the mailnode attributes are displayed in message headers along with the name (<code>Personal Name/OU1, OU2</code>). This is useful when selecting similar entries from the directory. Without this setting you must scroll across the window to see the mailnode. The setting also applies to the display of addresses when either composing or reading a message.</p> <p>A way to resolve an unresolved address is to right-click the address. This displays possible alternatives, which include the mailnode.</p>
ShowCustomAttributes	<p>The <code>ShowCustomAttributes=1</code> option specifies that custom attributes, other than the mailnode details (<code>Personal Name/OU1, OU2</code>), are displayed in message headers.</p> <p>If you set this option, you must also set the <code>UserDefinedAttributes</code> option to specify the attributes to be displayed.</p>

Table 36: Display Parameters for Microsoft Outlook

Parameter	Description
UserDefinedAttributes	<p><code>UserDefinedAttributes=%(attr_tag) [% (attr_tag)]</code> where <code>attr_tag</code> is the internal attribute tag for a Scalix directory attribute type defined in the <code>/var/opt/scalix/<nn>/sys/dir.attrs</code> file. This tag can be either a pre-defined Scalix system attribute type (a numerical value) or a custom attribute type you have defined.</p> <p>Use the <code>omshowatt -u</code> command on the Scalix server to list the internal attribute tags.</p> <p>For example, specifying the line <code>UserDefinedAttributes=%(1)%(8)%(9)</code> displays the Surname, Organization, and Country Code as the internal attribute tags for these Scalix attributes. The types are 1, 8, and 9, respectively, in the <code>dir.attrs</code> file. If you have defined a custom attribute type of <code>JobTitle</code> in the <code>dir.attrs</code> file, specifying the line <code>UserDefinedAttributes=%(1)%(JobTitle)</code> displays the Surname and Job Title.</p> <p>See the guidelines section that follows for more information about <code>UserDefinedAttributes</code>.</p>
LineLength	<p>The maximum length of a line in a plain text message can be specified. The format of the option is as follows: <code>LineLength=n</code></p> <p>It specifies the maximum number of characters in each line of a plain text message, where <code>n</code> can be a value up to 80.</p> <p>For example, <code>LineLength=60</code> ensures that the message text has no more than 60 characters per line. If the <code>LineLength=n</code> entry is missing or invalid then lines default to a maximum of 72 characters.</p> <p>To disable wrapping, add the entry <code>LineLength=0</code></p>
TabStops	<p>The <code>TabStops=n</code> specifies the number of spaces for tab stops used by plain text messages, where <code>n</code> must not exceed the <code>LineLength</code> value or 20, whichever is smaller. The default for <code>n</code> is 4 if the <code>TabStops</code> setting is missing.</p>
ShowCompleteInternetAddress	<p>The <code>ShowCompleteInternetAddress=1</code> option specifies that the entire Internet address is displayed. It causes a Scalix address that contains a DDA type of RFC-822 to be displayed as an Internet address.</p> <p>For example, the address of an incoming message such as <code>chris/linux/dd.RFC-822=cwolfe@pwd.scalix.com</code> displays as <code>chris</code> (by default), but if you set the value <code>ShowCompleteInternetAddress=1</code>, Scalix Connect displays the address as <code>cwolfe@pwd.scalix.com</code></p> <p><code>ShowCompleteInternetAddress=1</code> takes precedence over <code>ShowMailnodes=1</code>.</p> <p>The behavior of <code>ShowCompleteInternetAddress</code> is also affected by settings in the [Addressing] section. A setting of <code>InternetToOM=1</code> prevents interpretation of the RFC-822 DDA as an Internet address and causes <code>ShowCompleteInternetAddress</code> to be ignored. <code>HPMEXTTosSMTP=1</code> extends the behavior of <code>ShowCompleteInternetAddress</code> to <code>HPMEXT</code> DDAs.</p>

Guidelines for UserDefinedAttributes

For the UserDefinedAttributes option to be applied correctly, note the following guidelines.

The [Display] section must also include the following setting:

```
ShowCustomAttributes=1
```

The [Display] section must not include the setting `ShowMailnodes=1` because this setting takes precedence over UserDefinedAttributes and results in an address of the following form:

```
Eric Smith / ou1, ou2
```

The UserDefinedAttributes setting can include up to ten entries, including a maximum of six custom attributes.

Any attribute specified in UserDefinedAttributes must also appear in the properties option of the Address Book. If the attribute is not one of the standard X.400 addressing fields or teletext equivalents (Scalix internal format Group 1 and 3), as displayed in the Name/Address Fields and the DDA pages, then you must add it to the custom attribute page through the mapi.cfg [Name Attributes] section.

In other words, any tags in UserDefinedAttributes outside the value ranges 1-23 and 51-68 must also appear in the [Name Attributes] section. For example:

```
[Name Attributes]
Heading=Custom
1=Phone:, 116
2=My Own Data:, myown
[Display]
ShowMailnodes=0
ShowCustomAttributes=1
UserDefinedAttributes=%(2)%(1)%(116)%(myown)
```

[Directories] Parameters

The option in the [Directories] section enables additional directories from the server to be included. The server default directory is always opened by the MAPI Address Book provider.

Table 37: Directories Parameters for Microsoft Outlook

Parameter	Description
<i>n=directory name</i>	<p>Specifies an additional directory, where:</p> <ul style="list-style-type: none"> <i>n</i> is a consecutive sequence number (1 to 20). <i>directory name</i> is the name of the additional directory to be included. Directory names are case-sensitive. <p>For example, to include directories for your Sales and Overseas departments, specify the following lines:</p> <pre>[Directories] 1=SALES 2=OVERSEAS</pre> <p>Make sure these entries are case-sensitive, for example if you have the directory MYOWNNONE Shared LOCAL DB config update read modifyself (as shown by om.listdirs), the entry in this section must be:</p> <pre>1=MYOWNNONE</pre> <p>You also need to add these directories to the Client Directory Access (CDA) server (omaddcda) and then run omexeccda.</p> <p>Add the <code>-d <directoryname></code> option to enable type-down searching on this directory.</p>

[Name Attributes] Parameters

The option in the [Name Attributes] section enables additional attributes from the Scalix directory to be included as a name/address properties page and as the search page of the MAPI client.

Table 38: Name Attributes Parameters for Microsoft Outlook

Parameter	Description
<i>heading=text</i> <i>n=label,tag</i>	<p>This specifies the additional attributes for the Properties and Search pages, where:</p> <ul style="list-style-type: none"> <i>text</i> is the text used as the page tab heading. You can specify up to 16 characters. <i>n</i> is the sequence number for the custom attribute. You can specify up to six attributes (1 to 6). <i>label</i> is the text for the label displayed for the attribute on the page. You can specify up to 24 characters. <i>tag</i> is the numeric value of the internal attribute tag for the corresponding Scalix directory attribute. To see the list of available tags, use the <code>omshowatt -u</code> command. <p>For example, to include three additional custom attributes, specify the following lines:</p> <pre>[Name Attributes] heading = Custom 1=Job Title:, 111 2=Department:, 115 3=Phone:, 116</pre>

[PAW] Parameters

The Personal Assistant Wizard (PAW) appears as a menu option under **Tools > Personal Administration Wizard**. The [PAW] section in mapi.cfg has the following options.

Table 39: PAW Parameters for Microsoft Outlook

Parameter	Description
URL	The URL pointing to the Web server for the user, for example: URL=http://zaphod.pwd.scalix.com This option is required for the PAW to be available to the user.
AutoLogon	The automatic login option that uses 1 or 0 as a value. 1 bypasses the Web-based login page and logs in automatically to the PAW home page. 0 does not bypass the Web-based login page and you must enter your user name and password. This option is not required. PAW is still available to a user if this option is not set.
Profile	The profile option determines the language for the PAW application at start-up. For example: Prof=PAW-ENGLISH This option is not required. PAW is still available to a user if this option is not set.

Before Scalix Connect includes PAW as a menu option (**Tools > Personal Administration Wizard**), Scalix Connect checks the following requirements:

- A valid Scalix server profile
- A valid mapi.cfg file with the [PAW] section included in the configuration file
- If the [PAW] section exists within the mapi.cfg file, Scalix Connect checks that the URL is defined for the PAW server

The PAW option in the Microsoft Outlook Tools menu is unavailable if any of these requirements are missing or invalid.

User-Specific Configuration Options

A subset of the options used in the `general.cfg` file can be specified for individual users. The options for each user are held in files with the name of that user's Scalix ID number in the following folder:

```
/var/opt/scalix/<nn>/s/sys/user.cfg
```

For example, if the Scalix user `Chris Wolf/ny,hq,mis` has a Scalix ID of 103, then options specific to him are in the file `~/sys/user.cfg/103`

To get the user's ID number

1 Use the `omshowu` command with the `-G` option. For example:

```
omshowu -n "Jane Smith" -G
```

2 In the information returned, look for the **Internal user Id**, for example 103.

The `user.cfg` folder can need to be created. It must be owned by the user Scalix with permissions of 555 (`dr-xr-xr-x`). User files within this folder must be owned by the user Scalix with permissions of 444 (`-r--r--r--`).

See the descriptions in the “System-Wide Configuration Options” section for the following options:

- `IMAP_AUTOMATIC_MDN=FALSE`
- `IMAP_BB_FOLDER_PREFIX=#bb`
- `IMAP_BB_FOLDER_SEPARATOR=/`
- `IMAP_DELETE_SUBFOLDERS=FALSE`
- `IMAP_FOLDER_PREFIX=`
(not defined in this document)
- `IMAP_FOLDER_SEPARATOR=/`
- `IMAP_IDLE_TIMEOUT=30`
- `IMAP_LOGLEVEL=0`
- `IMAP_MDNSENT_FLAG=$MdnSent`
- `IMAP_MIN_SIZE_ESTIMATE=0`
- `IMAP_SEARCH_TIMEOUT=0`
- `IMAP_X_NETSCAPE_URL=`
(not defined in this document)

IMAP Client User-Specific Options

Configure the options in the following folder:

`/var/opt/scalix/<nn>/s/sys/user.cfg`

Table 40: IMAP Client User-Specific Options

Parameter	Description
<p><code>IMAP_CAPABILITIES=<i>capabilities-list</i></code></p>	<p>Lists the capabilities that the IMAP server advertises to the client. Each item in the list is separated by a space. Note that capabilities you specify here are added to those specified on a system-wide and client-wide basis.</p> <p>The default list of capabilities is "IMAP4 IMAP4rev1 IDLE NAMESPACE AUTH=LOGIN"</p> <p>The capabilities that can be included in the list are:</p> <p>IMAP4 Support for the basic protocol as defined in RFC 1730. Note that the IMAP4 commands defined in RFC 1730 but absent in RFC 2060 are still supported even if this capability is not advertised.</p> <p>IMAP4rev1 Support for the basic protocol as defined in RFC 2060. The IMAP server always advertises this capability.</p> <p>CHILDREN Support for a means of indicating whether or not folders have child folders. This is not a standard extension.</p> <p>IDLE Support for the <code>IDLE</code> extension as defined in RFC 2177. This extension can provide a significant performance benefit for clients that can use it.</p> <p>LITERAL+ Support for non-synchronizing literals as defined in RFC 2088. Use this capability with caution because it leaves the server open to denial-of-service attacks.</p> <p>NAMESPACE Support for the <code>NAMESPACE</code> command as defined in RFC 2342. This command is used by certain clients to discover the namespace prefix for public folders so that these can be seen by the client user.</p>

Table 40: IMAP Client User-Specific Options

Parameter	Description
IMAP_LOGFILE=~/.tmp/imap.%h	<p>Specifies the name of the file to which IMAP events are logged, provided that logging is turned on using the <code>IMAP_LOGLEVEL</code> option.</p> <p>When the file you specify already exists, new events are appended to it. Note that at certain log levels log files can contain sensitive information, such as passwords.</p> <p>You can use the following tokens in the log file name:</p> <ul style="list-style-type: none"> <code>%p</code> — Expands to the PID of the IMAP server process. One log file is created for each IMAP server process. <code>%h</code> — Expands to the name of the client host. One log file is created for each client host that connects to the IMAP server. <code>%u</code> — Expands to the Scalix UID. One log file is created for each Scalix user that connects to the IMAP server. <p>If logging has been enabled in the system-wide or client-specific configuration file, this option has no effect.</p>

UAL Client Interface User-Specific Options

The User Access Layer (UAL) is a proprietary Scalix protocol that enables communication between clients and the Scalix server. Configure the options in the following folder:

```
/var/opt/scalix/<nn>/s/sys/user.cfg
```

Table 41: UAL Client Interface User-Specific Options

Parameter	Description
UAL_DEAD_TIMEOUT= <i>number_of_minutes</i>	<p>Specifies the amount of time that Scalix waits for the next UAL command of any type (as opposed to <code>UAL_IDLE_TIMEOUT</code>, which is triggered by active commands only) from a UAL client before assuming a time-out. Once the time-out period has been reached, Scalix assumes the connection to the client has been lost and logs out the user of the UAL client.</p> <p>If a time-out period is not specified, Scalix assumes the connection to the UAL client is good regardless of how long it has been waiting for another command.</p> <p>For serial connections, <code>UAL_DEAD_TIMEOUT</code> is overridden by <code>UAL_SERIAL_DEAD_TIMEOUT</code>.</p> <p>For local UAL clients, <code>UAL_DEAD_TIMEOUT</code> is overridden by <code>UAL_LOCAL_DEAD_TIMEOUT</code>.</p>
UAL_DIR_LIST_SORT_ORDER= <i>list_of_internal_attributes</i>	<p>Specifies the order in which directory attributes are sorted. The order is specified as a list of internal attribute names with each attribute separated by a <code>/</code>. The internal attribute names, which are numbers for the core Scalix attributes, are listed using the command <code>omshowatt -u</code></p>
UAL_DIR_MOD_FULL_NAME=TRUE	<p>Specifies that full name checking is always done on the <code>UAL_CHKLIST</code>, <code>UAL_CHKNAM</code>, <code>UAL_DELENT</code>, and <code>UAL_MODENT</code> commands.</p>
UAL_DISALLOW_AUTO_PASSWORD= TRUE	<p>If set, a client cannot log in to Scalix if the client has explicitly indicated that its password was obtained from a configuration file rather than having been entered interactively by a user. See also <code>UAL_DISALLOW_NON_USER_PASSWORD</code>.</p> <p>The user-specific setting of this option overrides the system-wide setting.</p>

Table 41: UAL Client Interface User-Specific Options

Parameter	Description
UAL_DISALLOW_NON_USER_PASSWORD=TRUE	<p>If set, a client cannot log in to Scalix if the client has not explicitly indicated that its password was obtained interactively from a user. See also UAL_DISALLOW_AUTO_PASSWORD.</p> <p>Note that this option only works with clients that supply the “password origination status”. If a client does not support this element, then it is not able to log in even if the password is actually entered interactively by the user.</p> <p>The user-specific setting of this option overrides the system-wide setting.</p>
UAL_DL_SIZE_LIMIT= <i>no_of_kilobytes</i>	<p>Sets the distribution list (DL) area size limit in kilobytes. A value of zero (0) means no size limit.</p> <p>Once you configure a limit, you must then configure the sanctions to be applied to those users who exceed it. If you do not configure sanctions, users can exceed their limits without effect.</p>
UAL_FC_SIZE_LIMIT= <i>no_of_kilobytes</i>	<p>Sets the filing cabinet (FC) size limit in kilobytes. A value of zero (0) means no size limit.</p> <p>Once you configure a limit, you must then configure the sanctions to be applied to those users who exceed it. If you do not configure sanctions, users can exceed their limits without effect.</p>
UAL_IDLE_SHUTDELAY= <i>number_of_minutes</i>	<p>Specifies the additional delay in shutting down a UAL client connection that has timed out.</p> <p>Used with UAL_IDLE_TIMEOUT.</p> <p>For serial connections, UAL_IDLE_SHUTDELAY is overridden by UAL_SERIAL_IDLE_SHUTDELAY.</p> <p>For local UAL clients, UAL_IDLE_SHUTDELAY is overridden by UAL_LOCAL_IDLE_SHUTDELAY.</p>

Table 41: UAL Client Interface User-Specific Options

Parameter	Description
<p><code>UAL_IDLE_TIMEOUT=</code> <i>number_of_minutes</i></p>	<p>Specifies the amount of time that Scalix waits for the next active UAL command from a UAL client before assuming a time-out (<code>PREPARE MESSAGE</code>, <code>ATTACH ITEM</code> are examples of active UAL commands, and <code>NEW MESSAGES</code> and <code>LIST ACK</code> are examples of passive UAL commands). Once the time-out period has been reached, Scalix assumes the connection to the client has been lost and logs out the user of the UAL client. (The logout can be delayed using <code>UAL_IDLE_SHUTDELAY</code>.)</p> <p>If a time-out period is not specified, Scalix assumes the connection to the UAL client is good regardless of how long it has been waiting for another command. <code>UAL_IDLE_TIMEOUT</code> is used with <code>UAL_IDLE_SHUTDELAY</code>. For example:</p> <p>If <code>UAL_IDLE_TIMEOUT</code> is set to 30 minutes and <code>UAL_IDLE_SHUTDELAY</code> is not set, the client is disconnected from the server 30 minutes after the last active UAL command is issued.</p> <p>If <code>UAL_IDLE_TIMEOUT</code> is set to 30 minutes and <code>UAL_IDLE_SHUTDELAY</code> is set to 10 minutes, 30 minutes after the last active UAL command is issued, the client displays a dialog box asking if the user wants to retain the connection. This dialog box is displayed for up to the 10 minutes specified by <code>UAL_IDLE_SHUTDELAY</code>.</p> <p>If the user responds with a Yes, that is considered an active UAL command, and the <code>TIMEOUT</code> countdown restarts from the beginning.</p> <p>If the user responds with a No, the connection is closed.</p> <p>If the user does not respond within the 10 minutes, the connection is closed.</p> <p>For serial connections, <code>UAL_IDLE_TIMEOUT</code> is overridden by <code>UAL_SERIAL_IDLE_TIMEOUT</code>.</p> <p>For local UAL clients, <code>UAL_IDLE_TIMEOUT</code> is overridden by <code>UAL_LOCAL_IDLE_TIMEOUT</code>.</p>
<p><code>UAL_INTRAY_SIZE_LIMIT=</code> <i>no_of_kilobytes</i></p>	<p>Sets the Inbox size limit in kilobytes. A value of zero (0) means no size limit. Once you configure an Inbox limit, you must then configure the sanctions to be applied to those users who exceed it. If you do not configure sanctions, users can exceed their limits without effect.</p> <p>Set Message Store size limits using the <code>omlimit</code> command.</p>
<p><code>UAL_ISO7_FROM_HOST=</code><i>language</i></p>	<p>This option is the same as <code>UAL_ISO7_HOST</code> except that the character set conversion only occurs when text is passed from Scalix to the client and not when it is passed back to the server.</p>
<p><code>UAL_ISO7_HOST=</code><i>language</i></p>	<p>This option allows clients to interoperate with a Scalix Message Store containing IA5 text that uses the ISO-7 extensions.</p> <p>If set, activates the option <code>UAL_ISO7_language</code> for a client using <i>language</i>. IA5 text with the ISO-7 extensions are converted to the ISO8859/1 character set when downloaded to or displayed by the client and conversely, the ISO8859/1 characters are mapped back into IA5 with ISO-7 extensions when entering the Scalix system from the client.</p> <p>Only one instance of this option can be used and the language string must match a string in the <code>/var/opt/scalix/<nn>/s/sys/LangMap</code> file.</p> <p>See also <code>UAL_ISO7_FROM_HOST</code>, <code>UAL_ISO7_TO_HOST</code>, and <code>SR_ISO7_HOST</code>.</p>

Table 41: UAL Client Interface User-Specific Options

Parameter	Description
UAL_ISO7_TO_HOST= <i>language</i>	This option is the same as UAL_ISO7_HOST except that the character set conversion only occurs when text is passed from the client to Scalix and not when it is passed back to the client.
UAL_LOCAL_DEAD_TIMEOUT= <i>number_of_minutes</i>	Specifies the amount of time that Scalix waits for the next UAL command of any type (as opposed to UAL_LOCAL_IDLE_TIMEOUT, which is triggered by active commands only) from a local UAL client before assuming a time-out. Once the time-out period has been reached, Scalix assumes the connection to the client has been lost and logs out the user of the UAL client. If a time-out period is not specified, Scalix assumes the connection to the local UAL client is good regardless of how long it has been waiting for another command. UAL_LOCAL_DEAD_TIMEOUT overrides UAL_DEAD_TIMEOUT. To remove a time-out for local UAL clients that was set using UAL_DEAD_TIMEOUT, set UAL_LOCAL_DEAD_TIMEOUT to 0.
UAL_LOCAL_IDLE_SHUTDELAY= <i>number_of_minutes</i>	Specifies the additional delay in shutting down a local UAL client connection that has timed out. Used with UAL_LOCAL_IDLE_TIMEOUT.
UAL_LOCAL_IDLE_TIMEOUT= <i>number_of_minutes</i>	Specifies the amount of time that Scalix waits for the next active UAL command from a local UAL client before assuming a time-out (PREPARE MESSAGE, ATTACH ITEM are examples of active UAL commands, and NEW MESSAGES and LIST ACL are examples of passive UAL commands). Once the time-out period has been reached, Scalix assumes the serial connection to the client has been lost and logs out the user of the UAL client. (The logout can be delayed using UAL_LOCAL_IDLE_SHUTDELAY.) If a time-out period is not specified, Scalix assumes the connection to the UAL client is good regardless of how long it has been waiting for another command. Used with UAL_LOCAL_IDLE_SHUTDELAY. UAL_LOCAL_IDLE_TIMEOUT overrides UAL_IDLE_TIMEOUT. To remove a time-out for local UAL clients that was set using UAL_IDLE_TIMEOUT, set UAL_LOCAL_IDLE_TIMEOUT to 0.
UAL_LOCAL_IGNORE_PASSWORD= TRUE or FALSE	Specifies whether a password check is made during login. Set the option to TRUE to remove the password entry stage from the login process. Set the option to FALSE to add the step back into the login process if it has been removed by setting UAL_LOCAL_IGNORE_PASSWORD in the general.cfg file. The login succeeds when the user has logged in using their Scalix mailbox Linux login and using a local UAL client.
UAL_MSTORE_SIZE_LIMIT= <i>no_of_kilobytes</i>	Sets the overall Message Store size limit in kilobytes. A value of zero (0) means no size limit. Once you configure a limit, you must then configure the sanctions to be applied to those users who exceed it. If you do not configure sanctions, users can exceed their limits without effect.
UAL_NMP_DELAY= <i>number_of_milliseconds</i>	Specifies the time delay before returning a reply to a command from a UAL client using a TCP/IP named pipes connection. By default, there is no time delay, but this can mean the receiving client system can “miss” the reply when it is sent. To overcome this problem, set the delay to between 10 and 100 milliseconds.

Table 41: UAL Client Interface User-Specific Options

Parameter	Description
UAL_NO_DESIGNATE_SIGNON=TRUE or FALSE	Specifies whether the designate login feature is used. Set the value to <code>TRUE</code> to remove the designate login feature. Set the value to <code>FALSE</code> to add the designate login feature if it has been removed by setting <code>UAL_NO_DESIGNATE_SIGNON</code> in the <code>general.cfg</code> file.
UAL_NO_WB_EMPTY=TRUE	Stops a user's Trash (or waste basket, WB) from being emptied when the user has finished using a UAL client and logs out. If this option is set, use the <code>omtidyu</code> or <code>omtidyallu</code> command to ensure the Trash continues to be emptied regularly.
UAL_PASSWORD_AGED=IGNORE, WARN, or ERROR	This option determines the effect of an expired password on a user logging in to Scalix through a client. The default value is <code>ERROR</code> . If the user's password has expired, an error is generated when the user attempts to log in and the login fails. The login can only succeed when a valid new password is supplied. If set to <code>WARN</code> and the user's password has expired, the user can log in using the expired password but a warning message is placed in their Inbox stating that their password has expired and is to be changed immediately. (This message appears in the Inbox for the first login of the day.) If set to <code>IGNORE</code> any user password expiry condition is ignored, and a Scalix user is allowed to log in even when their password has expired.
UAL_PEND_SIZE_LIMIT= <i>no_of_kilobytes</i>	Sets the pending tray size limit in kilobytes. A value of zero (0) means no size limit. Once you configure a limit, you must then configure the sanctions to be applied to those users who exceed it. If you do not configure sanctions, users can exceed their limits without effect. Set Message Store size limits using the <code>omlimit</code> command.
UAL_PWD_WARNING_DAYS= <i>days</i>	Activates the mechanism to generate advisory messages to users whose mailbox passwords are due to expire within the period specified by days. The warning message appears as a new message in the user's Inbox for the first login of the day. Use this option if clients are being used that do not recognize the password expired login error. These clients cannot log in successfully once the user's password has expired.
UAL_SCK_DELAY= <i>number_of_milliseconds</i>	Specifies the time delay before returning a reply to a command from a UAL client using a TCP/IP sockets connection. By default, there is no time delay, but this can mean the receiving client system can "miss" the reply when it is sent. To overcome this problem, set the delay to between 10 and 100 milliseconds.

Table 41: UAL Client Interface User-Specific Options

Parameter	Description
UAL_SERIAL_DEAD_TIMEOUT= <i>number_of_minutes</i>	<p>Specifies the amount of time that Scalix waits for the next UAL command of any type (as opposed to UAL_SERIAL_IDLE_TIMEOUT, which is triggered by active commands only) from a UAL client using a serial connection before assuming a time-out. Once the time-out period has been reached, Scalix assumes the connection to the client has been lost and logs out the user of the UAL client.</p> <p>If a time-out period is not specified, Scalix assumes the serial connection to the UAL client is good regardless of how long it has been waiting for another command.</p> <p>UAL_SERIAL_DEAD_TIMEOUT overrides UAL_DEAD_TIMEOUT. To remove a time-out for UAL clients that was set using UAL_DEAD_TIMEOUT, set UAL_SERIAL_DEAD_TIMEOUT to 0. This removes the time-out for all UAL clients using a serial connection.</p>
UAL_SERIAL_IDLE_SHUTDELAY= <i>number_of_minutes</i>	<p>Specifies the additional delay in shutting down a UAL client serial connection that has timed out.</p> <p>Used with UAL_SERIAL_IDLE_TIMEOUT.</p>
UAL_SERIAL_IDLE_TIMEOUT= <i>number_of_minutes</i>	<p>Specifies the amount of time that Scalix waits for the next active UAL command from a UAL client using a serial connection before assuming a time-out (PREPARE MESSAGE, ATTACH ITEM are examples of active UAL commands, and NEW MESSAGES and LIST ACL are examples of passive UAL commands). Once the time-out period has been reached, Scalix assumes the serial connection to the client has been lost and logs out the user of the UAL client. (The logout can be delayed using UAL_SERIAL_IDLE_SHUTDELAY.)</p> <p>If a time-out period is not specified, Scalix assumes the connection to the UAL client is good regardless of how long it has been waiting for another command.</p> <p>UAL_SERIAL_IDLE_TIMEOUT is used with UAL_SERIAL_IDLE_SHUTDELAY.</p> <p>UAL_SERIAL_IDLE_TIMEOUT overrides UAL_IDLE_TIMEOUT. To remove a time-out for UAL clients that was set using UAL_IDLE_TIMEOUT, set UAL_SERIAL_IDLE_TIMEOUT to 0. This removes the time-out for all UAL clients using a serial connection.</p>
UAL_SIGNON_ALIAS=YES, ONLY, or NONE	<p>Specifies whether aliases are used for login. Any UAL_SIGNON_ALIAS entries in the <i>user.cfg</i> file take precedence over the UAL_SIGNON_ALIAS entry in the <i>general.cfg</i> file. This enables you to set a default use of aliases in <i>general.cfg</i> and then set overrides for specific users in <i>user.cfg</i>.</p> <p>The YES option means aliases can be used for login and users can also continue to use their personal name if they want to.</p> <p>The ONLY option means aliases can be used to login, but not the personal name.</p> <p>The NONE option means aliases are not used.</p> <p>UAL_SIGNON_ALIAS is used with UAL_SIGNON_ALIAS_CONFIG and UAL_USE_SIGNON_ALIAS.</p>
UAL_SIZE_ON_RECEIPT=FALSE	<p>Specifies whether a user whose Message Store components exceed their configured limits is prevented from receiving messages.</p> <p>If set to FALSE (the default), users are not prevented from receiving messages even if the size of their Message Store component is greater than its configured limit.</p>

Table 41: UAL Client Interface User-Specific Options

Parameter	Description
<p>UAL_SIZE_ON_SEND=FALSE</p>	<p>Specifies whether a user whose message store components exceed their configured limits is prevented from sending messages.</p> <p>If set to <code>TRUE</code>, then message delivery rules can be implemented that limit a user's ability to send messages. These rules utilize the <code>OMLIMIT-EXCEEDED</code> message attribute filter.</p> <p>If set to <code>FALSE</code> (the default), then rules based on the <code>OMLIMIT-EXCEEDED</code> filter have no effect.</p>
<p>UAL_TRACE_FILE=<i>file_specification</i></p>	<p>The name stub of the file to which UAL trace information is logged (UAL logging must be enabled). <code>%p</code> in the <i>file_specification</i> is replaced with the PID of the UAL process, <code>%s</code> by the notification session-ID, and <code>%u</code> by the Scalix UID. A leading <code>~</code> represents the Scalix home directory. Note that the existing log file is overwritten. Without a leading <code>~</code> or <code>/</code> character, the file(s) are created in the <code>~scalix/tmp</code> folder.</p> <p>UAL trace output is enabled by using the <code>UAL_TRACE_LEVEL</code> option. The default value is <code>OM%u</code>.</p> <p>The substitutions in the log file name allow log files to be created on a per-ual-process, per-notif-session, or per-user basis. This allows MAPI and Scalix Web Access sessions that use concurrent UAL sessions to be traced without any loss of data. UAL client session must be restarted to enable the changes to this option.</p> <p>Example: <code>UAL_TRACE_FILE=ual.%u.%p</code> creates log files in the <code>~scalix/tmp</code> folder with a stub of <code>ual.user_id.pid</code>, for example: <code>ual.102.1773U.log</code> <code>ual.102.1773U.f0001</code></p> <p>Example: <code>UAL_TRACE_FILE=/tmp/ual-logs/%u.%p</code> creates log files in the <code>/tmp/ual-logs</code> folder with a stub of <code>user_id.pid</code>, for example: <code>/tmp/ual-logs/102.1773U.log</code> <code>/tmp/ual-logs/102.1773U.f0001</code> In this example, the <code>/tmp/ual-logs</code> folder must be created before any trace files can be written. See <code>UAL_TRACE_LEVEL</code> for more information.</p>

Table 41: UAL Client Interface User-Specific Options

Parameter	Description
UAL_TRACE_LEVEL= <i>trace_level</i>	<p>Activates UAL client interface tracing. The trace files are placed in the <code>~/tmp</code> folder. If this folder cannot be found, they are placed in the <code>/tmp</code> directory. File names begin with “OMuser-no”, where user-no is the Scalix user number, and end according to the trace level set.</p> <p>If you require several kinds of trace information, add the numbers for the levels you require and set the entry to the total.</p> <ul style="list-style-type: none"> 0 — No tracing (default) 1 — Raw (unformatted) command/reply tracing (file name: nameN.trc) 2 — Command statistics 4 — Message Store file name mapping. No trace file. The subject of an item listed or displayed in the client is replaced by its corresponding Message Store file name. 8 — Full tracing of command/reply and file transfer data. This can be used to rerun a session (file name: nameU.log and nameU.fnnnn). 16 — Raw (unformatted) command/reply tracing and file transfer data (file name: nameN.trc) <p>Also use this entry to set Event Log logging on the server for the client. Set the entry to the required Event Log logging level multiplied by 100.</p>
UAL_LINUX_PASSWORD=TRUE or FALSE	<p>Specifies whether the user uses their Linux password instead of their Scalix password when logging in. TRUE sets Scalix to use the Linux password, and FALSE (the default) sets Scalix to use the Scalix password.</p>
UAL_USE_SIGNON_ALIAS=FALSE or TRUE	<p>Specifies whether the alias is used after login.</p> <p>If set to FALSE, the UAL client reverts to using the user’s personal name for the remaining time the user is logged in (the alias or personal name is used on the “Creator” part of a message).</p> <p>If set to TRUE, the alias is used for the remaining time the user is logged in.</p> <p>UAL_USE_SIGNON_ALIAS is used with UAL_SIGNON_ALIAS and UAL_SIGNON_ALIAS_CONFIG.</p>
UAL_WB_SIZE_LIMIT= <i>no_of_kilobytes</i>	<p>Sets the Trash size limit in kilobytes. A value of zero (0) means no size limit. Once you configure a limit, you must then configure the sanctions to be applied to those users who exceed it. If you do not configure sanctions, users can exceed their limits without effect.</p> <p>Set Message Store size limits using the <code>omlimit</code> command.</p>

Offline Folder Synchronization Options (Microsoft Outlook Clients)

Table 42: Offline Folder Synchronization Options

Parameter	Description
OFS_ENABLED=FALSE	<p>Specifies whether folder synchronization is enabled on the Scalix server. The default is FALSE.</p> <p>If set to TRUE in the <i>general.cfg</i> file, it can be overridden on a per-user basis by setting it to FALSE in the relevant user-specific configuration files.</p>
OFS_LOG_SIZE_LIMIT= <i>kilobytes</i>	<p>Specifies, in kilobytes, the maximum size of the folder synchronization change log. Set a value between 20 and 10000 KB. The default is 100 KB.</p> <p>When the size of a change log exceeds this value, the older entries can be deleted when the change log file is compacted.</p> <p>Use this option to prevent change logs from growing too large when logging is activated but synchronization is not taking place for any reason. Take care when you set this value, because removal of any valid entries causes the entire folder to be resynchronized.</p> <p>A value you set in the <i>general.cfg</i> file can be overridden on a per-user basis by setting a lower value for this option in the relevant user-specific configuration file.</p>
OFS_LOG_AGE_LIMIT= <i>days</i>	<p>Specifies, in days, the maximum age of entries in the folder synchronization change log. Set a value between 1 and 18000 days. The default is 90 days.</p> <p>When the age of a change log entry exceeds this value, it can be deleted when the change log file is compacted.</p> <p>Use this option to prevent change logs from growing too large when logging is activated but synchronization is not taking place for any reason. Take care when you set this value, because removal of any valid entries causes the entire folder to be resynchronized.</p> <p>A value you set in the <i>general.cfg</i> file can be overridden on a per-user basis by setting a lower value for this option in the relevant user-specific configuration file.</p>

Language-Specific Configuration Options

You can add files that specify defaults to use for various languages, for example the character sets to use.

The files are located in the following folder:

```
/var/opt/scalix/<nn>/s/sys/lang.cfg
```

By default, three files are provided: Korean, Japanese, and Chinese. Use one of these files as an example. The Korean file is shown here:

```
#  
# Korean settings for POP3 and IMAP4.  
#  
BRW_MIME_SUBJECT_CHARSET=KSC5601  
BRW_MIME_OMIT_DEF_CTENC_HDR=T  
BRW_MIME_SUBJECT_ENCODING=B  
BRW_MIME_SUBJ_BENC_NONASCII=T  
BRW_MIME_SUBJECT_FOLDING=T  
BRW_MIME_TEXTFILE_ENCODING=N
```

The BRW_ options are outlined in Table 13, “Internet Mail Gateway Options,” on page 183.

Command Line Reference

This chapter summarizes the following collections of Scalix commands:

- “Access Control List Commands” on page 248
- “Audit Log Commands” on page 249
- “Client Directory Access (CDA) Commands” on page 249
- “Configuration and Installation Commands” on page 250
- “Directory Commands” on page 250
- “Directory Relay Server Commands” on page 251
- “Directory Synchronization Commands” on page 251
- “Error Manager Commands” on page 251
- “Event Log Commands” on page 252
- “Internet Address Commands” on page 252
- “Internet Mail Gateway Commands” on page 253
- “LDAP Commands” on page 253
- “Mailbox Access Commands” on page 254
- “Mailnode Commands” on page 254
- “Message Store Commands” on page 255
- “Miscellaneous Commands” on page 256
- “Public Distribution List (Group) Commands” on page 256
- “Public Folder Commands” on page 257
- “Routing Table Commands” on page 257
- “Service, Queue, and Daemon Commands” on page 258
- “System Configuration and Maintenance Commands” on page 259
- “User Account Commands” on page 259

Introduction

After you log in to your Scalix server, you can enter Scalix commands in a Linux terminal window, using the Scalix command line interface (CLI). Scalix commands have a prefix of “om” followed by extensions that define the action and the object. For example, the command to add a user is `omaddu` followed by extensions.

Because interpretations of command characters vary by shell program, you can be required to use escape sequences for some command elements. For example, if you enter parentheses while using the `omsearch` command, some shell programs can require that the

parentheses be escaped with backslashes (\) before the shell program can interpret the command correctly.

Note

Some Scalix commands can be used only by a Scalix Administrator with system administration privileges, for example the root user.

The following table lists the location of additional information (manual, or MAN, pages) about command formats and matching rules not covered in this chapter. An example of use is to enter

```
man omaddress
```

in a terminal window to view information about the omaddress command.

Table 1: Commands Explained in MAN Pages

Command	Description
omaddress	Enter O/R address, mailnodes, and pattern matching rules.
omattribs	Attribute input and output formats.
omdiratt	Formatting of attribute definition files.

The rest of this chapter catalogs Scalix commands. For more information about syntax and extensions, see the MAN page for each command.

Access Control List Commands

Access Control Lists (ACLs) control user access to Scalix resources, such as public folders, directories, scripts, and services.

Table 2: ACL Commands

Command	Description
omaddacl	Add an Access Control List.
omaddacln	Add capabilities for users to an Access Control List.
omchkacln	Check capabilities of a user in an Access Control List.
omdelacl	Delete an Access Control List.
omdelacln	Delete capabilities for users from an Access Control List.
ommodacln	Modify capabilities for users in an Access Control List.
omshowacl	Show the contents of an Access Control List.

Audit Log Commands

Audit log levels have commands. An audit log records user activity, for example, and can identify usage patterns. There are also event logs, outlined later.

Table 3: Audit Log Commands

Command	Description
omconfaud	Configure audit logging levels.
omshowaud	Show audit logging levels for the following services: Service Router Local Delivery Internet Mail Gateway Local Client Interface Remote Client Interface Administration Request Server Directory Synchronization Bulletin Board Server (public folders) Background Search Service POP3 Interface Omscan Server Archiver

Client Directory Access (CDA) Commands

The Client Directory Access server builds access tables for Scalix directories to provide sorted lists of directory entries.

Table 4: Client Directory Access Commands

Command	Description
omaddcda	Add a directory to the Client Directory Access server configuration.
omdelcda	Delete a directory from the Client Directory Access server configuration.
omexeccda	Force the Client Directory Access server to process a directory immediately.
ommodcda	Modify the Client Directory Access server configuration for a directory.
omshowcda	Show the Client Directory Access server configuration for a directory.

Configuration and Installation Commands

Some commands relate directly to the Scalix installation.

Table 5: Configuration and Installation Commands

Command	Description
omcptree	Copy or refresh a directory hierarchy.
omdelom	Delete a Scalix instance.
ommakeom	Make a Scalix instance.
ompatchom	Update a Scalix instance.
omredirtcp	Redirect socket connections to the correct Scalix system in a multisystem environment.

Directory Commands

Scalix directories include SYSTEM, USERLIST, and FREEBUSY.

Table 6: Directory Commands

Command	Description
omadent	Add one or more entries to a directory.
omdelent	Delete one or more entries from a directory.
omdiropt	Optimize a directory.
omdoptall	Optimize all directories.
omfmtent	Format directory and address attributes.
omlistdirs	List directories, such as SYSTEM and FREEBUSY. The USERLIST directory is hidden.
ommoddir	Modify a directory.
ommodent	Modify a directory entry.
omremdir	Delete a directory.
omsearch	Search a directory.
omshowatt	Show a list of available attribute types in the SYSTEM directory.

Directory Relay Server Commands

This applies to mailnodes.

Table 7: Directory Relay Server Commands

Command	Description
omresetmn	Reset a mailnode mapping file.
omaddmnp	Add entry to a mailnode mapping file.
ommodmnp	Modify entry in a mailnode mapping file.
omdelmnp	Delete entry in a mailnode mapping file.
omshowmnp	List entries in a mailnode mapping file.

Directory Synchronization Commands

Support for multiple Scalix servers and directory synchronization is available only in Scalix Enterprise Edition.

Table 8: Directory Synchronization Commands

Command	Description
omaddds	Add a directory synchronization agreement.
omdelds	Delete a directory synchronization agreement.
omlistds	List directory synchronization agreements.
ommodds	Modify a directory synchronization agreement.
omresyncds	Resynchronize a directory.
omshowds	Show details of a directory synchronization agreement.

Error Manager Commands

You can name a user to manage errors generated. The default error manager is sxadmin.

Table 9: Error Manager Commands

Command	Description
omconfenu	Configure (designate) a user to be an error manager.
omshowenu	Show the address of the error manager. The default is sxadmin.

Event Log Commands

See also the audit log section earlier.

Table 10: Event Log Commands

Command	Description
omconflvl	Configure event log logging levels.
omshowlog	Show the event log.
omshowlvl	Show event log logging levels for the following services: Service Router Local Delivery Internet Mail Gateway Local Client Interface Remote Client Interface Administration Request Server Directory Synchronization Bulletin Board Server (public folders) Background Search Service POP3 Interface Omscan Server Archiver

Internet Address Commands

This includes mailnodes too.

Table 11: Internet Address Commands

Command	Description
omaddiam	Add an entry to the Internet address mapping file.
omdeliam	Delete an entry from the Internet address mapping file.
omgeniamods	Generate a script to modify Internet addresses.
ommodiam	Modify a mapping between O/R address and Internet address.
ompreviewia	Preview the automatically generated Internet address.
omshowiam	List mappings between O/R addresses and Internet addresses.

Internet Mail Gateway Commands

A gateway passes messages from the Scalix network to different mail environments. They convert outgoing messages from a Scalix format to one that an external service can send and later convert the addresses into a format that the target environment can handle.

Table 12: Internet Mail Gateway Commands

Command	Description
omconfux	Configure the Internet mail gateway.
omshowux	Show the configuration of the Internet mail gateway, meaning the MIME and TNEF information.

LDAP Commands

The table lists commands for the Lightweight Directory Access Protocol (LDAP).

Table 13: LDAP Commands

Command	Description
omldapadd	Add one or more entries to an LDAP directory.
omldapdelete	Delete one or more entries from an LDAP directory.
omldapmodify	Modify an LDAP directory entry.
omldapmoddn	Modify the Distinguished Name (DN) of an LDAP entry.
omldapsearch	Search an LDAP directory.

Mailbox Access Commands

You can log in to a Scalix server, list mail, and read it, for example. Log in as follows:

```
omlogon -h scalix1 -u "Jane Rogers"
```

where scalix1 is the name of the Scalix server and Jane Rogers is the user account. Then list mail with

```
omlist
```

then view the second message listed with

```
omread 2
```

Table 14: Mailbox Access Commands

Command	Description
omdelete	Delete a message.
omlist	List messages.
omlogoff	Terminate an omlogon connection to Scalix.
omlogon	Obtain a connection to Scalix; log in.
omnew	List newly arrived messages.
omread	Read a message.
omsend	Send a message.

Mailnode Commands

You can manage mailnodes, for example list them and add them.

Table 15: Mailnode Commands

Command	Description
omaddmn	Add a mailnode.
omdelmn	Delete one or more mailnodes.
ommodmn	Modify a mailnode.
omshowmn	List local mailnodes.

Message Store Commands

The Message Store is the mail database.

Table 16: Message Store Commands

Command	Description
omcontain	Manipulate containers in the Message Store.
omcpinu	Copy a user's Message Store data from a file.
omcpoutu	Copy a user's Message Store data to a file.
omdosur	Create a data file for restoring a single user.
omdref	Convert a Scalix DirectRef into a readable description of the item represented, including Message Store item hierarchy.
omdumpis	Write Item Structure database to standard output.
omgetsur	Get files from an archive.
omlimit	Set Message Store size limits globally or for a user.
omnewis	Create an empty database.
omprepsur	List files required for single user restore.
omscan	Scan, report, and repair Scalix data inconsistencies.
omshowis	Display the date omupdtis was last run.
omsuspend	Halt all client activity temporarily.
omtidyallu	Delete items from the Message Store.
omtidyu	Delete items from the Message Store for an individual and search nested folders for an item to delete.
omupdtis	Read Item Structure log entries and update the database.
tfbrowse	Convert between Scalix transaction file format and textual format.

Miscellaneous Commands

Table 17: Miscellaneous Commands

Command	Description
ombconv	Convert a numeric value into a variety of numeric bases.
ombprint	Print messages in batch mode.
omenquire	Enquire about Scalix system status and report the results.
omsolve	Display solutions to an error message.

Public Distribution List (Group) Commands

When you create a group, you create a public distribution list (PDL), or mailing list, because all mail addressed to the group goes to all members of the group.

The pdl commands listed here let you add and modify public distributions lists, but not designate members.

The aci commands listed here give users control of the public distributions lists. For example, with the omaddaci command, you specify users who can modify a public distribution list.

Table 18: PDL Commands

Command	Description
omaddpdl	Add a public distribution list.
omaddpdln	Add an entry to a public distribution list.
omdelpdl	Delete one or more public distribution lists.
omdelpdln	Delete one or more entries from a public distribution list.
ommodpdl	Modify a public distribution list.
ommodpdln	Modify public distribution list entries.
omshowpdl	List public distribution lists. Example: omshowpdl -l all to display all groups. Example: omshowpdl -l "sales" to display all user accounts in a group called sales.
omshowpdln	List entries in a public distribution list.
omaddaci	Add an Access Control Item member.
omchkaci	Check Access Control Item capabilities for a user.
omdelaci	Delete an Access Control Item member.
ommodaci	Modify an Access Control Item member.
omshowaci	Show the contents of Access Control Item.

Public Folder Commands

Public folders can be accessed by Premium users.

Table 19: Public Folder Commands

Command	Description
omaddbb	Add a top-level public folder. Example: omaddbb -s "Public 2" to add a public folder called Public 2 The public folder has no owner when you add it using the command line.
omdelbb	Delete a top-level public folder. Example: omdelbb -m "Public 2" to delete a public folder called Public 2.
omlistbbs	List top-level public folders.
ommaintbb	Maintain top-level public folders by deleting items, for example when they are a number of days old (-e option). Example: ommaintbb -a -e 30 to delete items added more than 30 days ago from all public folders.
ommodbb	Modify a top-level public folder, such as its name or expiry date.
omshowbb	Show details of a top-level public folder, such as owner, expiry date, and size. Example: omshowbb -m "Public 1" to show information about a public folder called Public 1.
omaddbbsa	Add a public folder synchronization agreement.
omdelbbsa	Delete a public folder synchronization agreement.
omlistbbsa	List public folder synchronization agreements.
ommodbbsa	Modify a public folder synchronization agreement.

Routing Table Commands

You can set message delivery rules for any given route so that special routing instructions are handled at the server level. For example, you can use router rules to reject mail from certain senders before it reaches users.

Table 20: Routing Table Commands

Command	Description
omaddrtr	Add a route.
omdelrt	Delete a route.
ommodrt	Modify a route.
omshowrt	List routes and show how an address is routed.

Service, Queue, and Daemon Commands

You can use commands to stop and start Scalix and its services. The services are:

Notification Server	Local Client Interface
Database Monitor	Remote Client Interface
LDAP Daemon	Test Server
Directory Relay Server	Request Server
IMAP Server Daemon	Print Server
SMTP Relay	Directory Synchronization
Mime Browser Controller	Bulletin Board Server
Event Server	Background Search Service
Service Router	Dump Server
Local Delivery	CDA Server
Internet Mail Gateway	POP3 interface
Sendmail Interface	Archiver
	Omscan Server

For example, to stop the Notification Server, enter

```
omoff "Notification Server"
```

The daemons are as follows and can be listed with the omstat command:

Service Router	Print Server
Local Delivery	Bulletin Board Server
Internet Mail Gateway	Background Search Service
Local Client Delivery	CDA Server
Remote Client Interface	POP3 interface
Test Server	Omscan Server
Request Server	

Table 21: Service, Queue, and Daemon Commands

Command	Description
omisoff	Check Scalix services are off.
omoff	Stop one or more services.
omon	Start one or more services.
omrc	Start Scalix.
omreset	Reset status of services or remove Scalix.
omresub	Resubmit messages.
omresubdmp	Resubmit messages processed by the Archive Server.
omsetsvc	Display the status of a service in detail; configure auxiliary processes.
omshut	Stop Scalix.
omstat	List Scalix daemons.

System Configuration and Maintenance Commands

To view the Scalix version number, use the omvers command.

Table 22: System Configuration and Maintenance Commands

Command	Description
omcheck	Check Scalix file permissions and ownership.
ommon	Monitor the operation of Scalix.
omstat	Show the status of the system.
omvers	List version numbers of all binaries and scripts.

User Account Commands

You can use commands to add and delete user accounts.

Table 23: User Account Commands

Command	Description
omaddu	Add a user account.
omadmidp	Configure system IDs for use by Scalix users.
omconfpwd	Configure password controls.
omdelu	Delete one or more user accounts.
ommoddl	Modify distribution list entries and auto-action addresses, for example when a user changes their name.
ommodu	Modify a user account.
omshowpwd	Show password controls, such as expiry period and minimum length of passwords.
omshowu	List users or display details about a specific user.

A

Access Control Lists	
commands	130
types	128
Active Directory	135
administrator	
error manager	196
full administrator	46
group manager	49, 71
groups	47
types, roles defined	45
alias configuration options	217, 241
ALL-ROUTES file	153
ALL-ROUTES.VIR file	154, 220
anti-virus, configuration options	220
archive e-mail	171
authentication ID format	27

B

backup	
export/import	109
full	100
incremental	108
individual user	109
restore	110

C

catch-all user account	143
character sets	182, 189, 213, 238, 245
Client Directory Access	
commands	142
configuration options	173
use	141
commands	
Access Control Lists	130
Client Directory Access	142
directories	137
directory synchronization	251
e-mail	254
error manager	251
general	250
group	73
LDAP	253
logs	249
mailnode	44, 251, 252
message store	255
public distribution lists	73
public folders	125
routing	152
services and daemons	87
user accounts	64
Community Edition	12
components installed, viewing	87
conference rooms	75
configuration files	169

connections, IMAP	179
connections, User Access Layer	207
contact information	35, 58
country name	131

D

Deferred Mail Manager	152
delegates	64, 240
deleted mail, recover	148
designate user	240
Direct member of group	65
directories	
Client Directory Access	141
commands	137, 142
configuration options	174
create	139
FREEBUSY	136
search	139
SYSTEM	136, 138
USERLIST	136
directory synchronization	176, 251
disaster recovery	110
disk space, monitor use	85
domain	29
mail	37
mailnode	42
server	26

E

editions of Scalix	12
Effective member of group	65
e-mail	
archive	171
commands	254
configuration options	177
delay delivery	159
delegates	64, 240
delivery rules	155
force delivery of deferred mail	164
forwarding using script	98
log information about	183
monitor queues	86
non-delivery configuration	196
non-delivery notice	144, 161
non-delivery, account to receive	143
recover deleted	148
searches	63, 165
view deferred messages	164
e-mail address	
adding for user	58
delete	59
for public folder	95
format	29
group	70
public folder	119, 124
resource, shared	76

- e-mail domain 42
 - Enterprise Edition 12
 - error manager 196
 - executable plug-ins 89
- F**
- file permissions 259
 - filter 19
 - forward e-mail 98
 - freebusy directory 136
 - full administrator 46
- G**
- gateway
 - commands 253
 - configuration options 183
 - general.cfg configuration file 169
 - group
 - add 67
 - add users 69
 - administrator 47
 - change name 70
 - commands 73
 - delete 71
 - e-mail address 70
 - manager 71
 - users in a group 69
- H**
- help 10
 - help, MAN pages 248
 - hostname, change for server 145
- I**
- IMAP
 - configuration options . . . 177, 182, 216, 224, 235
 - logs 180, 236
 - set Scalix server for 180
 - stop and start service 82, 258
 - Inbox
 - read mail using commands 254
 - set size with configuration option 212, 238
 - IP address, change for server 146
- L**
- language, configuration options 245
 - LDAP
 - commands 253
 - configuration options 195
 - see Setup and Configuration Guide 135
 - license
 - add 24
 - view 24
 - local mailbox using SmartCache 62
 - lock out user 34
 - locked user account, unlocking 62
 - log information about e-mails 183
 - login
 - alias configuration options 217, 241
 - as group manager 72
 - block repeat failure 34
 - configuration options 213, 243
 - designate configuration option 240
 - format 17, 27
 - log in 16
 - troubleshoot 62
 - logout 21
 - logs
 - commands 249, 252
 - configuration options 172, 193
 - IMAP 180
 - IMAP configuration options 236
 - set level for service 83
 - view 83
- M**
- mail
 - domain 37
 - local cache 28
 - monitor queues 86
 - read from command line 254
 - mailbox full 214, 218, 239, 241
 - mailbox size
 - messages to users 218
 - set for user account 61
 - set globally 30
 - set with configuration option 214, 239
 - mailing lists 67
 - mailnodes
 - add 41
 - commands 44, 251, 252
 - delete 44
 - delete all user accounts from 60
 - delete user accounts from 43
 - domain 42
 - move users among 43
 - resource, boardroom, etc 76
 - view 40
 - MAN pages for information 248
 - meetings, scheduling 75, 78
 - message queues, monitor 86
 - message store
 - commands 255
 - configuration options 193, 222
 - monitor space used 85
 - size configuration option 214, 239
 - Microsoft Active Directory 135

Microsoft Exchange, public folders and 124

Microsoft Outlook

- book meeting room 78
- configuration options 226, 244
- directory entries 141
- folder synchronization 197
- password retention configuration option . . . 228
- search 165
- SmartCache 28, 62
- TNEF 171

monitor

- components installed 87
- deferred mail 164
- disk space 85
- message queues 86
- operation 259
- users logged in 84

multiserver installation

- backups 109
- synchronize public folders 120

N

name, change server 145

No SIS URL for this user 167

O

O/R address attributes 131

omscan 198

organizational unit 131

Outbox, set size with configuration option . . . 215

out-of-office notice, limit number 32, 194

P

passwords

- configuration options 210, 215, 216, 236, 240, 243
- do not work 62
- expiry and repeat use 33
- for shared resource 79
- for user accounts 57
- set format 33

permissions

- file 259
- public folders 116

personal name 131

plug-ins to run executables 89

POP

- configuration options 182, 199, 216
- stop and start service 82, 258

printers 75

projectors 75

public distribution lists 65

public folders

- Access Control Lists 128
- add 114

- commands 125
- configuration options 200, 210, 214
- configuration options for IMAP clients 182
- create using script 95
- deleting 119
- disable and enable access 210
- e-mail address 119, 124
- maintaining 119
- migrate 124
- permissions 116, 208
- Premium users only 114
- synchronize 120
- view/list 115
- with Lotus Notes 124
- with Microsoft Exchange 124

Q

queue, configuration options 201

R

recovery folder

- configuration options 202, 223
- default hold period 149
- disable by setting to 0 149
- empty it 150
- restore deleted e-mail 148
- view, make visible 148

redirect account for undeliverable mail 143

resource

- booking 78
- delete 80
- e-mail address 76
- passwords 79
- set up 76

routing

- commands 152
- configuration options 203
- create e-mail delivery rule 155

rules for e-mail delivery 151

S

SASL 222

Scalix Community Edition 12

Scalix components installed 87

Scalix Enterprise Edition 12

Scalix Management Console 15

Scalix Recovered Items folder 147, 202

Scalix Search and Index Service

- create index 166
- disable 167
- languages 168
- re-create index 167
- types of documents searched 166

Scalix Small Business Edition 12

Scalix version number 87, 259

Scalix Web Access

- book meeting room 78
- Scalix Recovered Items folder 147
- search 165

ScalixAdmins 47, 66

ScalixGroupAdmins 47, 66

ScalixUserAdmins 47, 66

ScalixUserAttributesAdmins 47, 66

search

- configuration options 202
- directory for user accounts 139
- disable for user accounts 167
- fix for users 167
- index for user accounts 166
- languages 168
- mailbox 63
- repair 63
- time-out 181
- types of documents searched 166

Search and Index Service. See Scalix Search...

Service Router 155

services

- commands 87
- logs 83
- start, stop 82, 88, 258

Show Recovery Folder button 148

SIS URL 167, 168

Small Business Edition 12

SmartCache 28, 62

space, check how much being used 30, 198

start Scalix with omrc command 88

stop Scalix with omshut command 88

synchronize directories, options 176

synchronize folders, Microsoft Outlook 244

synchronize public folders 120

format 27

group manager 49, 71

information 35

Internet Mail user 51

log in as group manager 72

log in as user 16

login format to use 17

mailbox size 30, 61

passwords 57

Premium and Standard user 51

search directory for 139

SmartCache 28, 62

troubleshoot login 62

types 14

view deferred mail of 164

V

version number of Scalix 87, 259

versions of Scalix 12

view, change in Scalix Management Console 19

virus, configuration options 220

T

TNEF 171

U

undeliverable mail

- create account to receive 143
- user who receives notice 144

unlock user account 62

User Access Layer configuration options 181, 207, 236

user accounts

- add 53, 64
- add to group 69
- change type 59
- commands 64
- contact information 58
- currently logged in 84
- delete 60, 64
- e-mail address format 29
- e-mail addresses 58

