

Lucent Technologies
Bell Labs Innovations



INTUITY™ Messaging Solutions
Enhanced-List Application
Release 1.0

585-310-575
Comcode 107975674
Issue 1
July 1997

Copyright © 1997, Lucent Technologies
All Rights Reserved
Printed in U.S.A.

Notice

Every effort was made to ensure that the information in this book was complete and accurate at the time of printing. However, information is subject to change.

Your Responsibility for Your System's Security

Toll fraud is the unauthorized use of your telecommunications system by an unauthorized party, for example, persons other than your company's employees, agents, subcontractors, or persons working on your company's behalf. Note that there may be a risk of toll fraud associated with your telecommunications system and, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

You and your system manager are responsible for the security of your system, such as programming and configuring your equipment to prevent unauthorized use. The system manager is also responsible for reading all installation, instruction, and system administration documents provided with this product in order to fully understand the features that can introduce risk of toll fraud and the steps that can be taken to reduce that risk. Lucent Technologies does not warrant that this product is immune from or will prevent unauthorized use of common-carrier telecommunication services or facilities accessed through or connected to it. Lucent Technologies will not be responsible for any charges that result from such unauthorized use.

Lucent Technologies Fraud Intervention

If you *suspect that you are being victimized* by toll fraud and you need technical support or assistance, call Technical Service Center Toll Fraud Intervention Hotline at 1 800 643-2353.

Federal Communications Commission Statement

Part 15: Class A Statement. This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Part 68: Network Registration Number. This equipment is registered with the FCC in accordance with Part 68 of the FCC Rules. It is identified by FCC registration number xxx.

Part 68: Answer-Supervision Signaling. Allowing this equipment to be operated in a manner that does not provide proper answer-supervision signaling is in violation of Part 68 Rules. This equipment returns answer-supervision signals to the public switched network when:

- Answered by the called station
- Answered by the attendant
- Routed to a recorded announcement that can be administered by the CPE user

This equipment returns answer-supervision signals on all DID calls forwarded back to the public switched telephone network. Permissible exceptions are:

- A call is unanswered
- A busy tone is received
- A reorder tone is received

Canadian Department of Communications (DOC) Interference Information

This digital apparatus does not exceed the Class A limits for radio noise emissions set out in the radio interference regulations of the Canadian Department of Communications.

Le Présent Appareil Numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la class A prescrites dans le règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

Trademarks

See the preface of this document.

Ordering Information

Call: Lucent Technologies Publications Center
Voice 1 800 457-1235 International Voice 317 361-5353
Fax 1 800 457-1764 International Fax 317 361-5355

Write: Lucent Technologies Publications Center
P.O. Box 4100
Crawfordsville, IN 47933

Order: Document No. 585-310-575
Comcode 107975674
Issue 1, July 1997

For additional documents, refer to the section in "About This Document" entitled "Related Resources."

You can be placed on a standing order list for this and other documents you may need. Standing order will enable you to automatically receive updated versions of individual documents or document sets, billed to account information that you provide. For more information on standing orders, or to be put on a list to receive future issues of this document, contact the Lucent Technologies Publications Center.

Comments

To comment on this document, return the comment card at the front of the document.

Acknowledgment

This document was prepared by the Product Documentation Development, Lucent Technologies, Denver, CO and Columbus, OH.



Contents

About This Book

- Purpose v
- Intended Audiences v
- Trademarks and Service Marks vi
- Related Resources viii
- How to Comment on This Book viii

1 Enhanced-List Application

- Overview 1
 - Audience 1
 - What You Should Know 1
- Enhanced-List Application 2
- What ELA Can Do for You 2
- ELA Administration 3
 - Basic Concepts 3
 - Planning with Professional Services 3
 - Things to Consider 4

2 Installation

- Overview 9
- Installing the Software 9
- Rebooting the System 11

3 Administering AUDIX for ELA

- Overview 13
- Activating ELA 14
- Verifying that ELA is Enabled 14

Contents

■ Increasing the Number of Mailing Lists Allowed on the System	15
■ Defining an ELA Class of Service	16
■ Setting Up ELA and Shadow Mailbox Community IDs	19
Things to Consider	19
Before You Begin	20
ELA Community ID	20
Shadow Mailbox Community ID	22
■ Administering TCP/IP	23
Before You Begin	23
■ Setting Up IMAPI Sessions for Trusted Server Access	26
■ Defining Two ELA Trusted Servers	28
Before You Begin	28

4 Administering ELA for AUDIX

■ Overview	33
■ Defining the AUDIX server and Administering Access	33
Before You Begin	33
■ Guidelines for Naming Enhanced Lists	37
■ Creating Enhanced Lists	38
Guidelines for Selecting Enhanced-List Members	41
Adding Members to Enhanced Lists	41
Adding/Deleting Members to an Enhanced List	43
■ Deleting an Enhanced List	46
■ Recording Names for Enhanced Lists	48
■ Testing INTUITY Enhanced Lists	48

5 Preventative Maintenance and Troubleshooting

■ Overview	51
------------	----

Contents

■ Checking the Administrator's Log	51
■ Checking the Delivery Failure Log	52
■ Delivery Failure Codes	54
■ Troubleshooting ELA	55

6

Alarms

■ Overview	59
■ DELIVTS Resource Type	59
■ REGISTRY Resource Type	61
■ SHADOW Resource Type	62
■ EL — Enhanced-List Application	65

IN

Index

Contents

About This Book

Purpose

This book contains instructions for installing and administering the Enhanced-List Application (ELA) on an INTUITY™ AUDIX® R4 system.

Intended Audiences

This book is intended primarily for the on-site technical personnel who are responsible for installing and configuring the system and performing initial administration and acceptance testing. Secondary audiences include the following from Lucent:

- Field support — Technical Service Organization (TSO)
- Helpline personnel
- Factory assemble, load, and test (ALT) personnel
- Provisioning project managers — Sales and Technical Resource Center (STRC)

This book assumes that the primary users of this book have completed the INTUITY AUDIX Administration training course.

Trademarks and Service Marks

The following trademarked products are mentioned in books in the Lucent INTUITY document set:

- AT™ is a trademark of Hayes Microcomputer Products, Inc.
- AUDIX® is a registered trademark of Lucent Technologies™.
- cc:Mail® is a registered trademark of cc:Mail, a subsidiary of Lotus Development Corporation.
- COMSPHERE® is a registered trademark of Lucent Technologies™ Paradyne Corp.
- CONVERSANT® Voice Information System is a registered trademark of Lucent Technologies™.
- DEFINITY® is a registered trademark of Lucent Technologies™.
- DMS-100™ is a trademark of Northern Telecom Limited.
- Dterm™ is a trademark of NEC Telephones, Inc.
- Equinox™ is a trademark of Equinox Systems, Inc.
- 5ESS® is a registered trademark of Lucent Technologies™.
- INTUITY™ is a trademark of Lucent Technologies™.
- Lotus Notes® is a registered trademark of Lotus Development Corporation.
- MEGAPORT™ is a trademark of Equinox Systems, Inc.
- MEGAPLEX™ is a trademark of Equinox Systems, Inc.
- Meridian™ is a trademark of Northern Telecom Limited.
- MERLIN LEGEND® is a registered trademark of Lucent Technologies™.
- Microcom Networking Protocol® is a registered trademark of Microcom, Inc.
- Microsoft® is a registered trademark of Microsoft Corporation.
- MS® is a registered trademark of Microsoft Corporation.
- MS-DOS® is a registered trademark of Microsoft Corporation.
- Mitel™ is a trademark of Mitel Corporation.
- NEAX™ is a trademark of NEC Telephone, Inc.
- NEC® is a registered trademark of NEC Telephone, Inc.
- Netware® is a registered trademark of Novell, Inc.
- Netware® Loadable Module™ is a registered trademark of Novell, Inc.
- Northern Telecom® is a registered trademark of Northern Telecom Limited.

- Novell® is a registered trademark of Novell, Inc.
- Paradyne® is a registered trademark of Lucent Technologies™.
- Phillips® is a registered trademark of Phillips Screw Company.
- Rolm® is a registered trademark of International Business Machines.
- SL-1™ is a trademark of Northern Telecom Limited.
- softFAX® is a registered trademark of VOXEM, Inc.
- SUPERSET™ is a trademark of Mitel Corporation.
- SX-100™ is a trademark of Mitel Corporation.
- SX-200™ is a trademark of Mitel Corporation.
- SX-2000™ is a trademark of Mitel Corporation.
- Telephony OneStip™ is a trademark of Lotus Development Corporation.
- TMI™ is a trademark of Texas Micro Systems, Inc.
- UNIX® is a registered trademark of UNIX Systems Laboratories, Inc.
- Voice Bridge® is a registered trademark of Voice Technologies Group, Inc.
- VOXEM® is a registered trademark of VOXEM, Inc.
- VT100™ is a trademark of Digital Equipment Corporation.
- Windows™ is a trademark of Microsoft Corporation.

Related Resources

If you need help with basic administrative procedures, see the *INTUITY™ Messaging Solutions Release 4 Administration* book, 585-310-564.

How to Comment on This Book

We are always interested in your suggestions for improving this book. Please complete and return the reader comment card that is located behind the title page.

If the reader comment card has been removed, send your comments to:

Lucent Technologies
Product Documentation
Room 22-2H15
11900 North Pecos Street
Denver, Colorado 80234

Alternatively, you can fax your comments to:

Lucent INTUITY Writing Team
(303) 538-1741

Please be sure to mention the name and order number of this book.

Enhanced-List Application

1

Overview

This chapter describes the Enhanced-List Application (ELA) on an INTUITY™ AUDIX® Release 4 system.

Audience

Read this book if you are the AUDIX system administrator responsible for the configuration and maintenance of an INTUITY AUDIX Release 4 system.

What You Should Know

The procedures in this chapter assume you know basic Lucent INTUITY commands and navigation, such as logging in and out of the system, the difference between the VM and SA logins, command prompt function and usage, and how to move from field-to-field within a screen or window.

If you are not familiar with Lucent INTUITY system basics, please read Chapter 1 in *INTUITY Messaging Solutions Release 4 Administration* before you continue.

Enhanced-List Application

The Enhanced-List Application (ELA) greatly expands your business' capability to deliver messages to large numbers of recipients. A single enhanced list can contain 1500 addresses and you – the system administrator – can create up to 100 such lists. Enhanced lists can be nested (or embedded) in each other, that is, a list (containing 1500 addresses) can be a member contained in another list. By doing so, your users can record a message, address it to the parent enhanced list, and send it to nearly 150,000 people – just as easily as if the message were being sent to a person 1 desk away.

All users administered in AUDIX (including e-mail and remote users) can send messages to the recipients on enhanced lists, or you can administer your system to only allow selected users in your AUDIX network access to the enhanced lists.

ELA has the following characteristics:

- Up to 1500 recipients can be contained in an enhanced list (compared to 250 addresses in a standard AUDIX mailing list.)
- Up to 100 enhanced lists can be created on an INTUITY AUDIX machine
- Nesting (embedding an enhanced list within another Enhanced List) enables a total recipient population of nearly 150,000
- Changes in an enhanced list propagate to all lists that refer to the changed list
- Access to enhanced lists from anywhere within the AUDIX network (standard AUDIX mailing lists are only accessible to those users with mailboxes on the same machine as the lists)
- Delivery to local and remote AUDIX users, administered e-mail users, and remote AMIS pre-administered users
- Cross-domain delivery from an e-mail trusted server to AUDIX. This enables administered e-mail users to access the Enhanced Lists

What ELA Can Do for You

ELA can:

- Distribute messages to a targeted audience.

You can create a list of people that you send messages to frequently. Then, you can send them all the same message by entering one enhanced-list address.

- Centralize messages into one AUDIX mailbox.

First select one office as your primary location. Then create an enhanced list at each secondary location that has, as its only member, the number of your primary office location. When a mailbox at a secondary location receives a message, ELA puts it into the mailbox for the primary office.

- Forward messages to support staff automatically.

If you often forward incoming messages, you can create an enhanced-list mailbox that automatically forwards messages to your staff. Your staff can review the messages and then respond to them as they normally would.

ELA Administration

Only the system administrator (sa) login can administer enhanced lists.

Basic Concepts

To understand ELA, you first need to understand some concepts and terminology, such as *trusted servers* and *domains*.

A *trusted server* is a computer or a software application in a domain outside of INTUITY AUDIX that uses its own login and password to launch an IMAPI session and access AUDIX mailboxes. The ELA software, acting as a trusted server, can access and manipulate an AUDIX message just as the AUDIX application does.

For the purposes of ELA, a *domain* is a logical boundary defined by the application. INTUITY AUDIX voice/fax mail messaging is one domain, and ELA is another domain. The two domains are linked together to allow messages to be distributed between domains.

For a complete discussion and definition of trusted server and domain, see your *INTUITY Messaging Solutions Release 4 Administration* book.

Planning with Professional Services

ELA is a separately purchasable feature that incurs a Right-to-Use (RTU) fee. ELA requires some solid planning to ensure your system makes effective use of the feature. You can contract with Professional Services to work with you to plan and administer ELA, or you can do the planning and administration yourself using ELA worksheets that your account representative provides. In either case, the result of that planning is completed ELA worksheets that you will use as you proceed to implement ELA.

ELA also requires some AUDIX Administration, as well as administration of the ELA server itself.

This administration can be divided as follows:

AUDIX Administration:

- Contact Professional Services (or your account representative, if you did not contract with Professional Services) to have ELA installed.
- Contact Professional Services (or your account representative, if you did not contract with Professional Services) to have ELA activated.
- Verify that ELA is enabled for your system.
- Increase the number of mailing lists AUDIX allows on the system.
- Define an ELA Class of Service.
- Set up ELA and shadow mailbox Community IDs.
- Administer TCP/IP on the AUDIX server.
- Define two ELA trusted servers to the AUDIX server and administer access (including the surrounding security requirements).
- Set up IMAPI sessions for ELA server access to AUDIX.

ELA Administration:

- Define the AUDIX server to the ELA servers and administer access.
- Select shadow mailbox extension.
- Create and administer the Enhanced List(s).
- Record a name for the enhanced list (optional).

The next section highlights the planning considerations for implementing ELA. Administration procedures begin with "Installing the Software" on page 2-9.

Things to Consider

ELA is a powerful messaging tool that can distribute large quantities of messages. The following section discusses various planning considerations that should be addressed to ensure effective implementation and use of ELA.

ELA Message Delivery

We recommend that you schedule delivery for large enhanced lists during off-peak hours.

ELA can deliver up to 100 messages a minute. However, during peak traffic hours, your system also processes other user-generated messages. ELA intentionally slows delivery of messages to large enhanced lists during peak traffic so your system can continue to process these other messages.

Hardware/Software Requirements

ELA runs on the same machine as AUDIX.

- ELA must be installed on a Lucent INTUITY R4.2-4 or higher machine. If your site has an earlier release, contact your Lucent service representative to obtain the necessary upgrade. ELA is not available for pre-R4 Lucent INTUITY systems.
- MAP/40s machines require 64k of RAM.

LAN Impact

If your configuration includes a LAN, planning ELA implementation should involve your PC/LAN administrator(s) to ensure that AUDIX and the network are not adversely affected. The amount of LAN traffic on your system from ELA messages could increase if ELA will be sending messages for delivery to an e-mail or Message Manager recipient or to TCP/IP-networked remote machines. If none of these are valid for your site, ELA will not cause any LAN traffic.

See Chapter 6 in your *INTUITY Messaging Solutions Release 4 Administration* book:

- If your site has e-mail, to calculate some initial traffic estimates
- If your site has Message Manager, to calculate some initial traffic estimates

Remote Message Impact

If your site is networked, estimate the increase in the amount of remote traffic by first determining the percent of current traffic that is remote and calculating the number of messages/minute that percent represents. When ELA is actively sending messages, add that number of messages to the traffic estimate for remote message delivery.

NOTE:

For typical applications of ELA, the increase in messaging traffic can be negligible.

Port Usage Impact

Voice port usage increases as recipients retrieve messages sent by ELA. Plan for the increase with Professional Services when you purchase ELA. Refer to the worksheets that were compiled at the time of the purchase to determine the port usage impact.

You should monitor your system to determine if your Grade of Service (GOS) falls below acceptable levels. If that happens frequently, particularly during the peak busy hour, contact your Lucent account representative to purchase more ports, if necessary. For more information about GOS and monitoring your system, see your *INTUITY Messaging Solutions Release 4 Administration* book.

NOTE:

If, in its application, ELA degrades service, you might suggest that those users with access to enhanced lists schedule delivery of ELA messages for off-peak hours, for example, at 10:00 p.m. or 4:00 a.m. That way, delivery of messages will not conflict with other user-generated traffic.

Security

Securing a system that allows access from another domain involves a 2-pronged approach. You must consider security from both an internal and an external perspective. External security involves administration to prevent access from an unauthorized source, such as an e-mail or AMIS-Analog message originator that decides to send "mail bombs" to an Enhanced List. Internal security focuses on preventing, or recovering from, damage if a breach occurs, for example, a virus is transmitted in a message component such as an attached software file.

For an in-depth discussion and definition of such terms as *trusted server* and *domain*, see your *INTUITY Messaging Solutions Release 4 Administration* book.

External Security

A new option — the trusted server — has been introduced in this release. The ELA application runs as a trusted server, making requests of the AUDIX server, via IMAPI, to distribute messages to designated recipients. The trusted server is empowered to do anything to an ELA mailbox that an AUDIX user can do.

To prevent unauthorized access to AUDIX from an external source such as a trusted server, system administrators have two levels of security at their disposal:

- Trusted server password
- IMAPI password

The trusted server password is administered on both the AUDIX server and on the trusted server. The trusted server must use this password when it connects to AUDIX.

The IMAPI password is an optional, secondary level of security used to prevent an unauthorized source external to AUDIX from starting an IMAPI session. We *strongly recommend* that you take advantage of this extra protection.

If you choose to administer an IMAPI password, we recommend that you change it on a regular basis, for example, monthly. (If you have set your administrator's password to age automatically, the system prompts you to change your password. You can use this prompt to remind you to change the IMAPI password as well.)

⇒ NOTE:

If you change an IMAPI password in AUDIX, all trusted servers must be administered with the new IMAPI password. For example, if your INTUITY AUDIX R4 supports an e-mail server, the e-mail administrator must also administer the e-mail trusted server to reflect the new IMAPI password.

In addition to trusted server security, there is the possibility that an administered e-mail or remote AMIS Analog user could use an ELA mailbox in an unauthorized manner. One example is to send "mail bombs" to an Enhanced List. Mail bombs are harassing messages that do not serve your business needs, and impose unnecessary traffic on your system. ELA mailboxes are no more vulnerable to unauthorized use than other voice mailboxes. However, the impact on system performance can be many times greater than the potential for harassment when sending messages to an individual mailbox. Sending to an enhanced list that forwards a message to 1500 recipients will obviously have much farther reaching consequences than that of a handful of messages sent to individual mailboxes.

To prevent unauthorized access to an ELA mailbox from an external source such as e-mail users or remote AMIS Analog users, you can place those users in a community with sending restrictions. See:

- "Setting Up ELA and Shadow Mailbox Community IDs" on page 3-19 for information about administering ELA community sending restrictions
- "Setting Up Community Sending Restrictions" in Chapter 3 of your *INTUITY Messaging Solutions Administration* guide for information about the implications of administering Community IDs

Internal Security

INTUITY AUDIX R4 allows the transmission of 2 new message components, text (originating from Message Manager or e-mail) and binary file attachments (software files, such as a spreadsheet or word processing file). With these new components come new security considerations, namely, the inadvertent delivery of a virus that may be embedded in a file attachment. This can occur in any system that supports the delivery of software files. While the AUDIX machine

cannot be infected with viruses embedded in these software files, client machines may become infected when a user launches the application associated with the software file.

 **CAUTION:**

ELA does not perform any virus detection. Your company should evaluate the security risks of file attachments carefully and make provisions for virus detection software on PCs running Message Manager or an e-mail application supported by INTUITY AUDIX R4.

At a minimum, you should advise your users that file attachments should be detached (not launched) and scanned for viruses before use.

IMAPI Session Requirements

An IMAPI session is invoked when an e-mail trusted server, Message Manager, or the ELA trusted server needs to communicate with the AUDIX server. The AUDIX server must have a sufficient number of IMAPI sessions administered to provide adequate access for all IMAPI requests. Additionally, the ELA server must be registered as an AUDIX trusted server.

Shadow Mailbox

The shadow mailbox is a special mailbox that ELA uses to distribute messages. The use of a shadow mailbox prevents replies to ELA-delivered messages from being sent back to the entire Enhanced List. However, you can administer enhanced lists such that recipients can reply to the person who originally sent the message. The shadow mailbox must belong to a community that cannot receive messages.

Overview

This chapter describes how to install ELA on a Lucent INTUITY R4.2 or higher system.

Installing the Software

The ELA package is provided on a tape labeled *Enhanced-List Application*.

To install ELA on a Lucent INTUITY R4.2 or higher system:

1. Log in to the Lucent INTUITY system using `craft` or `tsc`.
2. Starting from the main menu, select:

```
> Customer/Services Administration
```

```
>System Management
```

```
>UNIX Management
```

```
>Software Install
```

The system displays the Software Install menu (Figure 2-1).

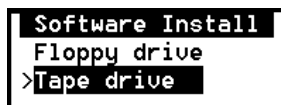


Figure 2-1. Software Install Menu

3. Insert the tape labeled *Enhanced-List Application* into the tape drive.
4. Select:



The system displays the message:

```
Insert a tape into the Tape Drive.
Type [go] when ready
or [q] to quit: (default: go)
```

5. Press **(ENTER)** to go ahead with the install.

The system displays the message:

```
Installation in progress. Do not remove the tape.
```

```
The following packages are available:
1 ELA      Enhanced List Application Package

Select package(s) you wish to process (or 'all' to
process all packages). (default: all) [?, ??, q].
```

⇒ NOTE:

If you receive a `device open failure` message, the tape was inserted *after* you selected `Tape Drive` or the system did not see the tape. In that case, complete step a through step d below.

- a. Enter **q**
The system displays the Software Install menu (Figure 2-1).
- b. Remove the tape from the tape drive.
- c. Re-insert the tape into the tape drive.
- d. Repeat step 4 and step 5.

6. Press `(ENTER)` to select all.

The system installs the software and displays several status messages. When the software installation is complete, the system displays the message:

```
Installation of Enhanced List Application Package
was successful.
```

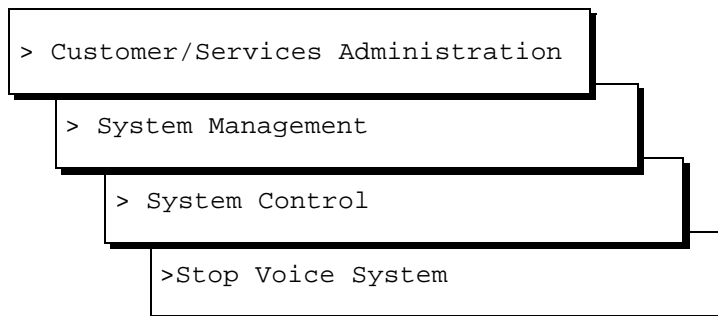
```
Insert a tape into the Tape Drive.
Type [go] when ready
or [q] to quit: (default: go)
```

7. Remove the tape from the tape drive and re-insert the back-up tape.
8. Enter **q**
9. Press (F6) `(CANCEL)` repeatedly to return to the main menu.
10. Continue with the next procedure, "Rebooting the System".

Rebooting the System

Rebooting is a 2-step process. First the voice system must be stopped, and then the machine can be rebooted. To stop the voice system:

1. Starting from the main menu, select:



The system displays the Wait Time window (Figure 2-2).



Figure 2-2. Wait Time Window

2. Enter **60** in the `Seconds :` field to have the system wait one minute for calls in progress to finish before stopping the voice system.

3. Press (F3) **(SAVE)**.

The system stops the voice system and displays the a series of status messages. When the voice system has stopped, the system displays the message:

```
The Voice System has stopped.  
Press Enter to Continue.
```

4. Press **(ENTER)**.
5. Press (F6) **(CANCEL)**.

The system displays the System Control window.

6. Select

```
>Shutdown System
```

The system displays the Wait Time window (Figure 2-2).

7. Enter **0** (zero) to indicate you would like an immediate shutdown.
8. Press (F3) **(SAVE)**.

The system displays the following message:

```
Shutdown started.
```

When the system is completely shut down, the system displays the message.

```
The system is down.  
Press Ctrl-Alt-Del to reboot your computer.
```

9. Make sure that there is no diskette in the diskette drive.
10. Press **(CONTROL) (ALT) (DEL)**.

The system performs a power-on self test (POST). The screen lists various hardware components and the status of the tests performed on those components.

When the reboot is complete, the system displays the following prompt:

```
Startup of the Voice System is complete.  
Console Login:
```

Overview

To define the ELA server and functionality to AUDIX:

- Contact Professional Services (or your account representative, if you did not contract with Professional Services) to have ELA installed.
- Contact Professional Services (or your account representative, if you did not contract with Professional Services) to have ELA activated.
- Verify that ELA is enabled for your system.
- Increase the number of mailing lists AUDIX allows on the system.
- Define an ELA Class of Service.
- Set up ELA and shadow mailbox Community IDs.
- Administer TCP/IP on the AUDIX server.
- Define two ELA trusted servers to the AUDIX server and administer access (including the surrounding security requirements).
- Set up IMAPI sessions for ELA server access to AUDIX.

Depending on what services your business purchased from Professional Services during the planning phase for ELA, some of the following procedures may already be done. See your *INTUITY Messaging Solutions Release 4 Administration* book.

Activating ELA

After the ELA installation is complete, contact your Professional Services (or your account representative, if you did not contract with Professional Services). The technician from the remote support center will access your system remotely and activate the ELA feature.

When the remote support center has activated the ELA feature, continue with the next procedure.



NOTE:

You must log off the system and log back on to get enhanced lists to display as an option on the Lucent INTUITY main menu.

Verifying that ELA is Enabled

1. Log into the Lucent INTUITY system using sa.

The system should display the Lucent INTUITY main menu with Enhanced-List Manager as a menu option (Figure 3-1).

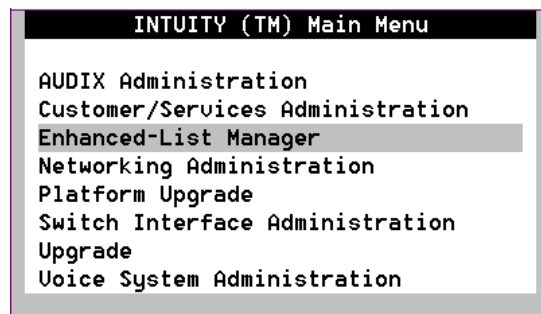
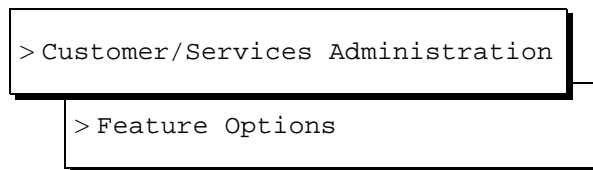


Figure 3-1. Lucent INTUITY Main Menu for Release 4 (with ELA)

2. If Enhanced-List Manager does not display on the main menu, select:



The system displays the Feature Options window.

3. Ensure the following fields are set to ON:
 - Enhanced List Application
 - TCP/IP Administration
4. If either of these fields is OFF, and you purchased/installed ELA, call the support center to request that the features be enabled for your Lucent INTUITY platform.
5. Press (F6) **CANCEL** to exit this window.

Increasing the Number of Mailing Lists Allowed on the System

The following task contains instructions for the fields that relate directly to ELA. See "Field Definitions: System-Parameters Limits Screen" in Chapter 3 of your *INTUITY Messaging Solutions Administration* guide for complete field descriptions and to understand their implications.

To administer AUDIX system limits to support ELA:

1. Starting from the main menu (Figure 3-1 on page 3-14), select:

```
> AUDIX Administration
```

2. At the `enter command:` prompt, enter either:

Full Command Version	Short Command Version
change system-parameters limits	ch sys li

The system displays the System-Parameters Limits screen.

3. Tab to the `Lists, Total Entries:` field and enter **200000**.
4. The `Lists/Subscriber` field has a default value of 100. If this setting has changed, enter a value of 15 or greater.

If the default value has not changed, skip this step.

5. The `Recipients/Lists` field has a default value of 250. If this setting has changed to less than the default, enter a value of **250**.

If the default value has not changed, skip this step.

NOTE:

If there was an administrative reason for reducing the value in this field, your system may not be able to support ELA. Review your system configuration and business needs to determine the implication of returning this setting to 250.

6. Press (F3) **(ENTER)** to save the information in the system database.
The cursor returns to the command line, and the system displays the message `Command Successfully Completed`.
7. Continue with the next procedure or enter **exit** to leave AUDIX Administration.

Defining an ELA Class of Service

The following task contains instructions for the fields that directly relate to ELA. The other fields should be administered to support all capabilities that you anticipate using, that is, maximum call answer length, announcement set, etc. See your *INTUITY Messaging Solutions Release 4 Administration* book for explanations of the other fields on these screens, and their implications.

⇒ NOTE:

ELA can take up to 12 hours to show the changes you make to subscriber information in INTUITY AUDIX.

Before you begin the following procedure, ensure that you have an unused Class of Service that you can define for ELA. We recommend that you use a COS that is between 2 and 11. (Customers often use COS 1 as their default Class of Service).

To administer a COS for ELA:

1. Starting from the main menu (Figure 3-1 on page 3-14), select:

```
> AUDIX Administration
```

2. At the `enter command:` prompt, enter either:

Full Command Version

Short Command Version

change cos *COS_number*

ch cos *COS_number*

where ***COS_number*** is the unique Class of Service you would like to use for ELA. For example, enter `ch cos 10`.

The system displays the Class of Service screen (Figure 3-2).

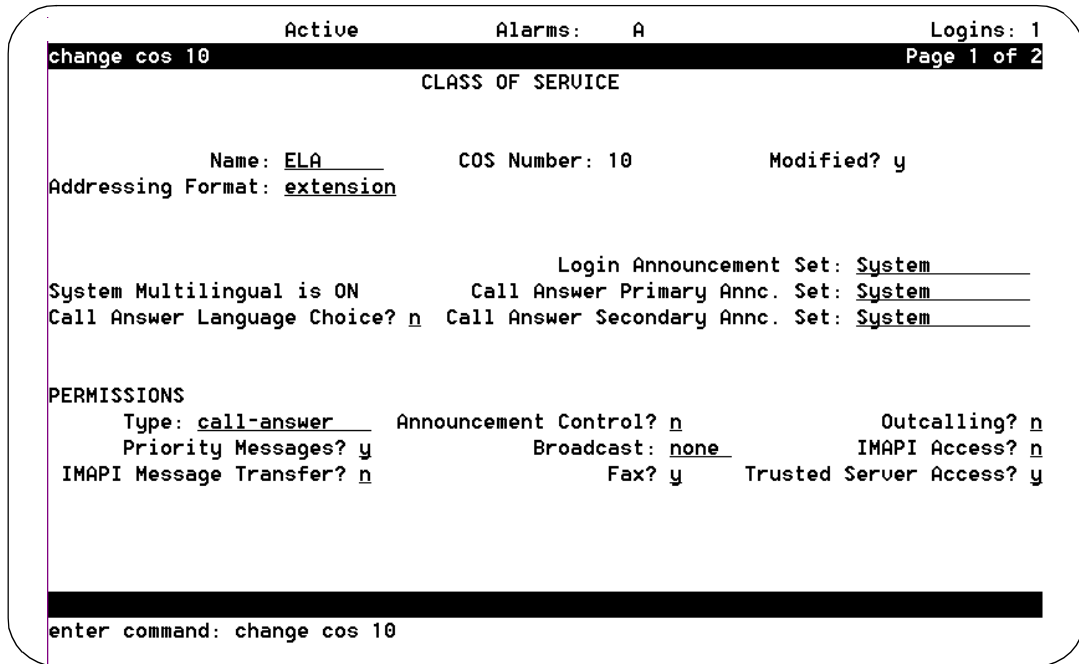


Figure 3-2. Class of Service Screen, Page 1; Defining a Class of Service for ELA

3. Although not required, we recommend that you change the name of the COS to be more descriptive, for example, enter ELA in the `Name:` field.

⇒ NOTE:

You should write down the COS number. You will need it later when you administer the ELA server.

4. If you would like ELA to be able to distribute call answer messages, enter **call-answer** in the `Type:` field (under `PERMISSIONS:`). Otherwise, enter **none**.

⇒ NOTE:

If you administer your system such that ELA mailboxes are to be accessible only by direct addressing and later decide you would like some ELA mailboxes with call answer capability, you do not need to create two Classes of Service. Administer the ELA COS to be call answer, but only administer the ELA mailbox extension as a number on the switch if/when you decide to allow call answer messages to be distributed to the members of that Enhanced List.

5. Enter **y** in following fields (under `PERMISSIONS:`):
 - Priority Messages?
 - Fax? (If you have purchased fax)
 - Trusted Server Access?
6. Press (F7) `(NEXTPAGE)`. The system displays page 2 (Figure 3-3).

```

drbash1          Active          Alarms: M A          Logins: 5
change cos 10    Page 2 of 2

CLASS OF SERVICE

INCOMING MAILBOX      Order: fifo          Category Order: nuo
Retention Times (days), New: 14      Old: 14              Unopened: 14

OUTGOING MAILBOX      Order: fifo          Category Order: nudaf
Retention Times(days),File Cab: 0      Delivered/Nondeliverable: 1

Voice Mail Message (seconds), Maximum Length: 1200 Minimum Needed: 8
Call Answer Message (seconds), Maximum Length: 1200 Minimum Needed: 8

End of Message Warning Time (seconds): 15

Maximum Mailing Lists: 6      Total Entries in all Lists: 1500
Mailbox Size (seconds), Maximum: 32767      Minimum Guarantee: 6

enter command: change cos 10

```

Figure 3-3. Subscriber Class of Service Parameters Screen, Page 2; Enabling ELA on a COS Basis

7. Enter the following information:

- **14** in the Retention Times (days), New: field. (This setting acts as a safety measure, should ELA encounter an operational problem, and cannot send messages for a couple of days.)
- **14** in the Retention Times (days), Old: field. (Ordinarily, there are no old or unopened messages. ELA will forward old/unopened messages in the event service is interrupted.)
- **14** in the Retention Times (days), Unopened: field. (The same explanation holds true for this field, as well.)
- **nudaf** in the Outgoing Mailbox, Category Order: field
- **0** in the Retention Times (days), File Cab: field
- **1** in the Delivered/Nondeliverable: field
- **6** in the Maximum Mailing Lists: field
- **1500** in the Total Entries in all Lists: field
- **32767** in the Mailbox Size, Maximum Length: field

⇒ NOTE:

Administer the other fields to be consistent with the messaging needs of your business.

- Press (F3) **(ENTER)** to save the information in the system database.
The cursor returns to the command line, and the system displays the message `Command Successfully Completed`.
- Continue with the next procedure or enter **exit** to leave AUDIX Administration.

Setting Up ELA and Shadow Mailbox Community IDs

The following task contains instructions that directly relate to ELA. "Setting Up Community Sending Restrictions" in Chapter 3 of your *INTUITY Messaging Solutions Administration* guide discusses the purpose and implementation of Community IDs in more detail.

Things to Consider

ELA mailing lists are a powerful messaging tool that all users in your AUDIX network can access. However, should your business needs indicate differently, you can control who can use the enhanced lists by administering community sending restrictions. Figure 3-4 illustrates a typical application of sending restrictions for ELA and this application of sending restrictions is used as a basis for the following discussion.

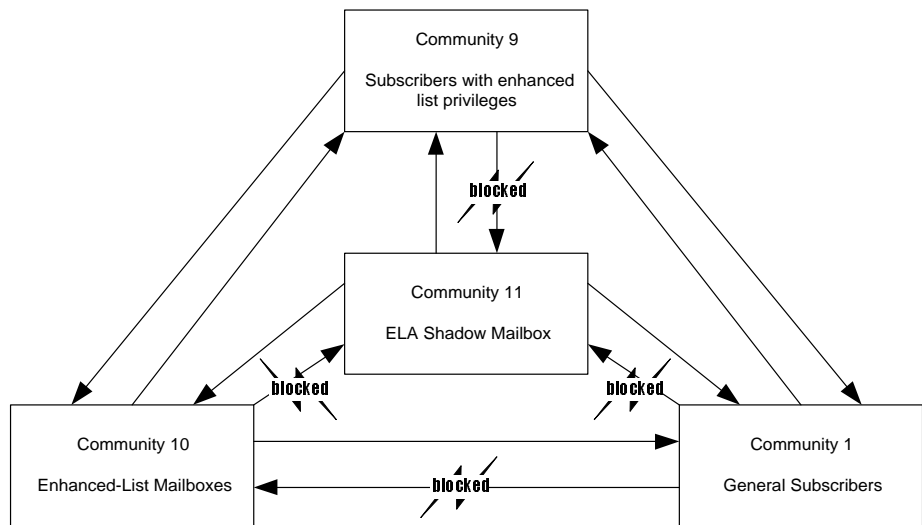


Figure 3-4. Example of Communities Administered for use with ELA

Let's say you set up the enhanced-list mailbox community to be Community 10. Community 10 is given permission to send to all other communities (except the shadow mailbox community). Then, you set up a special user community, Community 9, and administer Community 9 to send to all communities (except the shadow mailbox community). Only users you would like to have access to the enhanced lists are placed into Community 9. All other users would not be able to send a message to the ELA mailbox.

Additionally, you must set up a shadow mailbox community ID, for example Community 11. The shadow mailbox community ID is administered such that messages can be sent to any community, but messages cannot be received from any other community. You do this so replies from pre-Release 4 Lucent INTUITY machines or from DEFINITY AUDIX and AUDIX R1 machines do not go to the shadow mailbox.

Also, you will have to administer the rest of your user population to belong to a community restricted from sending messages to the enhanced-list mailbox community, for example, the default Community 1.

⇒ NOTE:

If your AUDIX system is networked with other Lucent INTUITY systems, all enhanced-list mailbox community sending restrictions must be consistently applied throughout the system, that is, the same Community ID numbers administered with the same restrictions. In particular, the shadow mailbox community must not be accessible by any other community on any machine in the network.

Before You Begin

Before you begin the following procedure, use the display system-parameters sending restrictions command in AUDIX administration and ensure that you have at least two Communities that you can use for ELA (4 communities are needed if you are going to implement a special community for selected users with access to ELA mailboxes.)

ELA Community ID

To set up sending an ELA Community ID:

1. Starting from the main menu (Figure 3-1 on page 3-14), select:

```
> AUDIX Administration
```

2. At the `enter` command: prompt, enter either:

Full Command Version

Short Command Version

change system-parameters sending-restrictions ch sy s

The system displays the Sending Restrictions screen (Figure 3-5).

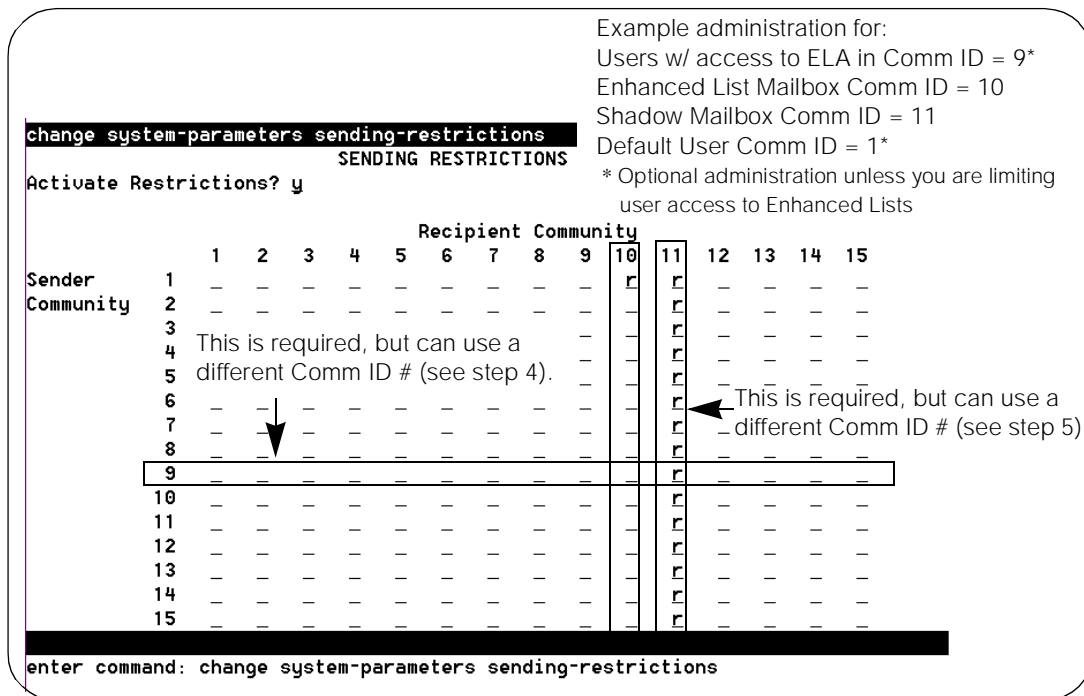


Figure 3-5. Sending Restrictions Screen

3. Enter **y** in the `Activate Restrictions?` field.
4. Leave all fields blank (horizontally) that correspond to the (sender) Community ID that you've assigned to ELA, and leave all fields blank (vertically) that correspond to the (recipient) Community ID you've assigned for users who will have access to the Enhanced Lists. (If all users are to have access to Enhanced Lists, the recipient community will be the default user community — usually community 1.)

Following the example discussed under "Things to Consider" on page 3-19, Sender Community 9 would be blank (horizontally from left to right) and Recipient Community 10 would be blank (vertically from top to bottom).

5. If all users are to have access to Enhanced Lists, skip this step.

Enter an **r** in the field that corresponds to the intersection between the (recipient) ELA Community ID and the (sender) community to which the rest of the user population belongs. This prevents those who do not have

access to enhanced lists from sending a message to an Enhanced List.

Following the example discussed under "Things to Consider" on page 3-19, there would be an **r** in the field corresponding to the intersection between Sender Community 1 (the default user community) and Recipient Community 10 (the Enhanced List Mailbox Community).

Shadow Mailbox Community ID

6. Enter an **r** in all (recipient community) fields in the column that corresponds to the Community ID that you've assigned to the shadow mailbox. This prevents messages from being sent into the shadow mailbox.

Following the example discussed under "Things to Consider" on page 3-19, Recipient Community 11 would contain **r**'s (vertically from top to bottom).

7. Press (F3) **ENTER** to save the information in the system database.

The system displays the message **Command Successfully Completed**, and the cursor returns to the command line.

8. Continue with the next procedure or enter **exit** to leave AUDIX Administration.

⇒ NOTE:

You must now use the Change Subscriber or Change COS screen to assign your users to either the community that does not have access to Enhanced Lists, or to the special community that does have access. If you used your default user community (Community 1) as the community that does not have access, then you only have to administer those selected individuals who will belong to the new special community with access to Enhanced Lists.

Administering TCP/IP

If your system is already connected to the LAN, you can skip this procedure. However, you need to know the IP Address to administer the trusted server, so — even if your system is already networked — perform step 1 of this procedure and write down your system's IP address.

TCP/IP is a set of protocols that links computers across a wide variety of networks. TCP/IP must be administered for the ELA trusted server to communicate with AUDIX.

Before You Begin

You will need to know the:

- Network IP address
- Host Identifier (AUDIX server name)
- Subnet mask
- Gateway Identifier (ID) to administer TCP/IP

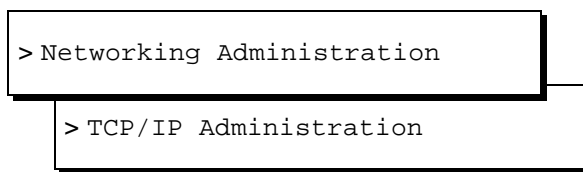
Your PC/LAN system administrator should have this information.

⚠ CAUTION:

Administering TCP/IP requires that you stop and restart the voice messaging software. Plan to do this procedure at a time when your business can tolerate some down time on your AUDIX system.

To administer TCP/IP Networking:

1. Starting from the main menu (Figure 3-1 on page 3-14), select:



The system displays the TCP/IP Administration window (Figure 3-6).

```
+-----+
| TCP/IP Administration |
+-----+
| UNIX Machine Name: denver1 |
| IP Address: xxx.x.xxx.x |
| Subnet Mask: 255.255.255.0 |
| Default Gateway IP Address: 135.9.180.254 |
+-----+
```

Figure 3-6. TCP/IP Administration Window; Administering TCP/IP for Enhanced-List Application (ELA)

2. Enter the AUDIX server name in the `UNIX Machine Name:` field. This name should be listed on the Installation Information worksheet, or you can obtain this name from your PC/LAN administrator. This is a case-sensitive field, so capital letters must be typed as capitals, and lowercase letters as lowercase.

⇒ NOTE:

This name must be the same as the local machine name specified on the Local Machine Administration screen. It cannot start with a number and cannot contain any embedded spaces, for example, `denver 1` is not allowed, but `denver_1` is allowed.

3. Enter the IP (Internet Protocol) address in the `IP Address:` field and press `(TAB)`. This is the Lucent INTUITY system's address. Your PC/LAN system administrator should have this information.

If your system is not connected to a LAN, enter any number in the format `w.x.y.z`, where each letter is a number, 0 to 255.

⇒ NOTE:

Write this IP address down, as you will need it when you administer the ELA trusted server later in this section.

4. Enter the subnet mask in the `Subnet Mask:` field.

The subnet mask is used to determine which bytes of the IP address specify the network and host addresses. This is an optional field. If there is no entry for this field on your worksheet, leave the field blank. The system will automatically use a default.

⇒ NOTE:

The default value may conflict with your LAN configuration. Check with your PC/LAN system administrator to ensure compatibility.

5. Enter the default gateway IP address in the Default Gateway IP Address: field.

The default gateway IP address is the address of the gateway router that serves to connect to addresses on other LANs. This field is left blank if the Lucent INTUITY system will only be communicating with other machines on the same LAN.

If your system is not connected to a LAN, enter the number you made up for step 3.

6. Press (F8) **CHG-KEYS** and then (F2) **BRD CNFG**. The system displays the Ethernet Board Configuration window (Figure 3-7).

The screenshot shows a terminal window with two main sections:

- TCP/IP Administration:**
 - UNIX Machine Name: denver1
 - IP Address: XXX.X.XX.XXX
 - Subnet Mask: _____
 - Default Gateway IP Address: XXX.X.XX.XXX
- Network Interface Types:**
 - 10BASE-T
 - AUI
 - BNC
 - Twisted Pair - No Link Integrity

Below these sections is the **Ethernet Board Configuration** window with the prompt: Network Interface Type: _____

At the bottom of the terminal window, the instruction reads: Select an interface type and press <Enter>

Figure 3-7. Ethernet Board Configuration Window; Administering TCP/IP for Enhanced-List Application (ELA)

7. Press (F2) **CHOICES** to display a list of the network interface types.
8. Highlight the network interface type to be used on this system and press **RETURN**. Your PC/LAN system administrator should have this information.
9. Press (F3) **SAVE** to save the Ethernet Board configuration.
10. Press (F6) **CANCEL** twice.
11. Press (F3) **SAVE** to save the TCP/IP administration values.
12. Press (F6) **CANCEL** repeatedly to return to the main menu.
13. Continue with the next procedure.

⇒ NOTE:

The changes to your system will not take effect until you reboot your system. See your *INTUITY Messaging Solutions Release 4 Administration* book for instructions.

Setting Up IMAPI Sessions for Trusted Server Access

Whenever a trusted server accesses an AUDIX mailbox, it uses an IMAPI session. IMAPI is the software that allows access to INTUITY AUDIX mailboxes. Depending on what INTUITY model you purchased, there can be up to 96 active sessions simultaneously, some of which you need to set for trusted server use.

⇒ NOTE:

IMAPI sessions cannot be reserved for use by ELA. The following procedure administers the maximum number of IMAPI sessions you will allow trusted servers to use simultaneously, but does not guarantee that an IMAPI session will be available. You should monitor ELA trusted server activity to see if trusted server requests for IMAPI sessions are frequently being denied because all sessions are in use (see your *INTUITY Messaging Solutions Release 4 Administration* book). If so, you may need to purchase more IMAPI sessions.

To set IMAPI sessions for trusted server use:

1. Starting from the main menu, select:

```
> AUDIX Administration
```

2. At the `enter command:` prompt, enter either:

Full Command Version

Short Command Version

change system-parameters imapi-options

ch sy i

The system displays the System-Parameters IMAPI-Options screen (Figure 3-8).

```

change system-parameters imapi-options                               Page 1 of 1
SYSTEM-PARAMETERS IMAPI-OPTIONS

NUMBER OF IMAPI SESSIONS

                                Total Sessions Purchased: 32

                                Maximum Simultaneous Sessions: 32
Simultaneous Sessions Available for Trusted Server Access: 6

IMAPI PARAMETERS

                                IMAPI Session Timeout (minutes): 5
Trusted Server Session Timeout (minutes): 5
                                Check New Messages? n
                                Deliver CA Message? n
                                Message Transfer? y

enter command: change system-parameters imapi-options

```

Figure 3-8. System-Parameters IMAPI-Options Screen, Page 1; Setting IMAPI Sessions for Trusted Server Access

⇒ NOTE:

The following contain instructions for the fields that directly relate to ELA. See your *INTUITY Messaging Solutions Release 4 Administration* book for complete field descriptions and to understand their implications.

3. In the `Maximum Simultaneous Sessions:` field enter 2 more than the current value. (For example, if the field currently reads 30, enter 32.)
This number includes sessions for users who are logged into their mailboxes using Message Manager or an e-mail application supported by INTUITY AUDIX R4, if applicable, and cannot exceed the value in the `Total Sessions Purchased` field.
4. In the `Simultaneous Sessions Available for Trusted Server Access:` field enter 2 more than the current value. (For example, if the field currently reads 2, enter 4.)
The maximum value for this field is 4 for MAP/40s and MAP/40 or 6 for MAP/100.
5. Enter **5** in the `IMAPI Session Timeout:` field.
6. Enter **5** in the `Trusted Server Session Timeout:` field.
7. Enter **y** in the `Message Transfer?` field.

8. Press (F3) **(ENTER)** to save this information to the system database.
The cursor returns to the command line, and the system displays the message `Command Successfully Completed`.
9. Continue with the next procedure or enter **exit** to leave AUDIX Administration.

Defining Two ELA Trusted Servers

The ELA software runs as two separate trusted servers. For the ELA servers to communicate with the INTUITY AUDIX server, they must be defined to the INTUITY AUDIX system. The installation worksheets you received from your account representative will have the exact names for the ELA trusted servers. However, for the purposes of this document, the first ELA trusted server will be referred to as the *administrative server* and the second ELA trusted server as the *delivery server*.

A request from ELA to send a message to an AUDIX mailbox involves invoking an IMAPI session and locking the ELA mailbox. A server that uses IMAPI to access an AUDIX mailbox is known as a trusted server.

SECURITY ALERT:

The procedures in this section include setting a password the trusted server must use to access AUDIX. There is a secondary layer of security (in addition to a trusted server password) that you can administer. This additional layer of security involves setting a separate IMAPI password that the trusted server must use before the system will allow an IMAPI session to be invoked.

*While administration of this additional password is optional, it is strongly recommended. See your *INTUITY Messaging Solutions Release 4 Administration* book.*

Before You Begin

Before adding the ELA trusted server to the system, you will need the following information:

- Two unique 1- to 10-printable character server names for the ELA trusted servers. These server names must be unique, not only from each other, but from all other machines in the network (including fax call delivery machines). Use the **li ma** and **li tr** commands to view all machines currently in your network.

Additionally, the server names must comply with the guidelines for naming machines your *INTUITY Messaging Solutions Release 4 Administration* book for complete information on naming conventions).

- The TCP/IP address for the AUDIX server (see page 3-23).

You will perform this procedure twice, first for the ELA administrative server, and then for the ELA delivery server. To add the ELA trusted servers to the INTUITY AUDIX server:

1. Starting from the main menu (Figure 3-1 on page 3-14), select:

```
> AUDIX Administration
```

2. At the `enter` command: prompt, enter either:

Full Command Version	Short Command Version
add trusted-server	ad tr

The system displays the Trusted-Server Profile screen (Figure 3-9).

(To see a list of existing trusted servers enter `li tr` at the command line.)

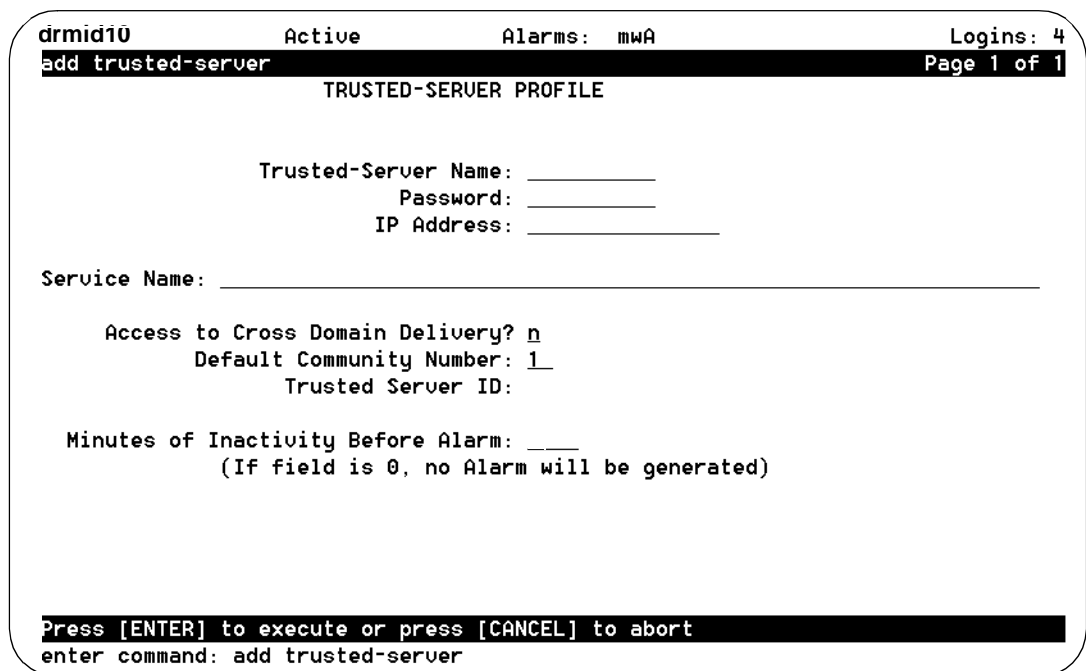


Figure 3-9. Trusted-Server Profile Screen; Defining a Trusted Server to the Lucent INTUITY System

3. In the **Trusted-Server Name:** field, enter a name for the first ELA trusted server. (See the Note below for tips on trusted server names.)

This name must be a unique 1- to 10-printable character entry. Additionally, this name cannot start with a number and cannot contain any embedded spaces, for example, denver 1 is not allowed, but denver_1 is allowed. (Use the **li tr** and **li ma** commands to view existing names and ensure that you are not using a name that is already assigned.)

⇒ NOTE:

You must administer two ELA trusted servers. The installation worksheets should have the ELA trusted server names. If not, we recommend that you use names that are descriptive enough that you can tell them apart, for example, enter the first ELA trusted server name as `ela_admin` and, when you add the second ELA trusted server, use `ela_deliv`.

4. Enter a 5- to 10-alphanumeric password that the trusted server must use to log on to the AUDIX server. As you type, your keystrokes display, but will appear as a series of asterisks (*) after you save.
5. Enter the TCP/IP address of this Lucent INTUITY in the form `w.x.y.z`, where each letter is a number, 0 to 255. (See page 3-23 for information how to determine your system's IP address.)

6. Enter **Enhanced-List Application** in the **Service Name:** field. Type exactly as listed, including the hyphen and capitalization.

Every ELA server will have the same service name. (For example, if you have two ELA servers, they will have separate trusted server names, but the same service name.)

7. Enter **n** in the **Cross-Domain Delivery?** field.
8. For the administrative ELA trusted server (`ela_admin`), enter **0** in the **Minutes of Inactivity Before Alarm:** field.

For the delivery ELA trusted server (`ela_deliv`), enter **255** in the **Minutes of Inactivity Before Alarm:** field

9. Press (F3) **ENTER** to save the information in the system database.

The cursor returns to the command line, and the system displays the message **Command Successfully Completed**.

10. You must now add the delivery ELA server. Return to step 2, and repeat this procedure, ensuring that you use a unique name for the delivery trusted server, that is, do not use the name of the ELA trusted server you just added.

11. Do you want to administer an IMAPI password?
 - If yes, follow the procedures for setting the IMAPI password in your *INTUITY Messaging Solutions Release 4 Administration* book before proceeding to the next section.
 - If no, go to Chapter 4 to Administer ELA, or enter **exit** to leave AUDIX Administration.

Overview

Now that the AUDIX system knows about the ELA trusted servers, you can do the initial administration of the ELA system. To make ELA fully functional, you must:

- Define the AUDIX server to ELA and administer access
- Create enhanced lists
- Add members to enhanced lists
- Record a name for the enhanced lists (optional)

Defining the AUDIX server and Administering Access

To allow communication between ELA and AUDIX, you must perform some initial ELA administration.

Before You Begin

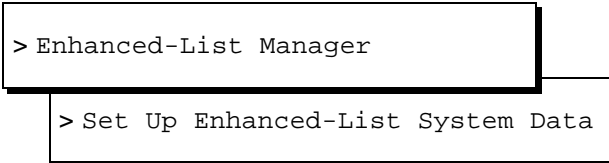
To administer the ELA server, you will need to know the:

- The sa or vm password
- IMAPI password (Optional, see your *INTUITY Messaging Solutions Release 4 Administration* book)
- ELA administrative trusted server name and password (see page 3-28)
- ELA delivery trusted server name and password (see page 3-28)
- A currently unused extension to use as the shadow mailbox

- Enhanced-list mailbox and shadow mailbox Community IDs (see page 3-20)
- ELA Class of Service (see page 3-16)

To administer the ELA server:

1. Starting from the main menu (Figure 3-1 on page 3-14), select:



The Set Up Enhanced-List System Data window displays (Figure 4-1).

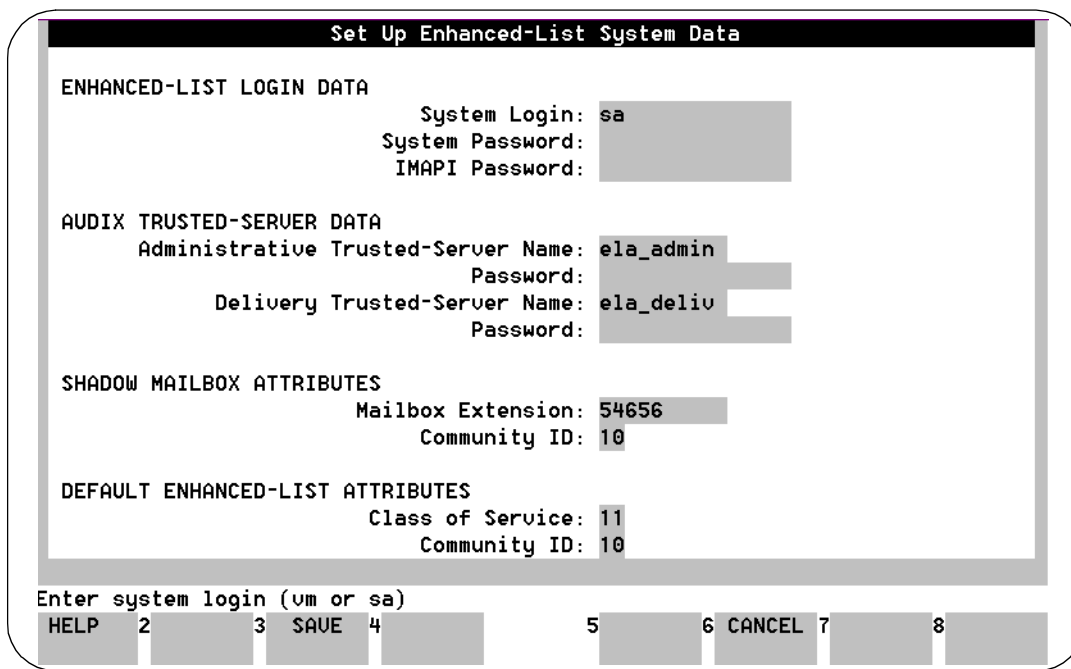


Figure 4-1. Set Up Enhanced-List System Data Window

2. Complete the fields in this window using the information in Table 4-1.

Table 4-1. Field Definitions: Set Up Enhanced-List System Data Window

Field Name	Description/Procedure
<p>System Login: <u>Valid Input:</u> sa, vm</p>	<p>Enter sa (system administrator login) or vm (voice mail administrator login).</p> <p>⇒ NOTE: Administrators using the vm login cannot administer enhanced lists or ELA trusted servers. This field allows ELA to log into AUDIX.</p>
<p>System Password: <u>Valid Input:</u> 6- to 8-alphanumeric characters</p>	<p>Enter your sa or vm administration password.</p> <p>The ELA server uses this password to perform AUDIX administration functions, such as adding or deleting an enhanced-list mailbox.</p>
<p>IMAPI Password: <u>Valid Input:</u> 0- to 8-alphanumeric characters</p>	<p>If you decided to require that trusted servers use an IMAPI password, enter the IMAPI password you administered in AUDIX.</p> <p>Some AUDIX functions do not require passwords.</p> <ul style="list-style-type: none"> ■ If a password is required, then the one you enter here must match that password exactly. ■ If a password is not required, you can delete any existing password as follows: <ol style="list-style-type: none"> 1. Open the Set Up Enhanced-List System Data window. 2. Enter some characters into the IMAPI Password: field. 3. Press (Backspace) until all the characters you entered have been deleted. 4. Press (F3) (SAVE) to save your changes.
<p>Administrative Trusted-Server Name: <u>Valid Input:</u> 1- to 10-alphanumeric characters</p>	<p>Enter the Administrative trusted server name that you administered in AUDIX.</p> <p>This name should be listed on the Installation Information worksheet. This field is case-sensitive, so capital letters must be typed as capitals, and lowercase letters as lowercase.</p> <p>This name cannot start with a number and cannot contain any embedded spaces, for example, denver 1 is not allowed, but denver_1 is allowed.</p> <p>⇒ NOTE: The ELA trusted server must be added in AUDIX before you can complete this procedure.</p>

Continued on next page

Table 4-1. Field Definitions: Set Up Enhanced-List System Data Window — Continued

Field Name	Description/Procedure
Password: <u>Valid Input:</u> 5- to 10-alphanumeric characters	Enter the Administrative trusted server password (see page 3-30).
Delivery Trusted-Server Name: <u>Valid Input:</u> 1- to 10-alphanumeric characters	Enter the name of the delivery trusted server that you administered in AUDIX. (This is the second ELA trusted server you added.) This name should be listed on the Installation Information worksheet. This field is case-sensitive, so capital letters must be typed as capitals, and lowercase letters as lowercase. This name cannot start with a number and cannot contain any embedded spaces, for example, denver 1 is not allowed, but denver_1 is allowed. ⇒ NOTE: The delivery trusted server must be added in AUDIX before you can complete this procedure.
Password: <u>Valid Input:</u> 1- to 15-alphanumeric characters	Enter the delivery trusted server password.
SHADOW MAILBOX ATTRIBUTES Mailbox Extension: <u>Valid Input:</u> 3- to 10-numeric characters	Enter the extension to be used for the shadow mailbox. ⚠ WARNING: <i>This mailbox must NOT currently exist in AUDIX and must not be translated on the switch.</i> When the system validates this form, ELA automatically creates a shadow mailbox.
SHADOW MAILBOX ATTRIBUTES Community ID: <u>Valid Input:</u> a number from 2 to 15	Enter the number of the community assigned to the shadow mailbox. This cannot be the same number as the enhanced-list mailbox Community ID. The shadow mailbox community must be administered to be able to send messages to all other communities, but to not be able to receive messages from any other community. See "Setting Up ELA and Shadow Mailbox Community IDs" on page 3-19.

Continued on next page

Table 4-1. Field Definitions: Set Up Enhanced-List System Data Window — Continued

Field Name	Description/Procedure
DEFAULT ENHANCED-LIST MAILBOX ATTRIBUTES Class of Service: <u>Valid Input:</u> a number from 2 to 11	Enter the number of the COS assigned to the enhanced-list mailbox and the shadow mailbox. ELA uses this COS number when you create new enhanced lists.
DEFAULT ENHANCED-LIST MAILBOX ATTRIBUTES Community ID: <u>Valid Input:</u> a number from 1 to 15	Enter the number of the community assigned to the enhanced-list mailbox. This cannot be the same number as the shadow mailbox Community ID. The enhanced-list mailbox community must be administered to be able to send messages to all other communities and receive messages from the community(ies) containing users with access to enhanced lists. See "Setting Up ELA and Shadow Mailbox Community IDs" on page 3-19.

3. Press (F3) **(SAVE)** to save the ELA server information to the system database.
 The system displays the message "Successfully Updated!" and asks you to press F1 acknowledge the message.
4. Press (F1) **(ACKNOWLG MESSAGE)**.
 The system redisplay the Enhanced List Manager menu.
5. Continue with the next procedure or press (F6) **(CANCEL)** repeatedly to return to the main menu.

Guidelines for Naming Enhanced Lists

We recommend that you use the following guidelines when you name an enhanced list. These guidelines can help prevent users from inadvertently sending their messages to the enhanced list, instead of to a person.

- Do not use embedded spaces in the name. If you would like a list to be called Marketing Department, type it **Marketing_Department_Llist**.
- Avoid naming an enhanced list after a person. INTUITY Message Manager does not differentiate between an enhanced list and a person's name.

Examples of names to avoid:

- Jane_Doe
- Doe_Jane

- Give enhanced lists names that reflect an organization or a function. Include the word *list*.

Examples:

- Marketing_Dept_List
- Maxfield_List
- Western_District_Salesforce_List

- If you want all enhanced lists to be grouped together, put the word *list* first.

Examples:

- List_Marketing_Dept
- List_Maxfield
- List_Western_District_Salesforce

- Begin the name with the number 1.

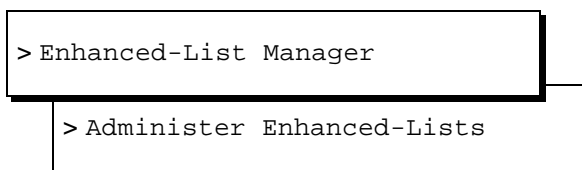
Example: 1_McDonnell_List

Users can reach the enhanced-list mailbox through Numbers Addressing as well as Names Addressing. Since there are no letters associated with keypad **1**, users will be less likely to inadvertently select the wrong address.

Creating Enhanced Lists

To create an enhanced list and add members:

1. Starting from the main menu (Figure 3-1 on page 3-14), select:



The system displays the Administer Enhanced-Lists window (Figure 4-2).

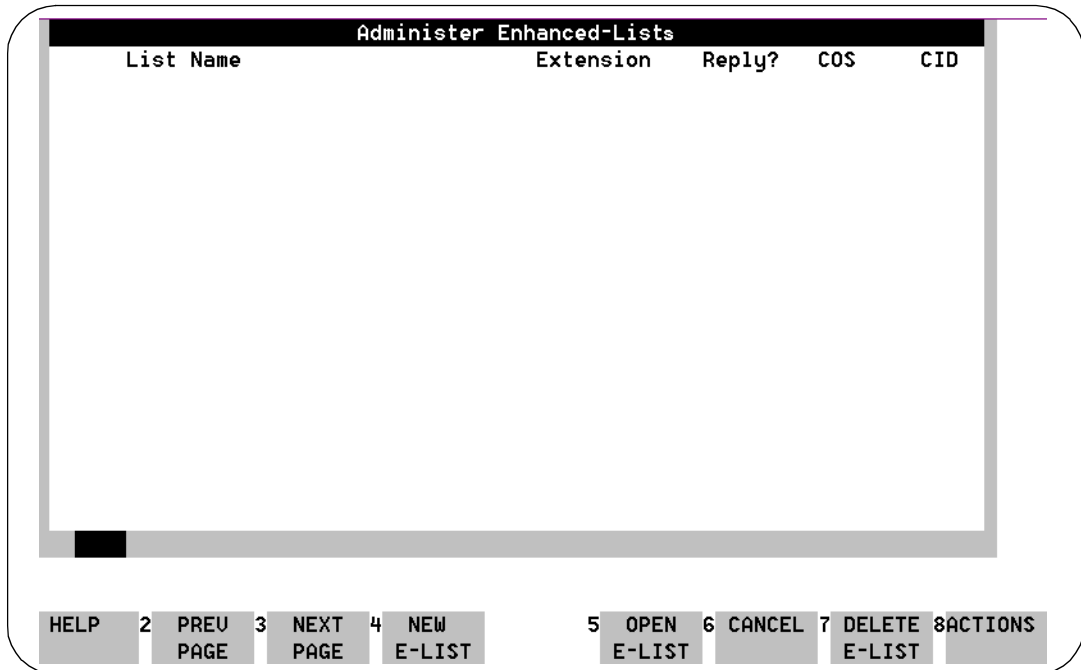


Figure 4-2. Administer Enhanced-Lists Window

2. Press (F4) **NEW E-LIST**.

The system displays the New Enhanced-List window (Figure 4-3).

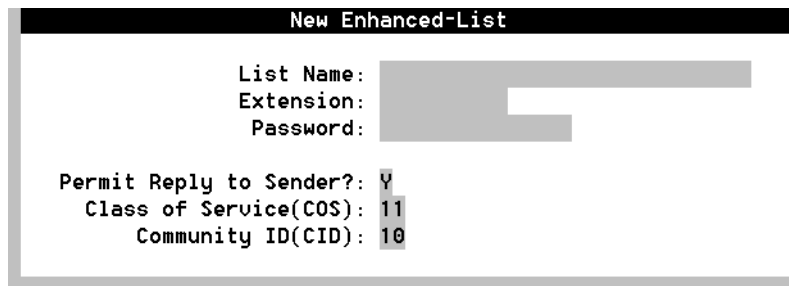


Figure 4-3. New Enhanced-List Window

3. Complete the fields in this window using the information in Table 4-2.

Table 4-2. Field Definitions: New Enhanced List Window

Field Name	Description/Procedure
List Name: <u>Valid Input:</u> 1- to 29-alphanumeric characters	Enter a name for the list. Use the "Guidelines for Naming Enhanced Lists" on page 4-37.
Extension: <u>Valid Input:</u> a 3- to 10-numeric characters	Enter the local extension for the list mailbox. This extension must comply with your system dial plan. ELA creates a mailbox at this extension automatically, if one does not already exist. Be sure that those users administered to have access to the list mailbox know this extension.
Password: <u>Valid Input:</u> 5- to 15-numeric characters	Enter the password for this list mailbox. This password is for administrative purposes only. Users who send messages to the ELA mailbox for distribution do not use a password.
Permit Reply to Sender?: <u>Valid Input:</u> y = yes (default) n = no	No entry is required if you want to allow a recipient of a message that is sent to an enhanced list to reply to the originator of the message. To reply, both the recipient and the enhanced list must be on an INTUITY AUDIX R4.1 or higher. Enter n (o) if you would not like recipients to reply to an ELA-delivered message.
Class of Service: <u>Valid Input:</u> a number from 2 to 11	No entry is required. The default value in this field is the ELA COS number you administered on the Set Up Enhanced-Lists System Data window (see page 4-35).
Community ID: <u>Valid Input:</u> a number from 1 to 15	No entry is required. The default value in this field is the ELA Community ID you administered on the Set Up Enhanced-Lists System Data window (see page 4-35).

4. Press (F3) **SAVE** to save this information in the system database.

The cursor displays in the Administer Enhanced Lists window on the line that shows the list you just entered. (If you have more than one list, the new list is placed in line alphabetically with the other lists).

Guidelines for Selecting Enhanced-List Members

The following subscribers can be members of an enhanced list:

- Local and remote subscribers. These members can be other enhanced lists.
- Call delivery numbers, including fax machines
- E-mail subscribers who are serviced by other trusted servers, including Lotus Integrated Messaging
- AMIS pre-administered subscribers

The following cannot be members of an enhanced list:

- Public or private subscriber-owned lists
- AMIS-casual addresses
- Broadcast mailboxes

Adding Members to Enhanced Lists

To add member names, extensions, and network (e-mail) addresses to a new enhanced list, perform the following tasks. Start on the Administer Enhanced Lists window.

1. Press (F5) **OPEN E-LIST**.

The system displays the Enhanced-List Membership for Listname (listextension) window (Figure 4-4).

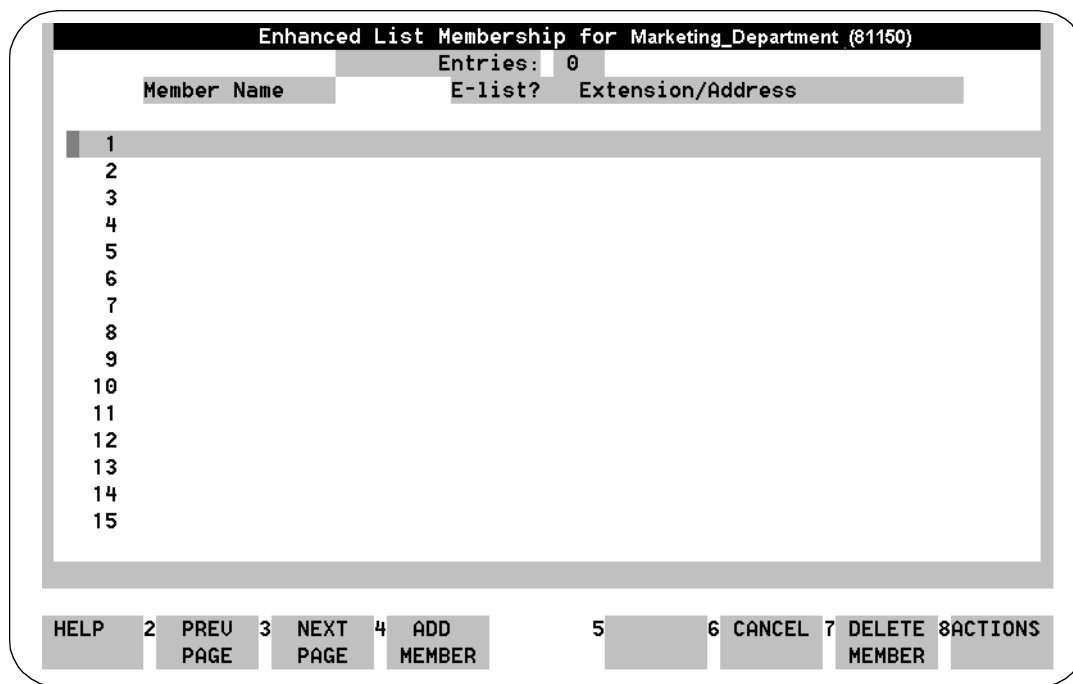


Figure 4-4. Enhanced List Membership for *Listname* Window

2. Press (F4) **ADD MEMBER**.

The system displays the Add Member data entry window (Figure 4-5).

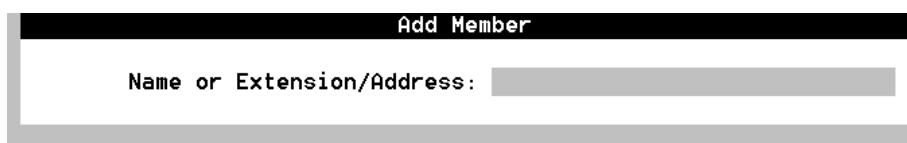


Figure 4-5. Add Member Window; Adding Members to an Enhanced List

3. Enter one of the following:
 - The user's name as it appears in the AUDIX system. This name can be another enhanced list.
 - The user's extension. This extension can be the extension for another enhanced list.
 - The user's network (e-mail) address in the format dictated by the e-mail system, for example, `username@trusted_servername`

4. Press (F3) **SAVE** to save this information in the system database.

⇒ NOTE:

The **Entries:** field at the top of the Administer Enhanced-Lists window increments each time you add a new member to the list.

5. Repeat Step 3 and Step 4 to continue adding member names, extensions, and e-mail addresses.

⇒ NOTE:

We recommend that you print a copy of the completed list to your system printer, if available. You can use this printout to search multiple lists for duplicate names or potential loops with a synchronized e-mail system. Additionally, should you inadvertently delete an enhanced list, you would have a source from which to recreate the enhanced list. (The system's nightly data backup also saves ELA setup data, lists, and memberships.)

6. Review the Administer Enhanced-Lists window. If you want to change or delete any information you just entered:
 - a. Press **CANCEL**.
The Enhanced List Membership window displays.
 - b. Select the member name you want to change or delete.
 - c. Press **DELETE MEMBER** (F7).
 - d. Go to Step 2 to re-enter member information, or go to Step 7 to continue.
7. When you have finished adding member names to this enhanced list, press (F6) **CANCEL** repeatedly to return to the main menu.

Adding/Deleting Members to an Enhanced List

To change data for a member of an enhanced list, such as the name or telephone extension, make the change in AUDIX as described under your *INTUITY Messaging Solutions Release 4 Administration* book. The change is automatically reflected in all enhanced lists that contain that member.

To add or delete the members of an existing enhanced list:

1. Starting from the main menu (Figure 3-1 on page 3-14), select:

```
> Enhanced-List Manager
```

```
> Administer Enhanced-Lists
```

The system displays the Administer Enhanced-Lists window (Figure 4-2). The names of your enhanced lists display in the window (along with other descriptive data).

2. Using the arrow keys, select the list you would like to add members to. If the list is not on the visible page, select the list by one of the following means:
 - Press **(NEXTPAGE)** until the desired list displays. Use the arrow keys to highlight the list you would like to edit.
 - Press **(F8) (ACTIONS)**. An **Actions** menu displays. Select **Find List** and press **(ENTER)**. Enter the name or extension of the list you would like to add or change and press **(F3) (FIND)**. The Administer Enhanced-Lists window will re-display with the specified list highlighted.
3. Press **(F5) (OPEN E-LIST)**.

The system displays the Enhanced-List Membership for Listname (listextension) window (Figure 4-6). The member names of the selected list display in the window. Accompanying each name is an extension number or network (e-mail) address and other descriptive data.

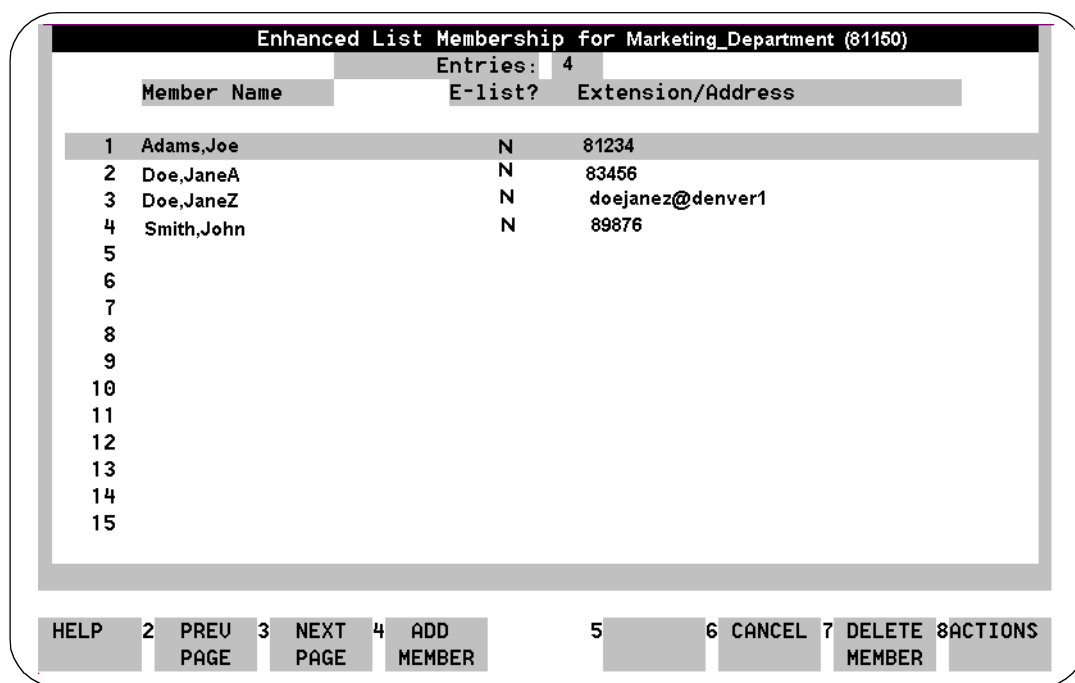


Figure 4-6. Enhanced-List Membership for Listname (listextension) Window

At this point you can:

- Add new members to the list (Step 4)
- Find a member of a list (Step 5)

- Delete a member from the list (Step 6)
- Print the list to your system printer (Step 7)

Adding a Member

4. Press (F4) **ADD MEMBER**.

The system displays the Add Member data entry window (Figure 4-5 on page 4-42).

- a. Enter one of the following:
 - The user's name as it appears in the AUDIX system
 - The user's extension
 - The user's network (e-mail) address in the format dictated by the e-mail system, for example, `username@trusted-servername`
- b. Press (F3) **SAVE** to save this information in the system database.
- c. Continue entering names/extensions/e-mail addresses until all new members have been added.
- d. Press (F6) **CANCEL** to return to the Administer Enhanced List window or proceed to Step 7 to print a copy of the list.

Finding a Member

5. To find a member name in a list:

- a. Press (F8) **ACTIONS**.

An **Actions** menu displays.

- b. Select **Find Member** and press **ENTER**.

- c. Enter the name or extension of the person or list you would like to find and press (F3) **FIND**.

The Enhanced-Lists Membership window re-displays with the specified person or list highlighted.

Deleting a Member

6. To delete a member:
 - a. Locate the member name to be deleted. See "Finding a Member" above.
 - b. Press (F7) **DELETE MEMBER**.
The system displays the confirmation message:

```
CONFIRM: Deleting
Name= List - Listname
Extension/Address= Listextension
Enter y to continue, n to abort.
```
 - c. Enter **y**
The Enhanced-List Membership window redisplay.
 - d. Continue with Step 7 to print a copy of the list.

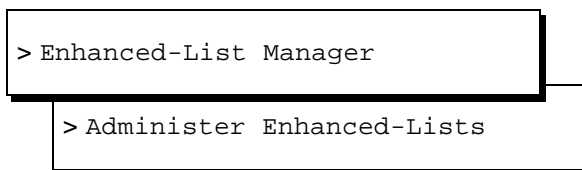
Printing an Enhanced List

7. Press (F8) **ACTIONS**. An Actions menu displays.
 - a. Select **Print List Membership** and press **ENTER**.
The system displays the message "Printing List Membership for Listname (listextension)" and sends the list to the system printer.
 - b. Press (F1) **ACKNOWLG MESSAGE**.
The system redisplay the Actions menu.
 - c. Proceed to Step 8.
8. When you have finished, press (F6) **CANCEL** repeatedly to return to the main menu.

Deleting an Enhanced List

To delete an existing enhanced list:

1. From the main menu, select:



The system displays the Administer Enhanced-Lists window (Figure 4-2 on page 4-39).

2. Use the arrow keys to highlight the line that represents the list you want to delete. If the list to be deleted does not appear on the visible page, select the list by one of the following means.
 - Press **(NEXTPAGE)** until the desired list displays. Use the arrow keys to highlight the list you would like to delete.
 - Select **(F8) (ACTIONS)**. An **ACTIONS** menu displays. Select **Find List** and press **(ENTER)**. Then enter the name or telephone extension of the list you would like to delete and press **(F3) (FIND)**. The Administer Enhanced-Lists window will re-display with the specified list highlighted.
3. Press **(F7) (DELETE E-LIST)**.

The system displays the Confirm Deletion of Enhanced-List window (Figure 4-7).

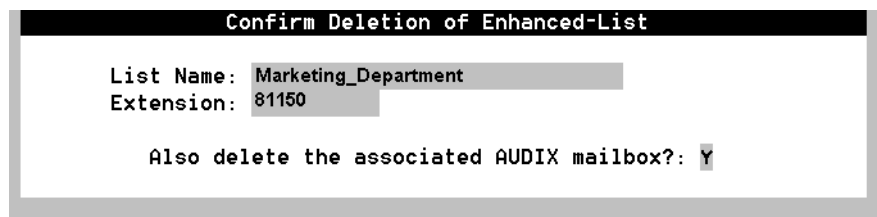


Figure 4-7. Confirm Deletion of Enhanced-List Window

4. Do you want to delete the associated AUDIX mailbox?
 - If yes, go to Step 5.
 - If no, enter **n**. To create a new enhanced list, see page 4-37.
5. Press **(F3) (DELETE)** to delete the enhanced list.

AUDIX deletes the mailbox and all information in it, including any enhanced-list members or messages.

The system displays the message "Deleted *Listname* (*Listextension*) Enhanced List" and asks you to press **F1** acknowledge the message.
6. Press **(F1) (ACKNOWLG MESSAGE)**.

The system redisplay the Administer Enhanced-Lists window.
7. Press **(F6) (CANCEL)** repeatedly to return to the main menu.


Recording Names for Enhanced Lists

Once you have established an enhanced list, it is a good idea to record a name for the list. That way, users will hear a meaningful name for the list when they send a message to an enhanced-list mailbox for distribution. However, you need to record the name using an administrative recording session.

To record a name for an enhanced list:

1. From a touch-tone telephone, log in as an administrator.
2. Press **9**.

The system prompts with "To record names, press 4."

 **NOTE:**

If you get an error message, open the Class of Service screen for the administrator's extension and change the **Announcement Control** field to **y**. Then start again.

3. Press **4**.

The system prompts with "Please enter the extension and pound sign."

4. Enter the extension for the enhanced-list mailbox.

The system prompts with "When finished recording, press pound to approve or 1 to edit your message. Record at the tone."

5. After the tone, speak the name of the list.
6. Press **#**.
7. Repeat Steps 4 through 6 to record additional names.
8. Press ***r** to return to the main menu.

 **CAUTION:**

You should also record a name for the Shadow mailbox, using the same procedure. Use a name such as, "Mailing list - Do not reply." That way, anyone who inadvertently enters the Shadow mailbox extension, will not try to send a message to it or to reply to a message from it.

Testing INTUITY Enhanced Lists

1. Perform the administration outlined below, including:
 - "Installing the Software" on page 2-9
 - "Activating ELA" on page 3-14
 - "Increasing the Number of Mailing Lists Allowed on the System" on page 3-15

- "Defining an ELA Class of Service" on page 3-16
 - "Setting Up ELA and Shadow Mailbox Community IDs" on page 3-19
 - "Administering TCP/IP" on page 3-23
 - "Setting Up IMAPI Sessions for Trusted Server Access" on page 3-26
 - "Defining Two ELA Trusted Servers" on page 3-28 (You must have two available, unused extensions, one for the shadow mailbox and one for the enhanced-list mailbox)
2. Using the procedures in the Installation manual specific to your platform, set up two test users and test telephones.
 3. Using the procedures in the Installation manual specific to your platform, use the test-1 telephone to create and send a voice mail message to the ELA mailbox. Record the following or a similar test message and then enter the address for the enhanced-list mailbox:

"This is a test ELA message for INTUITY AUDIX."
 4. Hang up the test-1 telephone to disconnect.
 5. Verify that the MWIs for the test users' telephones activate and that the test users received the message. (See the Installation manual specific to your platform.)
 6. Delete the test messages. (See the Installation manual specific to your platform.)
 7. Delete the test users. (See the Installation manual specific to your platform.)

Preventative Maintenance and Troubleshooting

5

Overview

This section describes how to check for system alarms relating to ELA and how to diagnose common application and end-user problems.

Checking the Administrator's Log

The system warns you of potential administrative problems with ELA by displaying a minor and warning message (`Alarms: w` or `Alarms: m`) on the AUDIX Administration status line when it logs an administration event. Check the status line (at the top of the AUDIX Administration screen) at least once a day.

Other events besides those generated by ELA create administrative log entries, but you can view ELA-specific events. You should do this on a regular basis to monitor ELA performance. To view ELA-specific log entries:

1. Starting from the main menu, select:

```
> AUDIX Administration
```

2. At the `enter command:` prompt, enter either:

Full Command Version

display administrators-log

Short Command Version

di ad

The system displays the Administrator's Log screen.

3. Enter the starting date and time.
4. Enter **EL** in the `Application:` field.

5. Press (F3) **SAVE** to display the alarm entries.
6. Examine the displayed entries. See the *Lucent INTUITY™ Messaging Solutions Release 4 Alarm and Log Messages*, 585-310-566 for a list of events and alarms, and associated repair procedures.
7. Take whatever corrective action is necessary.
8. Enter **exit** at the `enter command:` prompt to exit AUDIX administration.

Checking the Delivery Failure Log

The delivery failure log contains entries for all failed deliveries, along with descriptive data regarding cause for the failure and other information. Check this log to monitor ELA and system performance and if a user complains that messages are not being delivered.

To view the delivery failure log:

1. Starting from the main menu, select:

```
> Enhanced List Manager
>View E-List Delivery Failure Log
```

The system displays the Delivery Failure Log window (Figure 5-1).

Enhanced-List Delivery Failure Log				
Date	Time	Message Originator	Parent List	Child List
Failed Recipient		Failed Address		Failure Reason
07/17/96	09:18:21	82736@draudix	898278@drveitt	87253
Joe1,Joe			85589@draudix	Recipient Mailbox Full
08/17/96	14:52:10	82736@draudix	898278@drveitt	87253
Joe1,Joe			84804@cbaudix	Remote System not Fax Enabled

Figure 5-1. Delivery Failure Log Window

Table 5-1 explains the log entries in the report.

Table 5-1. Field Definitions: Enhanced-List Delivery Failure Log Window

Field Name	Description/Procedure
Date	The calendar date the delivery failure occurred
Time	The time that delivery failure occurred
Message Originator	The address of the user who sent the message to the enhanced list for distribution The address is in the format address@machine where <i>address</i> can be the telephone extension or the network (e-mail) address. The system truncates addresses that are longer than 21 characters.
Parent List	The list (mailbox) to which a user originally addressed the message
Child List	The last list mailbox a message reached prior to message delivery failure
Failed Recipient	The name of the recipient to which AUDIX attempted to send the ELA message. If no name is administered, this field is blank.
Failed Address	The address to which AUDIX attempted to send the ELA message The address is in the format address@machine where <i>address</i> can be the telephone extension or the network (e-mail) address. The system truncates addresses that are longer than 21 characters.
Failure Reason	This is descriptive text indicating the reason the delivery failure occurred, such as <code>Full Mailbox</code> , <code>Unsupported Media</code> , or <code>Transmission Problems</code> .

2. Press (F8) **PRINT** to send a copy of this report to the system printer, if you have a printer available.
3. Press (F6) repeatedly to return to the main menu.

Delivery Failure Codes

Delivery failure logs contain the following codes:

Table 5-2. Delivery Failure Codes

Reason of Failure	Description
Full mailbox	The recipient has a full mailbox.
Could not locate	ELA could not locate the recipient.
Transmission probs	Transmission difficulties occurred.
Permission denied	The message contains features ELA can not recognize. Permission is denied.
Sending restriction	Delivery denied because of sending restrictions
Login annc exists	The login announcement already exists.
AMIS wrong number	This is the wrong number for this AMIS analog recipient.
Too many AMIS xmits	Too many transmission attempts for AMIS analog resulted in a transmit-attempt exception.
AMIS unknown return	AMIS returned the message without identifying a reason.
misc internal fail	Miscellaneous internal delivery failure
AMIS longer > 8 minutes	The AMIS message is longer than eight minutes.
Unsupported media	The message contains media that ELA does not support for this particular system or subscriber.
Pvt to unsup remote	Private messages were not delivered to unsupported remote systems.
Message too large	The voice component of the message is too large for the remote system.

Troubleshooting ELA

Table 5-3 lists questions users ask the system administrator and suggested remedies to commonly encountered system problems.

Table 5-3. User Questions or System Functionality Symptoms

Question/Symptom	Possible Cause	Answer/Suggested Remedy
During an upgrade failure, installer/administrator cannot differentiate between AUDIX mailboxes and ELA mailboxes.		Use the li cos command from AUDIX Administration to determine the ELA Class(es) of Service. Use the li su command and note the extension(s) of all mailboxes with the applicable COS.
"I try to reply to a message I got, but I get a system message that I can't."	Message was sent to an enhanced list that did not permit "Reply to Sender."	<ul style="list-style-type: none"> ■ Administer the enhanced list to allow Reply to Sender, if appropriate. ■ Educate your users about ELA functionality.
	Community IDs for the user or recipient incorrectly administered	Administer Community IDs for user or recipient, if appropriate.
	Recipient is not on a Lucent INTUITY system or is on a pre-R4 system.	Upgrade system to Lucent INTUITY R4.2_4 or higher.
"I am getting multiple copies of the same message."	Recipient is on more than one list.	<ul style="list-style-type: none"> ■ ELA does not check nested lists to see if the same name appears in more than one place. Print out a copy of your enhanced lists and remove duplicates, if possible. ■ Educate your users about ELA functionality.
You inadvertently delete the shadow mailbox.		<p>ELA raises a warning alarm. Any messages waiting in the delivery "queue" is lost.</p> <p>Re-enter the shadow extension on the Set Up Enhanced-List System Data window and then press (F3) SAVE.</p>


Continued on next page

Table 5-3. User Questions or System Functionality Symptoms — Continued

Question/Symptom	Possible Cause	Answer/Suggested Remedy
Recipient claims s/he did not get an ELA message.	<ul style="list-style-type: none"> ■ Mailing list not current 	Check the mailing list for the recipient's name. Administer, if necessary.
	<ul style="list-style-type: none"> ■ Subscriber's mailbox not administered correctly 	<ul style="list-style-type: none"> ■ Check the Subscriber screen for the affected user. Look at the Mailbox size. Put user in a COS with a larger mailbox, if necessary. ■ Check the List Measurements Subscriber Day screen for the affected user. Look at the available mailbox space. Advise the user to delete unneeded messages and greetings, if appropriate. ■ Check that Community ID is correct.
	<ul style="list-style-type: none"> ■ System delivery failure 	<p>System delivery failures can arise from many sources.</p> <ul style="list-style-type: none"> ■ Check the Delivery Failure Log (see "Checking the Delivery Failure Log" on page 5-52). ■ Check the Administrator's Log for related alarms. If an alarm warrants further action, see <i>Lucent INTUITY Messaging Solutions Release 4 Alarm and Log Messages</i>, 585-310-566. ■ Verify network capabilities with your PC/LAN administrator.
	<ul style="list-style-type: none"> ■ Sending Restrictions not consistent across machines 	Administer Community IDs for all Lucent INTUITY machines, if appropriate.
An enhanced-list member keeps disappearing from Enhanced Lists.	System feature to delete non-administered remote users is active.	<ul style="list-style-type: none"> ■ From AUDIX Administration, enter ch sys fe. Access page 4 and change the Even if on Mailing List? field to n. ■ Re-administer the remote user.
"I can't send a message to an enhanced-list mailbox."	User belongs to a community with sending restrictions administered.	Consider whether to change this user's community ID to allow her/him to use Enhanced Lists.

Continued on next page

Table 5-3. User Questions or System Functionality Symptoms — Continued

Question/Symptom	Possible Cause	Answer/Suggested Remedy
<p>"Everyone else seemed to have received their enhanced-list message. I got mine much later."</p>	<p>User mailbox full</p>	<p>Check the List Measurements Subscriber Day screen for the affected user. Look at the available mailbox space. Advise the user to delete unneeded messages and greetings, if appropriate or consider putting the user in a COS with a larger mailbox.</p>
	<p>Enhanced list was very large.</p>	<p>Remember that ELA 'throttles' traffic during periods of heavy user traffic. Inform user that it message delivery to a large recipient population does take time.</p>
	<p>Networking problems between originator system and recipient system.</p>	<p>Perform networking troubleshooting. See <i>Lucent INTUITY Messaging Solutions Digital Networking</i>, 585-310-567 for more information.</p>
<p>You inadvertently delete an Enhanced List.</p>		<p>There are 2 ways to restore an Enhanced List:</p> <ul style="list-style-type: none"> ■ Re-enter the names on the list. ■ Restore the data from the previous night's tape backup. <p> WARNING:</p> <p><i>There is no way to selectively restore only enhanced lists from the backup tape. Your system will lose all incremental administration data from the point of backup. Use this method only if you are sure the business can tolerate the loss of recent administration.</i></p>

Alarms

6

Overview

The following alarms are associated with the Enhanced-List Application.

DELIVTS Resource Type

Alarm Code: 1

Event ID: ELA-delivts01

Alarm Level: Warning

Description: Trusted-server data lost, re-enter or restore.

Repair Action:

There are two recovery methods:

- Access the Set Up Enhanced-List System Data window and re-enter all field information.
- Restore data from the most recent backup of system data. See Chapter 3, "Common System Procedures," in your maintenance book for instructions about restoring data. If you would prefer to have assistance with this restore, contact your remote maintenance center.

Alarm Code: 2

Event ID: ELA-delivts02

Alarm Level: Warning

Description: Trusted-server data partially lost, re-enter or restore.

Repair Action:

There are two recovery methods:

- Access the Set Up Enhanced-List System Data window and re-enter all field information.
- Restore data from the most recent backup of system data. See Chapter 3, "Common System Procedures," in your maintenance book for instructions about restoring data. If you would prefer to have assistance with this restore, contact your remote maintenance center.

Alarm Code: 3

Event ID: ELA-delivts03

Alarm Level: Warning

Description: Trusted-server data corrupt, re-enter or restore.

Repair Action:

There are two recovery methods:

- Access the Set Up Enhanced-List System Data window and re-enter all field information.
- Restore data from the most recent backup of system data. See Chapter 3, "Common System Procedures," in your maintenance book for instructions about restoring data. If you would prefer to have assistance with this restore, contact your remote maintenance center.

Alarm Code: 4

Event ID: ELA-delivts04

Alarm Level: Warning

Description: Trusted-server data no longer valid.

Repair Action:

1. In AUDIX, enter **ch tr** *administrative_trusted_server_name*.

2. Verify/administer the screen information, as required.
3. Repeat for the delivery trusted server.
4. Enter **ch imapi** and verify/administer as required.
5. When complete, enter the correct information in the Set Up Enhanced-List System Data window.

REGISTRY Resource Type

Alarm Code: 1

Event ID: ELA-registry01

Alarm Level: Warning

Description: E-list registry lost, re-enter or restore. The ELA software has detected that registry database has disappeared.

Repair Action:

1. Re-administer the registry:
 - a. Go to the Administer Enhanced-Lists window.
 - b. Use (F4) NEW E-LIST to re-enter the name of each Enhanced List, one at a time. (The individual members do not need to be re-entered.)

See Lucent INTUITY™ Messaging Solutions Release 4 Administration, 585-310-564 for more detailed procedures.
2. If the alarm persists, restore system data from the nightly backup. See Chapter 3, "Common System Procedures," in your maintenance book for instructions about restoring data. If you would prefer to have assistance with this restore, contact your remote maintenance center.

Alarm Code: 2

Event ID: ELA-registry02

Alarm Level: Minor

Description: Unable to write updated E-list registry.

Repair Action:

This alarm requires intervention from the remote maintenance center.

SHADOW Resource Type

Alarm Code: 1

Event ID: ELA-shadow01

Alarm Level: Warning

Description: Shadow mailbox data lost, re-enter or restore.

Repair Action:

There are two recovery methods:

- Access the Set Up Enhanced-List System Data window and re-enter the shadow mailbox extension and community ID. If a shadow mailbox exists at the extension entered, the system displays a system prompt to that effect. If a shadow mailbox does not exist at the extension entered, a new mailbox will be created.
- Restore data from the most recent backup of system data. See Chapter 3, "Common System Procedures," in your maintenance book for instructions about restoring data. If you would prefer to have assistance with this restore, contact your remote maintenance center.

Alarm Code: 2

Event ID: ELA-shadow02

Alarm Level: Warning

Description: Shadow mailbox corrupt, re-enter or restore.

Repair Action:

There are two recovery methods:

- Access the Set Up Enhanced-List System Data window and re-enter the shadow mailbox extension and community ID. If a shadow mailbox exists at the extension entered, the system displays a system prompt to that effect. If a shadow mailbox does not exist at the extension entered, a new mailbox will be created.
- Restore data from the most recent backup of system data. See Chapter 3, "Common System Procedures," in your maintenance book for instructions about restoring data. If you would prefer to have assistance with this restore, contact your remote maintenance center.

Alarm Code: 3

Event ID: ELA-shadow03

Alarm Level: Warning

Description: Shadow mailbox data corrupt, re-enter or restore.

Repair Action:

There are two recovery methods:

- Access the Set Up Enhanced-List System Data window and re-enter the shadow mailbox extension and community ID. If a shadow mailbox exists at the extension entered, the system displays a system prompt to that effect. If a shadow mailbox does not exist at the extension entered, a new mailbox will be created.
- Restore data from the most recent backup of system data. See Chapter 3, "Common System Procedures," in your maintenance book for instructions about restoring data. If you would prefer to have assistance with this restore, contact your remote maintenance center.

Alarm Code: 4

Event ID: ELA-shadow04

Alarm Level: Warning

Description: Shadow mailbox does not allow trusted-server access.

Repair Action:

1. In AUDIX, enter **ch cos ELA_Class_of_Service_Name/Number**
2. Verify that the `Trusted Server Access?` field is set to **y**
3. Enter **di sub shadow_mailbox_extension**
4. Verify the `Class of Service` field is the appropriate cos. If it is, call 1-800-56 AUDIX for help.

Alarm Code: 5

Event ID: ELA-shadow05

Alarm Level: Warning

Description: Shadow mailbox does not exist at expected extension.

Repair Action:

Access the Set Up Enhanced-List System Data window and re-enter the shadow mailbox extension and community ID. If a shadow mailbox exists at the extension entered, the system displays a system prompt to that effect. If a shadow mailbox does not exist at the extension entered, a new mailbox will be created.

⇒ NOTE:

If you wish to move the shadow mailbox to a new extension, only use the Set Up Enhanced-List System Data window.

Alarm Code: 6

Event ID: ELA-shadow06

Alarm Level: Warning

Description: The shadow mailbox is full of messages for recipients who have full mailboxes. ELA cannot deliver these messages until the recipients make space in their mailboxes. Also, AUDIX can take up to two weeks to determine that a message is undeliverable and to generate a log entry for a delivery failure.

Repair Action:

You can correct single instances of this problem by deleting messages from the shadow mailbox. To access the shadow mailbox:

1. In AUDIX Administration enter **ch su extension** for the enhanced-list mailbox.
2. At the Subscriber screen, enter a new password in the **Password:** field. Remember this password for step 5 below.
3. Press (F3) **(ENTER)** to save the password.
4. At the **enter command:** enter **exit**
5. Use Message Manager to log into the shadow mailbox.
6. Open the Outgoing folder and delete messages that have been rescheduled for delivery to full mailboxes. Keep deleting messages until the shadow mailbox is less than 50 percent full.

We recommend that you make a list of the recipients whose mailboxes are full, so you can ask them to delete at least half of their messages. (You cannot use AUDIX to make this request, because it cannot deliver messages until the mailboxes have more room.)

7. Log out of the shadow mailbox.

If you regularly get this alarm, the following questions can help you evaluate how your business uses ELA:

- Do your subscribers use large enhanced lists too frequently? Are they being used for trivial or non-business purposes?
- Are subscriber mailboxes too small? Should you increase mailbox space or purchase more hours for storage?
- Is the ELA class-of-service correct? (Check the value in the `Mailbox Size (seconds), Maximum:` field on the Class of Service screen, Page 2. Is the ELA class-of-service assigned to the shadow mailbox?)
- Are the intervals for rescheduling delivery on the System Parameters Features screen appropriate?

EL — Enhanced-List Application

The following administrator's log messages and repair actions apply to the Enhanced-List Application.

Event ID: ELA-badreca01 through ELA-badreca12

Description: Bad record deleted from E-List registry. Check for missing lists. (extension)

ELA detected a corrupt record and took the following action:

- If the message displays an extension, ELA deleted its record.
- If the message does not display an extension, ELA could not determine the extension of the corrupt record and deletes the record.

Repair Procedure:

There are two recovery methods:

- Go to the Administer Enhanced-Lists window and note any lists that may be missing.

Use (F4) NEW E-LIST to re-enter each missing Enhanced List, one at a time. If ELA reports that an AUDIX mailbox already exists for a given extension, and the reported data match those of the missing list, answer 'y' to confirm the change of the existing mailbox into an enhanced-list mailbox.

- Restore data from the most recent backup of system data. See Chapter 3, "Common System Procedures," in your maintenance book for instructions about restoring data. If you would prefer to have assistance with this restore, contact your remote maintenance center.

Event ID: ELA-lostlock01 through ELA-lostlock10

Description: Messages to an enhanced list could not be delivered because someone was logged into the shadow mailbox.

Repair Procedure:

No one should ever be logged into the shadow mailbox. However, if someone is, change the password for the shadow mailbox as follows:

1. In AUDIX Administration enter **ch su extension** for the enhanced-list mailbox.
2. At the Subscriber screen, enter a new password in the **Password:** field.
3. Press (F3) **ENTER** to save the password.

Event ID: ELA-no_members

Description: ELA received a message for delivery to an Enhanced List, but the enhanced list did not contain any members. In such a case, ELA will delete the message.

Repair Procedure:

Perhaps you forgot to add the members to the Enhanced List, or perhaps the enhanced list is no longer necessary. Go to the Administer Enhanced-Lists window and do one of the following:

- Highlight the list and use (F5) OPEN E-LIST to enter members into the Enhanced List.
- Use (F7) DELETE E-LIST to delete the Enhanced Lists.

See *Lucent INTUITY Messaging Solutions Release 4 Administration*, 585-310-564 for more detailed procedures.

Event ID: ELA-nestvioltn

Description: An enhanced list contains more than 20 nested lists.

For example, enhanced list 1 contains enhanced list 2 as one of its members. Inside enhanced list 2 is Enhanced List 3. Enhanced list 3 contains yet another enhanced list as one of its members, and so on.

Repair Procedure:

Evaluate list membership hierarchy and delete unnecessary nesting so that ELA can handle delivery of the message. See *Lucent INTUITY Messaging Solutions Release 4 Administration*, 585-310-564 for procedures.

Event ID: ELA-loopvioltn

Description: There are two enhanced lists that refer to each other. For example, enhanced list 1 contains enhanced list 2 as a member, and enhanced list 2 contains enhanced list 1 as a member.

Repair Procedure:

Go to the Administer Enhanced-Lists window.

1. Use (F5) OPEN E-LIST to open one of the indicated Enhanced Lists.
2. Search for the extension of the other Enhanced List.
3. Use (F7) DELETE E-LIST to delete the Enhanced List.

See *Lucent INTUITY Messaging Solutions Release 4 Administration*, 585-310-564 for more detailed procedures.

Event ID: ELA-mboxlock01

Description: An enhanced-list mailbox does not have trusted server access.

Repair Procedure:

1. In AUDIX, enter **ch cos *ELA_Class_of_Service_Name/Number***
2. Verify that the `Trusted Server Access?` field is set to **y**
3. Enter **ch su *Enhanced_List_mailbox_extension***
4. Verify the `Class of Service` field is the appropriate `cos`.

See *Lucent INTUITY Messaging Solutions Release 4 Administration*, 585-310-564 for more detailed procedures.

Event ID: ELA-chkrestrict

Description: A message was found in the shadow mailbox.

Repair Procedure:

1. In AUDIX, enter **ch sys se**

2. Verify that the shadow mailbox belongs to a community that cannot receive messages.



NOTE:

The sending restrictions must be identical on all machines in the INTUITY AUDIX network. Check the sending restrictions on all machines.

See *Lucent INTUITY Messaging Solutions Release 4 Administration*, 585-310-564 for more detailed procedures.

Event ID: ELA-shadow07

Description: Shadow mailbox space gridlock caused no ELA service for longer than number hours.

Repair Procedure:

See the procedure for SHADOW Resource Type, "Alarm Code: 6" on page 6-64.

Event ID: ELA-delivts05

Description: *Number* minutes with session resources unavailable for delivery trusted server.

The trusted server that delivers ELA messages cannot access AUDIX. The message shows the amount of elapsed time (in 30 minute increments) since ELA has stopped providing service.

When the time elapsed exceeds the value in the `Minutes of Inactivity Before Alarm:` field on the Trusted-Server Profile screen, AUDIX generates a minor alarm (event ID: SERVER0900, resource type SERVER, alarm code 900.)

Repair Procedure:

1. Open the System Parameters IMAPI-Options screen.
2. Is the value in the `Simultaneous Sessions Available for Trusted Server Access:` field at least 2?
 - If yes, go to step 3.
 - If no, change the value.
3. Determine if the AUDIX server is so overloaded that it has no resources available for ELA. Some questions to ask are:
 - How many trusted servers are on the network?
 - What are their activity cycles?

Index

A

administering, 34
 AUDIX, 3
 COS, 16
 LAN, 23
 TCP/IP, 23
administrator's log, 51
alarms, 51
 ELA-badreca01 through ELA-badreca12, 65
 ELA-chkrestrict, 67
 ELA-delivts01, 59
 ELA-delivts02, 60
 ELA-delivts03, 60
 ELA-delivts04, 60
 ELA-delivts05, 68
 ELA-loopvioltn, 67
 ELA-lostlock01 through ELA-lostlock10, 66
 ELA-mboxlock01, 67
 ELA-nestvioltn, 66
 ELA-no_members, 66
 ELA-registry01, 61
 ELA-registry02, 61
 ELA-shadow01, 62
 ELA-shadow02, 62
 ELA-shadow03, 63
 ELA-shadow04, 63
 ELA-shadow06, 64
 ELA-shadow07, 68
AMIS users, 2
AUDIX
 administering, 3
 administering system limits, 15
 mailboxes, 3, 28
 mailing lists, 2
 server name, 24

C

community IDs, 19, 21, 36, 37, 40
COS, administering, 16, 37, 40

D

delivery failure, 52
 codes, 54
domains, 3

E

ELA
 activating, 14
 administering COS, 16
 alarms, 51, 59
 characteristics, 2
 community IDs, 19, 21, 36, 37, 40
 delivery failure codes, 54
 domains, 3
 enhanced lists, 38
 hardware requirements, 5
 installation, 9
 LAN administration, 5, 23
 logs, 51
 mailboxes, 6, 7, 17
 mailing lists, 19
 passwords, 36
 planning for, 3
 ports, 6
 sending restrictions, 19
 shadow mailbox, 8, 19, 22, 36
 software requirements, 5
 traffic, 5
 troubleshooting, 55
 trusted servers, 3, 8, 23, 26, 28, 35
 virus detection, 8
ELA server, 34
 administering, 34
e-mail, 6
enhanced lists, 38
 deleting, 46
 members, 41
 naming, 38
 testing, 48

H

hardware requirements, 5

I

IMAPI
 passwords, 7, 28, 35
 sessions, 3, 8, 26
installation, 9
 rebooting the system, 11
IP addresses, 23

L

LAN administration, 5, 23
logs, 51
 delivery failure, 52

M

mailboxes, 6, 7, 17, 28
mailing lists, 19
 AUDIX, 2
messaging traffic, 5

P

passwords, 6, 28, 36
 IMAPI, 35
 list mailbox, 40
 system, 35
ports, 6

R

rebooting the system, 11

S

security
 e-mail, 6
 external access, 6
 passwords, 6
 trusted servers, 6
 virus prevention, 6
service degradation, ports and, 6
shadow mailbox, 8, 19, 22, 36
software requirements, 5
system limits, AUDIX, 15
system parameters, 1
system passwords, 35

T

TCP/IP, administering, 23
testing enhanced lists, 48
troubleshooting, 55

trusted servers, 28
 definition, 3
 IMAPI sessions, 26
 IP addresses, 23
 names, 35
 security, 6, 8

V

virus detection, 8
virus prevention, 6