Tekelec EAGLE® 5 Integrated Signaling System

ELAP Administration Manual - Up to ELAP 7.0

910-5264-001 Revision C

October 2008

Notice

Information in this documentation is subject to change without notice. Unauthorized use, copying, or translation of this documentation can result in civil or criminal penalties.

Any export of Tekelec products is subject to the export controls of the United States and the other countries where Tekelec has operations.

No part of this documentation may be reproduced, translated, or transmitted in any form or by any means, electronic or mechanical, including photocopying or recording, for any purpose without the express written permission of an authorized representative of Tekelec.

Other product names used herein are for identification purposes only, and may be trademarks of their respective companies.

RoHS 5/6 - As of July 1, 2006, all products that comprise new installations shipped to European Union member countries will comply with the EU Directive 2002/95/EC "RoHS" (Restriction of Hazardous Substances). The exemption for lead-based solder described in the Annex will be exercised. RoHS 5/6 compliant components will have unique part numbers as reflected in the associated hardware and installation manuals.

WEEE - All products shipped to European Union member countries comply with the EU Directive 2002/96/EC, Waste Electronic and Electrical Equipment. All components that are WEEE compliant will be appropriately marked. For more information regarding Tekelec's WEEE program, contact your sales representative.

Trademarks

The Tekelec logo, EAGLE, G-Flex, G-Port, IP7, IP7 Edge, and IP7 Secure Gateway are registered trademarks of Tekelec. TekServer, A-Port, EAGLE 5 ISS, and V-FLEX are trademarks of Tekelec. All other trademarks are the property of their respective owners.

Patents

This product is covered by one or more of the following U.S. and foreign patents:

U.S. Patent Numbers:

5,732,213; 5,953,404; 6,115,746; 6,167,129; 6,324,183; 6,327,350; 6,456,845; 6,606,379; 6,639,981; 6,647,113; 6,662,017; 6,735,441; 6,745,041; 6,765,990; 6,795,546; 6,819,932; 6,836,477; 6,839,423; 6,885,872; 6,901,262; 6,914,973; 6,940,866; 6,944,184; 6,954,526;6,954,794; 6,959,076; 6,965,592; 6,967,956; 6,968,048; 6,970,542; 6,987,781; 6,987,849; 6,990,089; 6,990,347; 6,993,038; 7,002,988; 7,020,707; 7,031,340; 7,035,239; 7,035,387; 7,043,000; 7,043,001; 7,043,002; 7,046,667; 7,050,456; 7,050,562; 7,054,422; 7,068,773; 7,072,678; 7,075,331; 7,079,524; 7,088,728; 7,092,505; 7,108,468; 7,110,780; 7,113,581; 7,113,781; 7,117,411; 7,123,710; 7,127,057; 7,133,420; 7,136,477; 7,139,388; 7,145,875; 7,146,181; 7,155,206; 7,155,243; 7,155,505; 7,155,512; 7,181,194; 7,190,702; 7,190,772; 7,190,959; 7,197,036; 7,206,394; 7,215,748; 7,219,264; 7,222,192; 7,227,927; 7,231,024; 7,242,695; 7,254,391; 7,260,086; 7,260,207; 7,283,969; 7,286,516; 7,286,647; 7,286,839; 7,295,579; 7,299,050; 7,301,910; 7,304,957; 7,318,091; 7,319,857; 7,327,670

Foreign Patent Numbers:

EP1062792; EP1308054; EP1247378; EP1303994; EP1252788; EP1161819; EP1177660; EP1169829; EP1135905; EP1364520; EP1192758; EP1240772; EP1173969; CA2352246

Ordering Information

Your Tekelec Sales Representative can provide you with information about how to order additional discs.

Table of Contents

List of Figures

List of Tables

1

Introduction

Overview

This manual describes how to administer the EAGLE LNP Application Processor (ELAP), and how to use the ELAP user interface menus to perform configuration, maintenance, debug, and platform operations.

The Local Number Portability (LNP) 384 Million Numbers feature supports a maximum of 384 Million provisionable telephone numbers (TNs).

NOTE: Refer to the *LNP Feature Activation Guide* for the available configurations.

The MPS hardware platform supports high speed provisioning of large databases for the Tekelec EAGLE 5 Integrated Signaling System (ISS). The MPS is composed of hardware and software components that interact to create a secure and reliable platform.

MPS running ELAP supports provisioning from the Local Service Management System (LSMS) to the EAGLE 5 ISS Services Module cards, using the LNP 384 Million Number feature for North American LNP.

Scope and Audience

This manual is intended for anyone responsible for ELAP administration and using the ELAP user interface in the EAGLE 5 ISS. Users of this manual and the others in the EAGLE 5 ISS family of documents must have a working knowledge of telecommunications and network installations.

Manual Organization

This document is organized into the following chapters:

- Chapter 1 Introduction contains general information about the ELAP user interface documentation, the organization of this manual, and how to get technical assistance.
- Chapter 2 Functional Description provides a description of ELAP overall design and operation.
- Chapter 3 ELAP Graphical User Interface describes how to log into the ELAP user interface and how to use the ELAP user interface menus.
- Chapter 4 Messages, Alarms, and Status Reporting describes ELAP status reporting, alarms, and error messages.
- Chapter 5 ELAP Software Configuration describes the text-based user interface that performs ELAP configuration and initialization.
- Appendix A Time Zone File Names , lists the valid UNIX file names for setting the time zone in ELAP software configuration.
- Appendix B ELAP Local Provisioning Utility , provides user guide information for the ELAP Local Provisioning Utility (LPU) batch command language.

Related Publications

For information about additional publications that are related to this document, refer to the *Related Publications* document. The *Related Publications* document is published as a part of the *Release Documentation* and is also published as a separate document on the Tekelec Customer Support Site.

Documentation Availability, Packaging, and Updates

Tekelec provides documentation with each system and in accordance with contractual agreements. For General Availability (GA) releases, Tekelec publishes a complete EAGLE 5 ISS documentation set. For Limited Availability (LA) releases, Tekelec may publish a documentation subset tailored to specific feature content or hardware requirements. Documentation Bulletins announce a new or updated release.

The Tekelec EAGLE 5 ISS documentation set is released on an optical disc. This format allows for easy searches through all parts of the documentation set.

The electronic file of each manual is also available from the Tekelec Customer Support site. This site allows for 24-hour access to the most up-to-date documentation.

Printed documentation is available for GA releases on request only and with a lead time of six weeks. The printed documentation set includes pocket guides for commands and alarms. Pocket guides may also be ordered as a set or individually. Exceptions to printed documentation are:

- Hardware or Installation manuals are printed only without the linked attachments found in the electronic version of the manuals.
- The Release Notice is available only on the Customer Support site.

NOTE: Customers may print a reasonable number of each manual for their own use.

Documentation is updated when significant changes are made that affect system operation. Updates resulting from Severity 1 and 2 PRs are made to existing manuals. Other changes are included in the documentation for the next scheduled release. Updates are made by re-issuing an electronic file to the customer support site. Customers with printed documentation should contact their Sales Representative for an addendum. Occasionally, changes are communicated first with a Documentation Bulletin to provide customers with an advanced notice of the issue until officially released in the documentation. Documentation bulletins are posted on the Customer Support site and can be viewed per product and release.

Documentation Admonishments

Admonishments are icons and text throughout this manual that alert the reader to assure personal safety, to minimize possible service interruptions, and to warn of the potential for equipment damage.

Table 1-1. Admonishments

	**DANGER**: (This icon and text indicate the possibility of *personal injury*.)
	**WARNING**: (This icon and text indicate the possibility of *equipment damage*.)
	**CAUTION**: (This icon and text indicate the possibility of *service interruption*.)

Customer Care Center

The Tekelec Customer Care Center offers a point of contact for product and service support through highly trained engineers or service personnel. The Tekelec Customer Care Center is available 24 hours a day, 7 days a week at the following locations:

- Tekelec, USA

  Phone:

  +1 888 367 8552 (US and Canada only)

  +1 919 460 2150 (international)

  Email: *support@tekelec.com*

- Tekelec, Europe

  Phone: +44 1784 467804

  Email:*ecsc@tekelec.com*

When a call is received, a Customer Service Report (CSR) is issued to record the request for service. Each CSR includes an individual tracking number.

After a CSR is issued, the Customer Care Center determines the classification of the trouble. If a critical problem exists, emergency procedures are initiated. If the problem is not critical, information regarding the serial number of the system, Common Language Location Identifier (CLLI), initial problem symptoms (includes outputs and

messages) is recorded. A primary Customer Care Center engineer is also assigned to work on the CSR and provide a solution to the problem. The CSR is closed when the problem is resolved.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Tekelec Customer Care Center 24 hours a day, 7 days a week. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with an EAGLE 5 ISS that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical problems affect service and/or system operation resulting in:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with the Tekelec Customer Care Center.

Locate Product Documentation on the Customer Support Site

To view or download product documentation, log into the Tekelec Customer Support site at:

https://support.tekelec.com/index.asp

1. Log in with your user name and password. (Click on **Need an Account?** if you need to register).
2. Select **EAGLE** from the Product Support menu.
3. Select the release number from the Release menu.
4. Locate the Notices section to view the latest Feature Notice.
5. Locate the Manuals section to view all manuals applicable to this release.

   The documentation is listed in alphabetical order by the manual name. Only the first three manuals display. Click **more…** to see the remaining manuals.
6. Locate the latest revision of the manual name.

   Confirm the release number and last available revision.

   Select the 936-xxxx-x01 part number to download the complete documentation set with all linked files.

   NOTE: The electronic file for this part number is quite large.
7. To view a manual, double-click the manual name.
8. To download a manual, right-click and select **Save Target As**.

NOTE: Customers may print a reasonable number of each manual for their own use.

2

Functional Description

General Description

The Local Number Portability (LNP) 384 Million Numbers feature supports up to 384 Million provisionable telephone numbers (TNs).

The LNP 384 Million Numbers feature utilizes the “master” or “golden” real-time LNP database on the Multi-Purpose Server (MPS).

The MPS hardware platform supports high speed provisioning of large databases for the Tekelec EAGLE 5 ISS. The MPS system is composed of hardware and software components that interact to create a secure and reliable platform.

MPS running the EAGLE LNP Application Processor (ELAP) software supports provisioning from the Local Service Management System (LSMS) to EAGLE 5 ISS Services Module cards. ELAP now supports up to 384 Million ported numbers for North American LNP.

Definition of Terms

The following terms are used throughout this manual:

MPS	One Tekelec 1100 Application Server (T1100 AS) is referred to as an MPS server. The two MPS servers installed at one EAGLE 5 ISS location are installed in one frame or rack. The two MPS servers that are located at one EAGLE 5 ISS location are “mate servers”—from one MPS server, the other MPS server in the rack can be referred to as its mate. The two servers are also referred to as “server A” and “server B.”
MPS System	An MPS system consists of two MPS servers and associated hardware that are located at one EAGLE 5 ISS location. Usually, a minimum of two MPS systems are deployed in the customer network (one at each mated EAGLE 5 ISS). These two MPS systems are considered “mate MPS systems” on mated EAGLE 5 ISSs.
ELAP	The EAGLE LNP Application Processor (ELAP) software that is supported by MPS includes support for the 384 Million Number LNP feature. An MPS server that is hosting ELAP is referred to as an MPS running ELAP. One MPS server running ELAP is also referred to as ELAP A, while the mate MPS server running ELAP is referred to as ELAP B. The two MPS servers running ELAP at each EAGLE 5 ISS site have exactly the same software installed. SP (or SPID) refers to the Service Provider ID. These are (4) alphanumeric characters assigned to each carrier. The ELAP can store up to 32,700 SP entries in the RTDB. MR (Message Relay) is another name for service (CNAM, CLASS, LIDB, ISVM, WSMSC). Each Message Relay entry contains ri (routing indicator) and ngt (new gtt translation) data. The ELAP is capable of storing up to 65,500 MR entries in the RTDB. MR Groups (Message Relay Groups) is a group of one or more MR entries that are grouped or assigned to a particular TN. The ELAP supports up to 2 million MR groups.

Overall Design

The Multi Purpose Server (MPS) hardware platform supports high speed provisioning of large databases for the EAGLE 5 ISS. MPS running ELAP supports the LNP 228 Million Numbers feature. **Figure 2-1** illustrates an ELAP with LNP 228 Million Numbers installation.

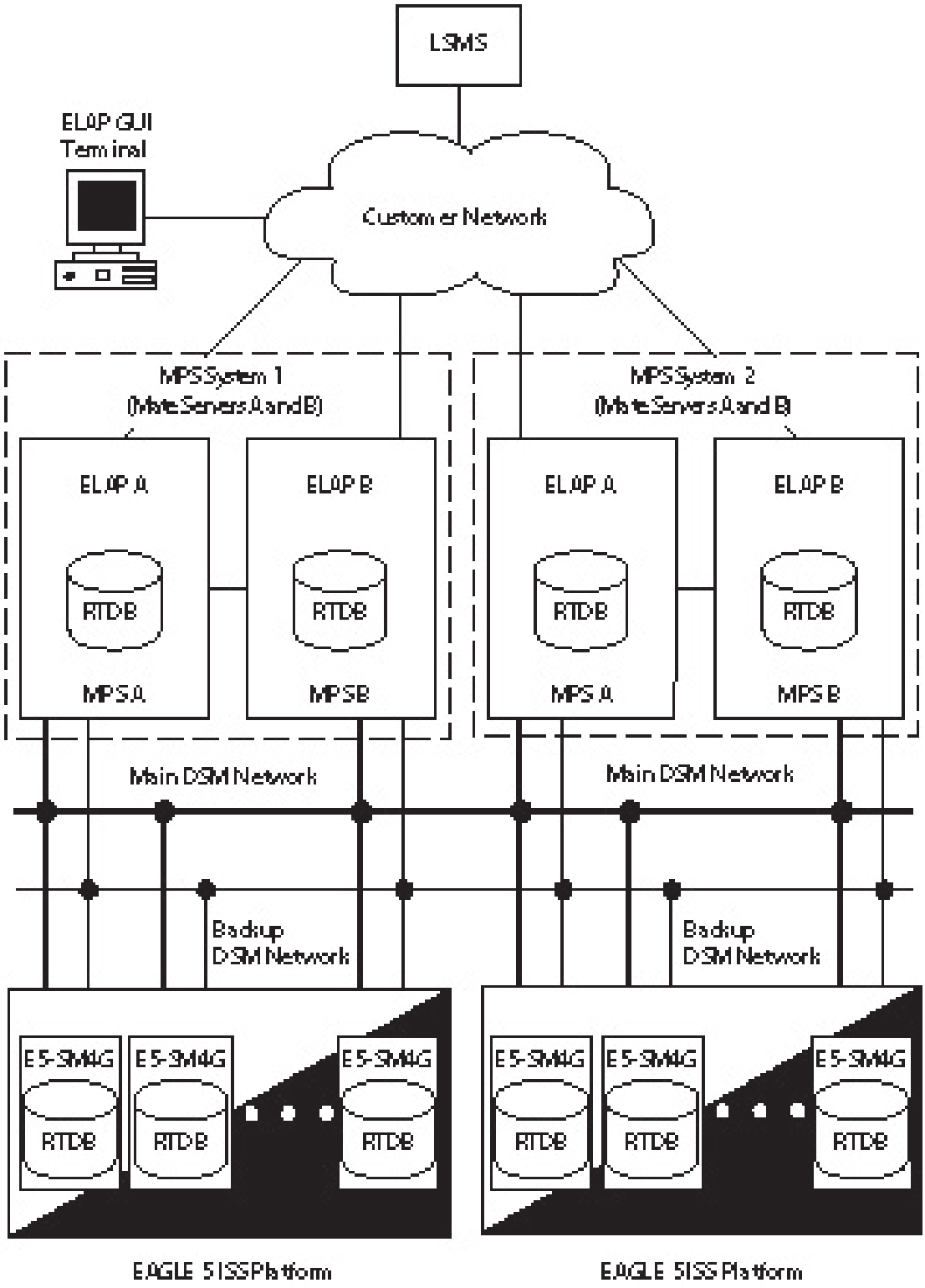
The main functions of ELAP are the following:

- Accept and store data provisioned by the customer from LSMS over the provisioning network
- Update and reload provisioning data to the EAGLE 5 ISS DSM cards.

During normal operation information flows through the ELAP with no intervention.

ELAP provides a direct user interface for performing configuration, maintenance, debugging, and platform operations. Overview of the ELAP User Interfaces describes the ELAP user interface menus and operations.

Figure 2-1. ELAP Installation for LNP 228 Million Number Support



An MPS system consists of two mated Tekelec 1100 AS processors (MPS Server A and MPS Server B) installed as part of an EAGLE 5 ISS. Each server runs ELAP - ELAP A on MPS Server A and ELAP B on MPS Server B.

Two Ethernet networks, referred to as the main and backup DSM networks, connect the DSMs and the ELAPs. Another Ethernet network connects the two ELAPs; it is referred to as the ELAP Sync network. (See Network Connections .)

Figure 2-1 shows the network layout. **Table 2-3** shows examples of typical IP addresses of the network elements.

The ELAPs connect to the LSMS at ELAP initialization and receive provisioning data from the LSMS. The ELAPs store the provisioning data in redundant copies of the real-time database (RTDB), and use the data to provision the EAGLE 5 ISS DSM cards. The set of DSMs, which each hold a copy of the RTDB, is part of the EAGLE 5 ISS.

One ELAP runs as the Active ELAP and the other as the Standby ELAP. In normal operation, the DSM database is provisioned through the main DSM network by the Active ELAP. In case of failure of the Active ELAP, the Standby ELAP takes over the role of Active ELAP and continues to provision the DSM databases.

In the case where the main DSM network fails the Active ELAP switches to the backup DSM network to continue provisioning the DSMs. At any given time there is only one Active ELAP using one DSM network per MPS system.

ELAP Switchover

ELAPs assume an Active or a Standby role through negotiation and algorithm. This role impacts the way the ELAP handles its various external interfaces. External provisioning is allowed only through the Active ELAP. Only the Active ELAP can provide maintenance information to EAGLE 5 ISS.

An ELAP can switch from an Active to a Standby role under the following circumstances:

1. The ELAP maintenance component becomes isolated from the maintenance component on the mate ELAP and from EAGLE 5 ISS.

   This implies that the maintenance subsystem has attempted and failed to establish communication with each of the following:

   - The mate ELAP maintenance task across the Sync network
   - The mate ELAP maintenance task across the main DSM network
   - Any Service Module card on any DSM network

2. The RTDB becomes corrupt.
3. All of the RMTP channels have failed
4. A fatal software error occurred.
5. The ELAP is forced to Standby by the user interface Force to Become Standby operation.

If the Active ELAP has one or more of the five switchover conditions and the Standby ELAP does not, a switchover occurs. **Table 2-1** lists the possibilities:

Table 2-1. ELAP Switchover Matrix

Active state	Standby state	Event	Switchover?
No switchover conditions	No switchover conditions	Condition occurs on Active	Yes
Switchover conditions exist	Switchover conditions exist	Conditions clear on Standby; switches to Active	Yes
No switchover conditions	Switchover conditions exist	Condition occurs on Active	No
Switchover conditions exist	Switchover conditions exist	Condition occurs on Active	No
Switchover conditions exist	Switchover conditions exist	Condition occurs on Standby	No
Switchover conditions exist	Switchover conditions exist	Conditions clear on Active	No

The following are exceptions to the switchover matrix:

1. If the mate maintenance component cannot be contacted and the mate ELAP is not visible on the DSM networks, the ELAP assumes an Active role if any Service Module cards are visible on the DSM networks.
2. If the ELAP user interface menu item is used to force an ELAP to Standby role, no condition causes it to become Active until the user removes the interface restriction with another menu item.

   (See " Force Standby Menu ").

If none of the Standby conditions exist for either ELAP, the MPS servers negotiate an Active and a Standby. The mate is considered unreachable after two seconds of attempted negotiation.

Network Connections

Each MPS system is equipped with four network connections. This section describes the four networks and the IP address assignment for the networks that require them.

Table 2-2. Sample Network IP Addresses Configured from UI

Network Connection	Sample MPS A Value	Sample MPS B Value
Hostname	MPSA-000000	MPSB-000001
Provisioning Network IP Address	10.25.50.45	10.25.50.46
Provisioning Network Netmask	255.255.255.0	255.255.255.0
Provisioning Network Default Router	10.25.50.250	10.25.50.250
Sync Network IP Address	192.168.3.100	192.168.3.200
Main DSM Network IP Address	192.168.1.100	192.168.1.200
Backup DSM Network IP Address	192.168.2.100	192.168.2.200

NOTE: These values are not the correct values for your network! The values that you enter while configuring the ELAPs will be unique to your network configuration. The *Signaling Products Hardware Manual* describes how to determine the actual values for your network.

DSM Networks

The main DSM network carries provisioning data from the RTDBs on the ELAP to the RTDBs on the Service Module cards, and carries reload and maintenance traffic to the Service Module cards. The 100BASE-T main DSM network runs half-duplex at 100 Mbps. The 10BASE-T backup DSM network carries only connection maintenance traffic unless the main network is not operational; if the main network fails, the backup network carries all of the traffic normally carried by the main network. The backup DSM network runs half-duplex at 10 Mbps. Each network connects ELAP A and ELAP B to each DSM on a single EAGLE 5 ISS.

The first two octets of the ELAP network addresses for this network are 192.168. These are the first two octets for private class C networks as defined in RFC 1597.

The third octet for each DSM network is configured, usually to the default value .120 for the main network and the default value .121 for the backup network These are not visible to any external networks, and should not need to be changed.

The fourth octet of the address is selected as follows:

- If the ELAP is configured as ELAP A, the fourth octet has a value of 100.
- If the ELAP is configured as ELAP B, the fourth octet has a value of 200.

Table 2-3 summarizes the derivation of each octet.

The configuration menu of the ELAP user interface contains menu items for configuring the ELAP network addresses. (See ELAP Configuration and Initialization).

Table 2-3. IP Addresses on the DSM Network

Octet	Derivation
1	192
2	168
3	Usually already configured as: 120 for DSM main network 121 for DSM backup network
4	100 for ELAP A 200 for ELAP B 1 - 25 for Service Module cards on the networks

ELAP Sync Network

The ELAP Sync network is a point-to-point network between ELAP A and ELAP B on a single MPS system. This network provides a high-bandwidth dedicated communication channel for MPS data synchronization. This network is a single Ethernet crossover cable, uses 100Base-T protocol, and runs at full-duplex 100 Mbps.

The ELAP Sync network carries RTDB and maintenance application traffic between the Active ELAP and the Standby ELAP on the MPS platform.

The first two octets of the ELAP IP addresses for the Sync network are 192.168. These are the first two octets for private class C networks as defined in RFC 1597.

The third octet for each ELAP Sync network address is set to .2 as the default. It can be changed if necessary. It is important to perform the instructions to Configure Sync Network if you change this octet value.

The fourth octet of the Sync network IP address is .100 for ELAP A, and .200 for ELAP B.

Dialup PPP Network

The Point-To-Point Protocol (PPP) Network allows multiple user interface sessions to be established to the ELAP from a remote workstation over a dialup connection. Dialup

The MPS servers are configured for the use of a modem on port a001 on the serial expansion board. The modem connection supports PPP (TCP/IP). With this capability, multiple networked applications can be run across the PPP link at the same time.

PPP also requires two IP addresses to be registered, one to the serial port on the server, and one to the client dialing into the server. These IP addresses are allocated on the Sync network.

If the IP address of the Sync network is changed using an ELAP user interface configuration menu item, the PPP IP addresses are updated by the user interface operation at the same time.

The remote dial-in serial port is configured as follows:

- Hardware flow control (RTS/CTS)
- 38400 bps port speed
- 8-bit data
- No parity

Contact Technical Services for assistance in configuring the Dialup PPP Network; see Customer Care Center .

If the remote dial-in serial port is not functional at one EAGLE 5 ISS site, dialing into the remote EAGLE 5 ISS site and connecting back to the functional MPS at the failed EAGLE 5 ISS site allow remote recovery.

Provisioning Network

The provisioning network is the only network attached directly to the customer's network. All provisioning information from the customer's provisioning system travels over this network. In addition, all traffic required to keep remote MPS systems synchronized also travels across this network.

The provisioning (customer) network carries ELAP user interface traffic and traffic between ELAP and the LSMS.

The port is a 10BASE-T/100BASE-T auto-sensing device; it automatically runs as fast as the customer's equipment allows. A dedicated network is recommended, but it is possible that unrelated customer traffic could also use this network.

LSMS-to-ELAP Connection

All normal LNP provisioning is conducted through the LSMS. (Localized retrieval of data can be accomplished through the ELAP user interface.)

The LSMS communicates with each ELAP in the MPS system using the LSMS High Speed Operation Protocol (HSOP. The LSMS connects to both ELAPs at initialization.

Two types of ELAP states are relevant to LSMS communication. The first is the existing Active or Standby role. The second is the ability of an ELAP to apply LNP updates to the RTDB. These two states affect LSMS connectivity as follows:

- A connection is established to each ELAP that is able to apply LNP data.
- Data is sent to only one of the ELAPs. If one ELAP is Active, data is sent to it.

The connection that the LSMS uses to send data to one of the ELAPs is called the LSMS primary connection. This is usually the connection to the Active ELAP. In the event that both sides are Standby or that only one side is available, the LSMS primary connection might not be to an Active ELAP (see **Table 2-4** and **Table 2-5**). An “Unable” or “Down” ELAP does not accept a connection from the LSMS. The following definitions apply:

Active/Able:	The ELAP is the **Active**ELAP, and it is **able** to accept LNP updates and apply them to the RTDB.
Standby/Able:	The ELAP is the **Standby**ELAP, and it is **able** to accept LNP updates and apply them to the RTDB.
Standby/Unable:	The ELAP is the **Standby**ELAP, and it is **unable** to accept LNP updates and apply them to the RTDB.
Down:	The ELAP is unreachable.

Based on the Active/Standby status returned to the LSMS on connection, the LSMS begins to provision LNP data to the Active ELAP across a TCP/IP connection in the customer network.

Table 2-4. ELAP Initial Connection to LSMS

Elap Status	Mate Status	Result
Active/Able	Standby/Able	Connection is established to both ELAPs. The LSMS chooses first ELAP for the LSMS primary connection.
Active/Able	Standby/Unable	Connection is established to first ELAP only. The LSMS chooses first ELAP for the LSMS primary connection.
Active/Able	Down	Connection is established to first ELAP only. The LSMS chooses first ELAP for the LSMS primary connection.
Standby/Able	Down	Connection is established to first ELAP only. The LSMS chooses first ELAP for the LSMS primary connection.
Standby/Able	Standby/Able	Connection is established to both ELAPs. LSMS chooses one of the ELAP for the LSMS primary connection.
Standby/Able	Standby/Unable	Connection is established to first ELAP only. The LSMS chooses first ELAP for the LSMS primary connection.
Standby/Unable	Standby/Unable	No connection is allowed.

Table 2-5. Existing ELAP-to-LSMS Connection

ELAP Status	Change	Result
Active/Able	Active —>Standby	The ELAP closes the connection. LSMS chooses the other ELAP for the LSMS primary connection if it is Active. The ELAP immediately allows another LSMS connection. This switchover

ELAP Status	Change	Result
		mechanism is used because the HSOP does not allow for ELAP status reporting to the LSMS.
Able	Able —>Unable	The ELAP closes the connection. LSMS sends data to the other ELAP if it is able to apply LNP updates. The ELAP does not allow another LSMS connection until it is able to apply LNP updates to the real-time database.

Data is collected at the LSMS from the Number Portability Administration Center (NPAC) (for subscription data) and from local provisioning on the LSMS (for default NPANXX, split NPANXX and other types of LNP records). This data is sent to the Job Routing Server (JRS) at the Active ELAP, which performs minimal parsing and validation before updating its real-time database (RTDB) and replicating the data to the mate ELAP RTDB. The ELAP with the LSMS primary connection ensures that the RTDBs on both ELAPs receive the provisioning data.

Network Time Protocol (NTP)

The Network Time Protocol (NTP) is a Internet protocol that synchronizes clocks of computers to Universal Time Coordinated (UTC) as a time reference. NTP reads a time server's clock and transmits the reading to one or more clients; each client adjusts its clock as required. NTP assures accurate local timekeeping with regard to radio, atomic, or other clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over extended time periods.

If left unchecked, the system time of Internet servers will drift out of synchronization with each other.

The MPS A server of each mated MPS pair is configured, by default, as a “free-running” NTP server that communicates with the mate MPS servers on the provisioning network. (“Free-running” refers to a system that is not synchronized to UTC; it runs off of its own clocking source.) This allows mated MPS servers to synchronize their time.

All MPS servers running the ELAP application have the option to be configured to communicate and synchronize time with an LSMS server or with a customer-defined NTP time server. The **`prefer`** keyword prevents “clock-hopping” when additional MPS or NTP servers (for example, LSMS servers) are defined.

If this optional feature uses an LSMS, the LSMS must be configured as an NTP server. Refer to the *LSMS Configuration Manual* for configuration instructions. When the LSMS has been configured, you can configure the MPS servers to synchronize with the LSMS. Refer to Procedure for Configuring ELAPs for instructions on configuring the MPS servers through the application user interface.

Understanding Universal Time Coordinated (UTC)

Universal Time Coordinated (UTC) is an official standard for determining current time. The UTC is based on the quantum resonance of the cesium atom. UTC is more accurate than Greenwich Mean Time (GMT), which is based on solar time.

The term ‘universal’ in UTC means that this time can be used anywhere in the world; it is independent of time zones. To convert UTC to your local time, add or subtract the same number of hours as is done to convert GMT to local time. The term coordinated in UTC means that several institutions contribute their estimate of the current time, and the UTC is calculated by combining these estimates.

UTC is disseminated by various means, including radio and satellite navigation systems, telephone modems, and portable clocks. Special-purpose receivers are available for many time-dissemination services, including the Global Position System (GPS) and other services operated by various national governments.

Generally, it is too costly and inconvenient to equip every computer with a UTC receiver. However, it is possible to equip a subset of computers with receivers; these computers relay the time to a number of clients connected by

a common network. Some of those clients can disseminate the time, in which case they become lower stratum servers. The industry-standard Network Time Protocol is one time dissemination implementation.

Understanding Network Time Protocol

NTP is an Internet protocol used to synchronize clocks of computers using UTC as a time reference. NTP primary servers provide their clients time that is accurate within a millisecond on a LAN and within a few tens of milliseconds on a WAN. This first level of accuracy is called stratum-1. At each stratum, the client can also operate as a server for the next stratum.

A hierarchy of NTP servers is defined with several strata to indicate how many servers exist between the current server and the original time source external to the NTP network, as follows:

- A stratum-1 server has access to an external time source that directly provides a standard time service, such as a UTC receiver.
- A stratum-2 server receives its time from a stratum-1 server.
- A stratum-3 server receives its time from a stratum-2 server.
- This NTP network hierarchy supports up to stratum-15.

Normally, client workstations do not operate as NTP servers. NTP servers with a relatively small number of clients do not receive their time from a stratum-1 server. At each stratum, it is usually necessary to use redundant NTP servers and diverse network paths to protect against broken software, hardware, or network links. NTP works in one or more of these association modes:

- Client/server mode, in which a client receives synchronization from one or more servers, but does not provide synchronization to the servers
- Symmetric mode, in which either of two peer servers can synchronize to the other, in order to provide mutual backup
- Broadcast mode, in which many clients synchronize to one or a few servers, reducing traffic in networks that contain a large number of clients. IP multicast can be used when the NTP subnet spans multiple networks.

The Tekelec MPS servers are configured to use the symmetric mode to share their time with their mate MPS servers. For an ELAP system, customers using the application user interface have the option to configure the MPS system to receive NTP from LSMS or a customer-provided NTP server.

LNP 228 Million Feature

The LNP 228 Million feature uses Feature Keys to enforce quantity limits. Feature keys also enforce the ON only philosophy. There is one general feature key to indicate the existence of the ELAP device. Three additional feature keys: LNP TN QTY, LNP NPANXX QTY and LNP LRN QTY regulate the maximum capacity allowed within the LNP DB System and contains a finite increment of the quantity field.

The LNP 228 Million feature auto-inhibits any SCCP application card that does not meet the minimum hardware requirements based upon feature key capacities and ELAP-Configuration Feature Keys. Refer to the *LNP Feature Activation Guide* for more information on minimum requirements.

Measurement collection is capped at 150,000 NPANXXs and 100,000 LRNs when collection is performed via the OAM. This limitation does not inhibit the provisioning of additional LRNs and NPANXXs, but further entries are not collected or reported. The reduced capacity LNP reports are generated to the FTA area of the fixed disk on

request, and are available for downloading to the local terminal via Kermit. If the number of provisioned LRNs exceeds 100,000 or the number of provisioned NPANXXs exceeds 150,000, the Measurements Subsystem generates a UIM at each hourly collection interval. The UIM is a warning that measurements data have been discarded. The UIM output can be suppressed by setting the UIM threshold limit to zero.

When measurements are being collected by the Measurement-Platform the collection is capped at 300,000 NPANXXs and 150,000 LRNs. When the Measurements Platform is installed, the Measurements Subsystem collects measurements data for all provisioned LRNs and NPANXXs, up to 150,000 LRNs and 300,000 NPANXXs. Full LNP reports are available via FTP on demand or by enabling the schedule option. LNP measurement reports are still available via FTA, but are limited to 100,000 LRNs and 150,000 NPANXXs.

Network Address Translation on MPS

The MPS supports 2 types of network address translation (NAT), Port Forwarding and Static Address Mapping. In both cases, the MPS will have private IP addresses that are not available outside of the firewall protected internal network. The firewall will translate particular addresses and port numbers to the internal addresses for the MPS.

The addresses in the following figure are examples. Addresses are not restricted to particular classes/ranges.

Port Forwarding

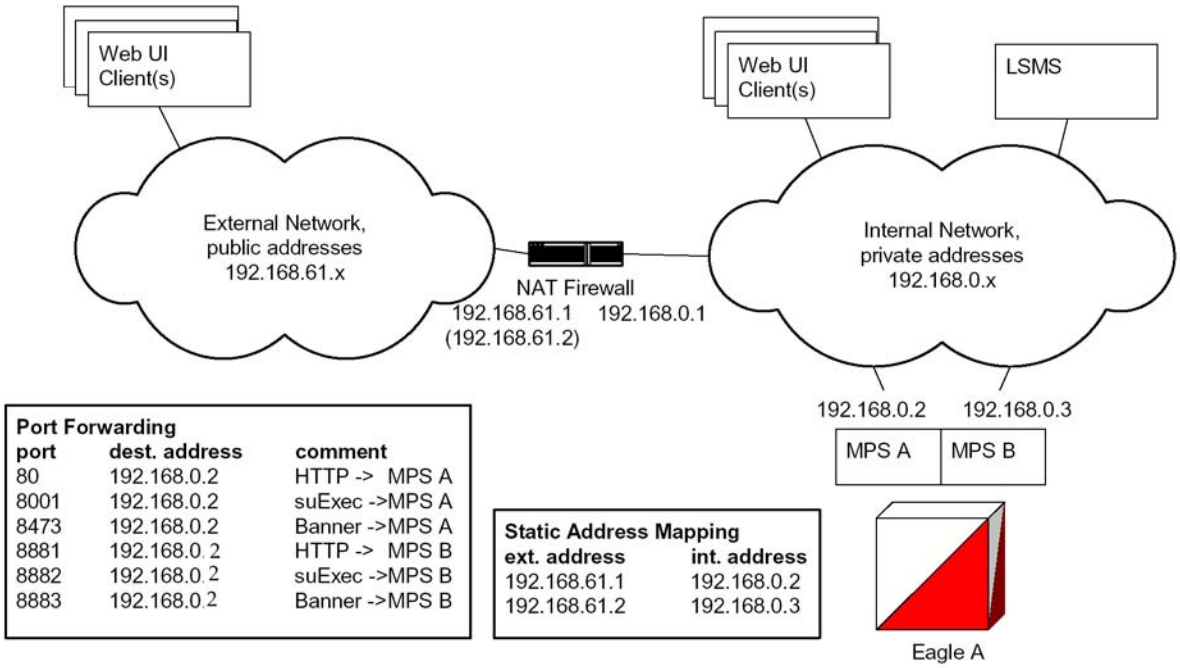
Port forwarding allows a single external address to be used for multiple internal systems. The port forwarding firewall maintains a list of services (basically port numbers) and corresponding internal addresses.

Although the MPS has two individual internal IP addresses, external clients are only allowed to reach the internal network using one external address. The MPS servers must use different port numbers for each externally available service in order to distinguish MPS A from MPS B to external clients.

The MPS uses 3 ports for the Web UI and another 2 ports for the LSMS and EBDA connections. At a minimum, one MPS side must be must be configured with 3 Web UI ports different from the default values. The firewall must be configured to forward 3 Web UI ports to MPS A and 3 different Web UI ports to MPS B. See [4] for a list of the default port numbers used by the MPS.

The LSMS does not currently allow configuration of alternate LSMS and EBDA ports. Until this changes, the LSMS is required to be on the internal network of a port forwarding firewall. Do not change the default values for these ports.

Figure 2-2. NAT on MPS.



Static Address Mapping

Static address mapping makes systems that are behind the firewall appear to have public addresses on the external network. A one-to-one mapping exists between internal and external addresses.

An external address must be assigned to the NAT firewall for each MPS side. The external addresses must be entered into the MPS database in order for the Web UI to be fully functional.

ELAP Security Enhancements

The ELAP Security Enhancements feature controls access to an ELAP GUI to specific IP addresses. The specified allowed IP addresses are kept in an ELAP list and can be added to, deleted from, and retrieved only by an authorized user. This feature also allows an authorized user to toggle IP authorization checking on and off through the GUI.

The administrator or user with IP action privileges can add, delete and retrieve IP addresses. Deleting an IP would result in that IP address no longer residing in the IP table, hence preventing that IP address from being able to connect to an ELAP.

NOTE: While each of the IP action privileges can be assigned to any individual user, the IP action privileges of add and delete should be granted only to users who are knowledgeable about the customer network.

The ability to add, delete, and retrieve client IP addresses and to toggle IP authorization checking is assignable by function. This is accessible through the ELAP GUI (refer to User Administration Menu). The IP mechanism implemented in this feature provides the user a means of further enhancing ELAP privilege control.

The ELAP Security Enhancements feature is available through the ELAP GUI and is available initially to only the administrator. The ability to view IP addresses on the customer's network is a security consideration and should be restricted to users with administration group privileges. In addition, privileged users can prepare a custom message to replace the standard 403 Forbidden site error message.

NOTE: IP access and range constraints provided by the web server and the ELAP Security Enhancement feature cannot protect against IP spoofing. (The term 'spoofing' refers to the creation of TCP/IP packets using another's IP address; it is IP impersonation or misrepresentation). The customer must rely on the security of the customer's intranet network to protect against spoofing.

ELAP maintains a list of the IP addresses that are authorized to access the graphical user interface. Only requests from IP addresses on the authorized list can connect to the ELAP GUI. Attempts from any unauthorized address are rejected.

NOTE: No IP addresses are restricted from accessing the ELAP GUI until the administrator toggles IP authorization to 'enabled'. When IP authorization checking is enabled, any IP address not present in the IP authorization list will be refused access to the ELAP GUI.

ELAP Security Enhancement also provides the means to enable/disable the IP address list once it is provisioned. If the list is disabled, the provisioned addresses are retained in the database, but access is not blocked from IP addresses not on the list. The ELAP GUI restricts permission to enable/disable the IP address list to specific user names and passwords.

The IP actions for adding, deleting, retrieving authorized IP Addresses and for toggling authorized IP checking are available only from the ELAP GUI (described in Chapter 3 ELAP Graphical User Interface Chapter 3), but not from the ELAP text-based UI (described in Chapter 5 ELAP Software Configuration).

LSMS/ELAP PING Enhancement

Depending on customer network architecture, the LSMS and ELAP may be on different internal networks. To increase security, as few ports as necessary should be required to be open inbound to the ELAP network. Currently the LSMS/ELAP interface supports a UDP PING function to monitor the connectivity between the two systems. This feature will move the monitoring function within the HSOP interface, such that the UDP PING port is no longer required.

Because this feature requires changes to both the ELAP and LSMS in order to function, the LSMS will continue to support the existing UDP PING method to address operation with ELAPs that have not been upgraded, as well as continued UDP PING operation in conjunction with the HSOP keep alive.

The procedures to set-up this feature are done on the LSMS.

Service Module Card Provisioning

One of the core functions of the ELAP is to provision the Service Module cards with database updates.

The ELAP provides real-time database loading and provisioning functions for the EAGLE 5 ISS Service Module cards using the main (and backup if necessary) DSM network between the MPS system and the EAGLE 5 ISS Service Module cards. Real-time updates are sent to the EAGLE 5 ISS Service Module cards in parallel using RMTP multicast technology.

The SCCP application, executing on the Service Module cards, conducts all database communications between the Active ELAP and each of the 25 Service Module cards.

Incremental Loading

Incremental loading occurs when a Service Module card has missed some updates, but does not need a complete reload.

The ELAP can broadcast a stream of current updates to all Service Module cards at a rate of 25 updates per second. When the ELAP detects that a Service Module card is back-level from the current provisioning stream, the ELAP attempts to start a new stream at that level.

NOTE: Incremental loading and normal provisioning are done in parallel. The Service Module card provisioning task supports up to five incremental loading streams in addition to the normal provisioning stream.

Incremental reload streams are terminated when the database level contained in that stream matches that of another stream. This is expected to happen most often when the incremental stream "catches up to" the current provisioning stream. Service Module cards accept any stream with the "next" sequential database level for that card.

Service Module Card Reload

Service Module cards might require a complete database reload in the event of reboot or loss of connectivity for a significant amount of time. The ELAP provides a mechanism to quickly load a number of Service Module cards with the current database. The database on the ELAP is large and may be updated constantly. The database sent to the Service Module card or cards is likely to be missing some updates, making it corrupt as well as back level. The upload process is divided in to two stages, one to sequentially send the raw database records and another to send all of the updates missed since the beginning of the first stage.

The Service Module card reload stream uses a separate RMTP channel from the provisioning and incremental update streams. This allows Service Module card multicast hardware to filter out the high volume of reload traffic from Service Module cards that do not require it.

Continuous Reload

The ELAP handles reloading of multiple Service Module cards from different starting points. Reload begins when the first Service Module card requires it. Records are read sequentially from the real-time database from an arbitrary starting point, wrapping back to the beginning. If another Service Module card requires reloading at this time, it uses the existing record stream and notifies the Service Module card provisioning task of the first record it read. This continues until all Service Module cards are satisfied.

Service Module Card Warm Restart

When a Service Module card is rebooted with a warm restart and there were no database updates transmitted during the reboot, the existing database is retained. If updates were transmitted from the ELAP RTDB during the reboot, the Service Module card database is reloaded when the reboot is complete.

ELAP User Interface Menus

The ELAP user interface consists of several menus of items that provide functions for configuration, maintenance, debugging, and platform operations. When a menu item is chosen, the ELAP performs the requested action.

ELAP Graphical User Interface describes how to log into the interface and how to use the menu items. The descriptions include the following information:

- Login user names that can access the user interface menus
- The menu presented to each user for each login name

- Basic function provided by each menu item
- Response syntax expected by any prompts presented to the user by each menu item
- Output that can be displayed for each menu item operation
- Error responses that can be expected

MPS/Service Module Card RTDB Audit Overview

General Description

The fact that the ELAP advanced services use several databases, creates the need for an audit that validates the contents of the different databases against each other. The audit runs on both MPS platforms to validate the contents of the Real-time databases (RTDBs). The active ELAP machine validates the database levels for each of the Service Module cards.

Functional Description

MPS RTDB Audit

This audit maintains the the integrity of the RTDB Database on the MPS. This audit cycles through the entire RTDB within a 24-hour period and reports any anomalies in the form of an alarm. Once the RTDB is determined to be corrupt, provisioning is stopped and a data reload is required.

The Audit is controlled through the MPS GUI Menu field Maintenance:RTDB Audit. The state of the audit can be viewed and Enabled or Disabled through this control (Maintenance Menu).

When this Audit is enabled, the RTDB validates the CRC32 values per record entry within all tables. If corruption is encountered, an alarm is set on the MPS scrolling banner. All provisioning from the LSMS is halted until the condition is corrected via RTDB Reload

ELAP-to-DSM Network Card DB Level

Each DSM card validates its own database level against the received ELAP database level. An inconsistent alarm is generated at the EAGLE 5 ISS for every inconsistent DSM card. The command **`rept-stat-db`** displays the LNP database on the DSM card as *Diff* level. See **Table 2-6** .

Table 2-6. Inconsistent DSM Card Alarm

UAM#	Severity	Message Text	Output Group (UI Output Direction)
444	Minor	RTDB database is inconsistent	`card`

EAGLE 5 ISS DSM Audit of MPS Databases

This audit is responsible for maintaining the integrity of the RTDB on the VSCCP-DSM Card. This audit cycles though the entire RTDB within a 24 hour period, reporting any anomalies in the form of alarms and possibly (attempts to repair any found corrupted records with those from a mate VSCCP-DSM card.

The STP Options (chg-stpopts) command is used to set this audit. This is done with the aid of the DSMAUD parameter which has three states, OFF, ON and CCC. When the DSMAUD parameter is set to OFF the auditing capabilities on each of the VSCCP-DSM cards is disabled from auditing the RTDB Databases. Setting the DSMAUD parameter to ON enables the auditing capabilities producing corruption alarms when corruption is detected. Setting the DSMAUD parameter to CCC enables the cross correction capabilities, providing a method for repairing corruption as it is encountered.

When corruption is encountered several events occur.

1. The RTDB DB is set to Corrupt Status
2. A UAM (Corrupted RTDB Database Alarm) is sent to the OAM
3. The Corruption is logged and stored in a memory array and contains:
    a. Table Id
    b. Record Number
    c. Table High-water-mark
    d. Old CRC32 value
    e. New CRC32 value
    f. Record Address in memory
    g. Record entry Contents

Table 2-7. Corrupted RTDB Database Alarm

UAM#	Severity	Message Text	Output Group (UI Output Direction)
443	Minor	RTDB database is corrupted	`card`

A maximum of 250 Log entries are permitted within an audit cycle. When this maximum is exceeded the first 25 corrected records are output to the DB output group and the card initiates a Full Re-Load.

VSCCP-DSM cards in the corrupted state continue to receive updates from the MPS and continue to service MSU traffic.

All records received from the MPS are validated through the CRC32 routines prior to being written to memory. If a corrupted record is encountered, data is collected and depending upon the loading phase state, events will differ:

Table 2-8. Effect of Corrupted record received from MPS

MPS Loading Phase	Effect of Corrupted Record Received
Phase I - Loading	Booting of Card and Full Reload Requested
Phase II - Resynchronization	Booting of Card and Full Reload Requested
Load Complete	Alarm Incoherent and Reload Required

Corruption Cross Correction

If a record within the RTDB database on any card should become corrupted, a mate VSCCP-DSM card can supply the corrected data. Corruption Cross Correction occurs across the IMT and for each corrupted record encountered a single broadcast message is sent from the affected VSCCP-DSM card to all mate VSCCP-DSM cards. When a VSCCP-DSM card receives a request for corruption correction, the current DB Level and requested record is evaluated for consistency. If the request is validated, a response is sent to the original card. Otherwise the request is simply discarded. This would occupy at most 26 messages on the IMT bus for each corrupted record encountered. When a Corruption Correction Response is received, it is evaluated for correctness and applied once passed. Any subsequent messages received for the same correction is simply discarded.

Status Reporting and Alarms

The MPS systems and ELAPs have no direct means of displaying output messages on EAGLE 5 ISS terminals. Maintenance, measurements, status, and alarm information must be routed from the Active ELAP to an arbitrarily selected Service Module card, known as the primary Service Module card. Static information is exchanged across this interface at initialization and dynamic information is exchanged on occurrence.

All the alarms are reported in a common message format. The Active ELAP generates and sends Maintenance Blocks to the primary Service Module card. One Maintenance Block is sent when the IP link is established between the Active ELAP and the primary Service Module card. Additional Maintenance Blocks are sent whenever the ELAP needs to report any change in status or error conditions. The information returned in Maintenance Blocks is included in the status reports produced by the **`rept-stat-mps`** command (see Commands).

The alarm reporting mechanism and various alarm messages are described in Chapter 4 Messages, Alarms, and Status Reporting .

3

ELAP Graphical User Interface

Overview of the ELAP User Interfaces

The EAGLE LNP Application Processor (ELAP) User Interface, consists of two user interfaces:

- The Graphical User Interface provides GUI menus that maintain, debug, and operate the platform; it and its associated error messages are described in this chapter.

- The text-based User Interface has a Configuration menu that performs the ELAP configuration and initialization; it is described in Chapter 5 ELAP Software Configuration .

The GUI provides the user with menus and screens to perform routine operations. The text-based user interface provides the ELAP Configuration menu to perform the initial configuration.

To communicate with the ELAP graphical user interface, you use a PC with a network connection and a network browser. For information about using the ELAP GUI, see ELAP Graphical User Interface

To configure ELAP, you use the ELAP text-based user interface. For information about configuring the ELAP and how to set up its PC workstation, refer to Chapter 5 ELAP Software Configuration .

ELAP Graphical User Interface

ELAP employs a web-based user interface. It uses the typical client-server paradigm. The front end appears on an Internet browser. The back end operates on the MPS platform. The front end is officially supported on Microsoft's Internet Explorer, version 5.0 or later, and on Mozilla Firefox, version 1.0.2 or later.

When using Firefox, you might encounter the following message upon logging into the ELAP GUI:

CAUTION: The User Interface may not function correctly with the browser you are using.Microsoft Internet Explorer, version 5 and later, has been certified for this application

The graphical user interface pages have three different sections.

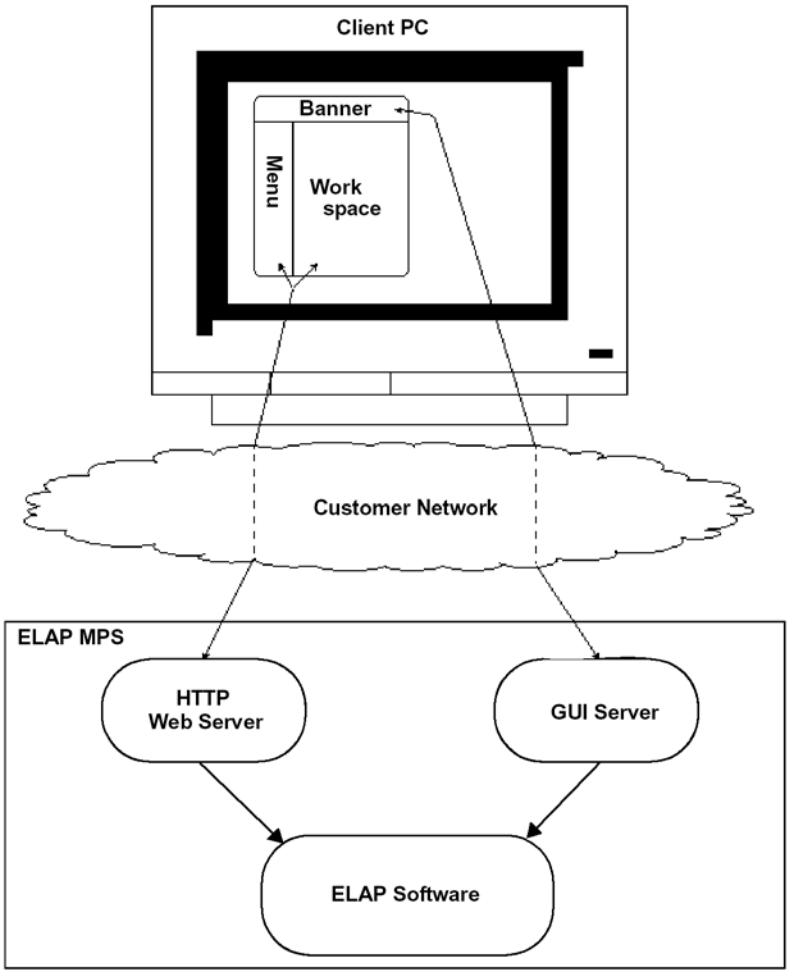
- A banner header section for displaying the real-time status of the MPS servers
- A menu section for selecting desired actions
- A work area section for filling out requested information and displaying results.

The banner header sections are a Java applet that communicates directly with the GUI Server process on the MPS. The menu and work area sections primarily consist of HTML and JavaScript generated by CGI (Common Gateway Interface) scripts on the back end.

An http web server starts the process of handling requests from browsers. It receives the requests and loads the requested document. If the document is a simple HTML file, the http web server just returns the document to the browser. The ELAP software may also connect with the GUI server to request that actions be performed. HTML output from the script is returned to the browser and displayed.

Figure 3-1 shows the process architecture view of the ELAP user interface.

Figure 3-1. Process Architecture View of the ELAP UI



This section describes the various screens, screen structure and layouts, and input prompts of the ELAP GUI. It describes the login screen, the contents of the main screen, and explains the three frames displayed in the browser window of the ELAP user interface.

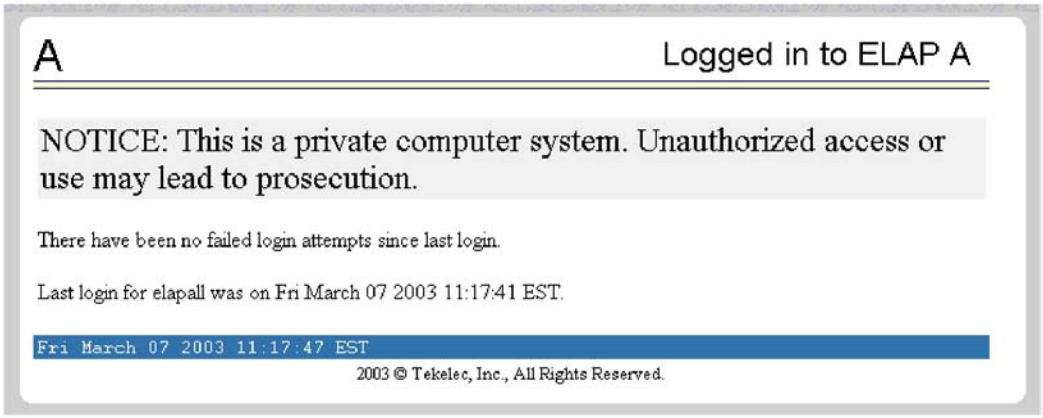
Login Screen

The first screen in the ELAP Internet interface is the login screen. Two fields are prompted for on this screen: **`Username`** and **`Password`**. To log in, enter a valid user name and password, and click the Login button. These fields provide the user identification and verification. See **Figure 3-2** .

Figure 3-2. ELAP UI Login Screen

When a user logs in successfully, the screen workspace indicates the user is logged in, as shown in **Figure 3-3** .

Figure 3-3. ELAP UI Login Screen



When a user logs into the ELAP UI, he does not need to log in again so long as the web browser session remains. This is due to the fact that subsequent user authentication is handled with “cookies,” which are stored in the user's browser and remain there throughout the duration of the browser's operation.

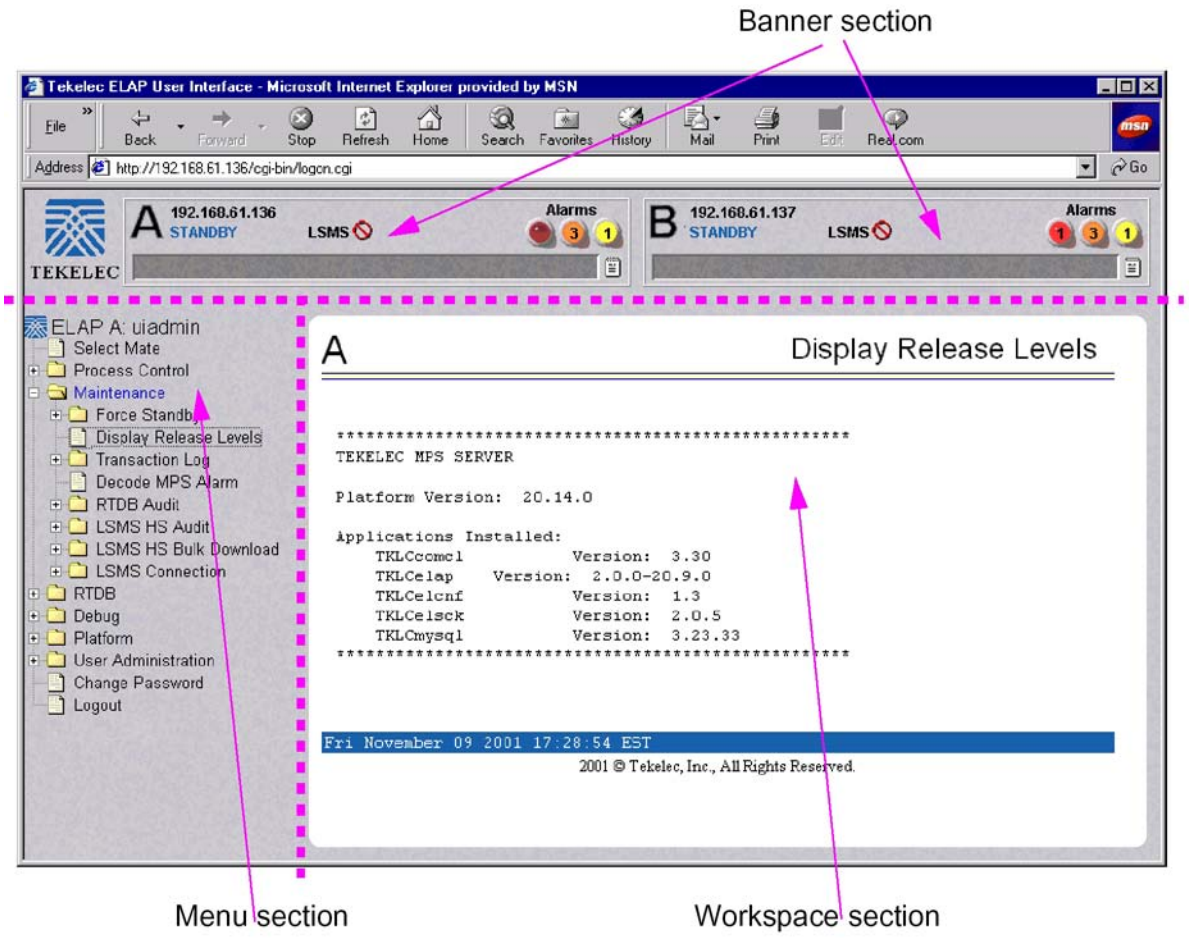
The user uses the Logout menu option to terminate the session and invalidate the cookie. Alternatively, the user can be logged out by session inactivity (defined by User Administration), terminated by the administrator, and by selecting another window on another independent browser.

ELAP GUI Main Screen

The ELAP graphical user interface main screen is composed of three “frames” or window sections. One window section, called the banner, is the topmost frame. It extends the entire width of the browser window.

The remainder of the browser window is divided vertically into two sections of unequal width. The smaller left section is known as the menu section. The larger right section is known as the workspace section. See **Figure 3-4** for a view of the ELAP GUI main screen.

Figure 3-4. ELAP GUI Main Screen



Details describing the three sections of the ELAP GUI window are next.

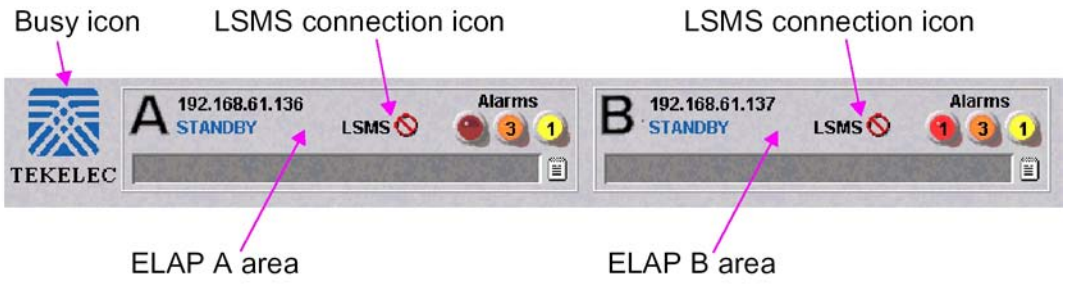
- Banner Section
- Menu Section
- Workspace Section

Banner Section

In order to display real time status information, the banner section (the top area of the UI screen shown in **Figure 3-4**) has a Java applet that remains in constant communication with the ELAP program. The banner applet displays current status of the ELAP, state of the alarms, etc.

The banner applet contains the ELAP A and B areas, and the busy icon. See **Figure 3-5** .

Figure 3-5. ELAP Banner Applet



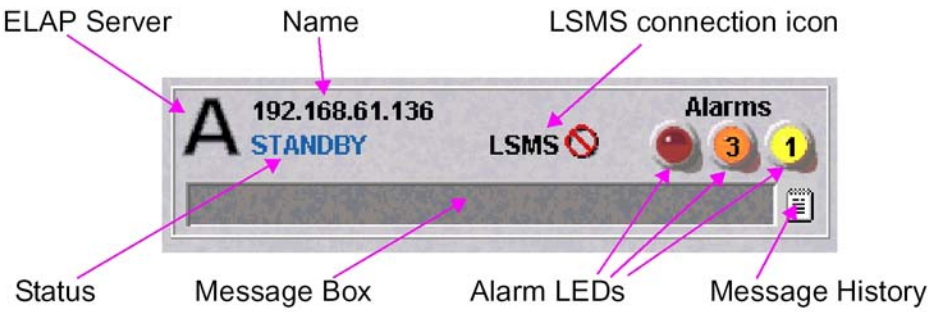
Busy Icon

The Tekelec company logo is located at the top left of the banner applet and performs as the busy icon. Its purpose is to serve as an indicator of activity in progress. When an action is being performed, the Tekelec icon moves; when the action ends, the icon is at rest.

ELAP Areas

The ELAP A and ELAP B areas contain information and displays to inform the user about the status and operation of the servers. See **Figure 3-6** .

Figure 3-6. ELAP Area



ELAP A and ELAP B each have their own sections in the applet, but are structured similarly. The ELAP areas are described:

- ELAP Server - This indicator simply shows which ELAP server (A or B) is represented in this area. There is no action available via click or mouse-over for this field.
- Name - The Name field displays the name of the ELAP represented by this area.
- Status - The Status field displays the current status of the ELAP. The following values can be displayed:
  - — NONE: No established connection exists to the ELAP GUI Server. This can result because of connectivity problems or because the ELAP GUI server is not running.
  - — DOWN: The maintenance task is not running. The box may be running or not.

— UP: The maintenance task is running (UP), but the box is experiencing some problem that prevents it from becoming ACTIVE or STANDBY. This condition can result from a hardware, software, or database problem.

— STANDBY: This ELAP is capable of being the active ELAP but is not for some reason. Valid reasons are either its mate ELAP is active, or there are no DSMs to provision. In the latter case, both ELAPs are STANDBY.

— FORCED STANDBY: This ELAP has been forced into the standby state by the user.

— ACTIVE: This ELAP is actively responsible for provisioning the DSM cards with data. It is also the machine that has the connection to the primary DSM for the passage of maintenance and alarm information.

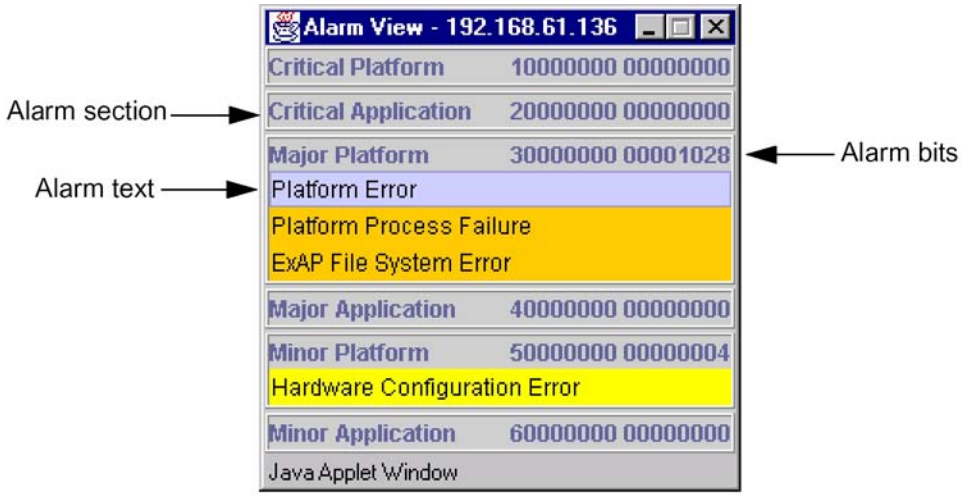
— VIOL: This is not a valid ELAP state. This indicator on the browser indicates that the client browser's Java policy file is incorrect. For details, refer to Java .

- LSMS Connection - The LSMS Connection field displays the connectivity status of the ELAP to the LSMS. If the LSMS is not connected, the label displays an icon indicating no connectivity. If the LSMS is connected, the icon displays an icon indicating a valid connection. When the LSMS is connected, a mouse-over of the label and icon displays the LSMS IP address and the JRS state.

- Alarm LEDs - The three Alarm LEDs show alarm conditions. The left LED indicates Critical alarms; it turns red when a Critical alarm occurs. The middle LED indicates Major alarms, and turns orange when a Major alarm occurs. The right LED indicates Minor alarms, and turns yellow when a Minor alarm occurs. Within each LED is a count of how many alarms of that type are currently active.

  Clicking on any LED or any count field brings up another window that gives more detail on the actual alarms present. See **Figure 3-7** .

Figure 3-7. Alarm View Window



The Alarm View window has the details about what alarms are present. The alarms are subdivided into six categories by alarm type and severity. Each category displays its alarm bit mask for comparing to the EAGLE 5 ISS MPS alarm output. Each alarm category also displays the actual text value and alarm number for each of its active alarms.

For more information about these six alarm categories, refer to Decode EAGLE 5 ISS MPS Alarm Screen .

- Message Box - The message box has a horizontal scroll box that displays text messages for the user. Banner information messages, sometimes referred to as “scroll by” messages, indicate the status of the ELAP machine.

  Here are some messages that are scrolled in the message box.

  — Backup file system successful

  — Restore RTDB in progress

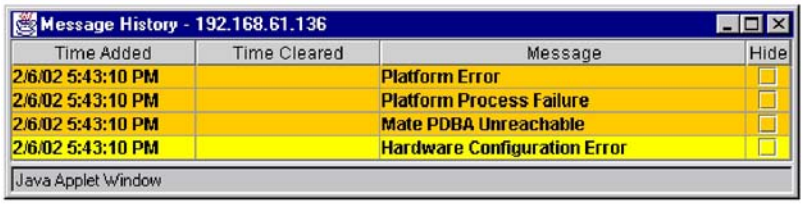
  — RTDB synchronization in progress

  See ELAP Error Messages for the complete list.

- Message History - The Message History icon links to a Java applet that displays in a separate window a history of the alarms and information messages for that server. Messages that scroll by are recorded in the message history box. It serves as a sort of visual log of error events.

  Entries are color-coded to match the severity of its Alarm LED. Messages are coded in the following manner: red are critical, orange are major, yellow are minor, and white are information messages. Optionally, you can suppress messages from appearing in the Message Box by clicking its entry in the ‘Hide’ box in the Message History Box, a useful tool when you want to temporarily hide a recurrent messages. Example of Message History has a sample Message History box.

Figure 3-8. Example of Message History

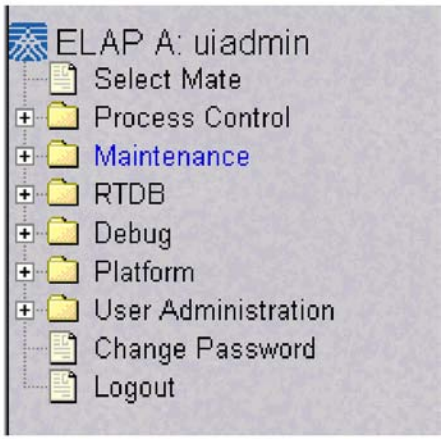


Menu Section

The ELAP graphical user interface menu is located in the left frame of ELAP browser interface. At the top of the frame is the software system title, ELAP, and a letter designation of the selected MPS machine, either A or B. One or more submenus appear below the title, depending on the access privilege of the user who views the menu. An icon accompanies the name of each submenu.

By clicking on the name or folder icon of a directory, the user may expand and contract the listing of the submenu's contents in the typical “tree-menu” fashion. Directory contents may be either menu actions or more submenus. When you click the Menu actions, the output is displayed in the workspace section, which is the right frame of ELAP browser interface. An example of a menu in the menu section is shown in Example of an ELAP Menu.

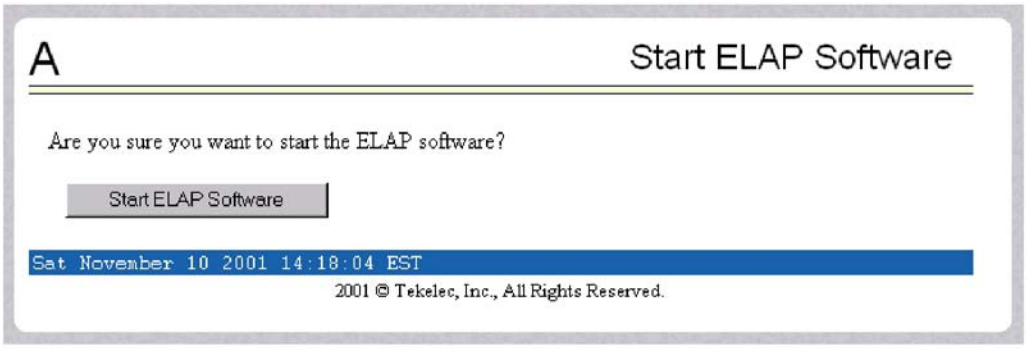
Figure 3-9. Example of an ELAP Menu



Workspace Section

The results of from menu actions are displayed in the workspace section. The content of the workspace section can be various things such as prompts or status reports. Every menu action that writes to the workspace uses a standard format. See the example of the workspace format in Example of Workspace Format.

Figure 3-10. Example of Workspace Format



The format for the workspace is a page header and footer, and page margins on either side. In the header two data fields are displayed. The left-justified letter A or B designates which MPS server this menu action affects. The other data field has the right-justified menu action title. The footer consists of a bar and text with the time when the page was generated. At the bottom of the footer, a Tekelec copyright notice appears.

Workspace Syntax Checking

The web browser user interface uses layers of syntax checking to validate user input for text-entry fields.

- Mouse-over syntax check: For many of the entry fields, you can move the mouse over the field, causing a list of syntax hints for that field to appear.

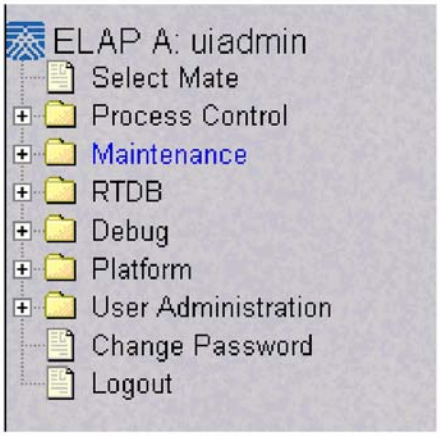
- Pop-up syntax checking: When you click the **Submit** button, syntax is verified on the client side by code running on the user's browser. Incorrect syntax appears in a pop-up window, which contains a description of the syntax error. When the window is dismissed, you can correct the error and submit the input again.

- Back-end syntax checking: When you have clicked **Submit** button and the client side syntax checking has found no errors, back-end syntax checking is performed. If back-end syntax checking detects an error, it is displayed in the work space with an associated error code.

ELAP GUI Menus

The ELAP menu is the main menu of the ELAP application. It provides the functions of the ELAP User Interface. **Figure 3-11** shows the ELAP main menu.

Figure 3-11. ELAP Menu



The ELAP menu provides three actions common to all users, Select Mate, Change Password, and Logout. All the remaining actions are options assignable by the system administrator to groups and individual users.

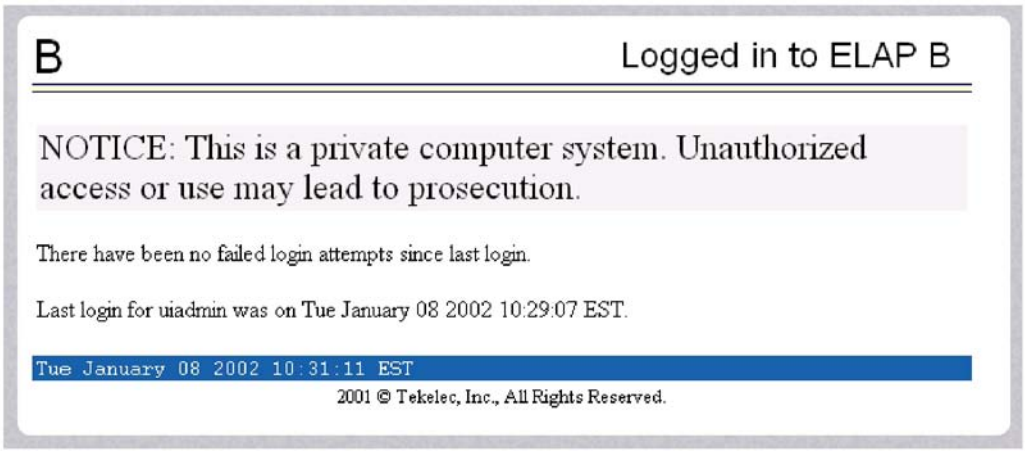
- Select Mate
- Process Control Menu
- LINK
- LINK
- Debug Menu
- Platform Menu
- User Administration Menu
- Change Password
- Logout

Select Mate

The Select Mate menu selection changes the menus and workspace areas to point to the ELAP mate. This selection exchanges the status of the active and standby ELAPs. This basic action is available to all users and is accessible from the main menu.

If you using ELAP A at the main menu, and you want to switch to ELAP B, you click the Select Mate button on the main menu. The initial sign-on screen for the alternate server now appears, as shown in **Figure 3-12** .

Figure 3-12. Select Mate Screen



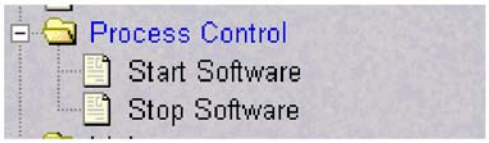
When you perform the Select Mate action, the contents of the banner do not change. However, the side (server) changes in the workspace and at the top of the menu area to indicate the active ELAP.

When you select a mate ELAP that is the standby ELAP, a subsection of the menu is displayed (corresponding to the menu actions that can be executed on the standby ELAP).

Process Control Menu

The Process Control menu allows the user to start and stop the ELAP software processes. .

Figure 3-13. Process Control Menu



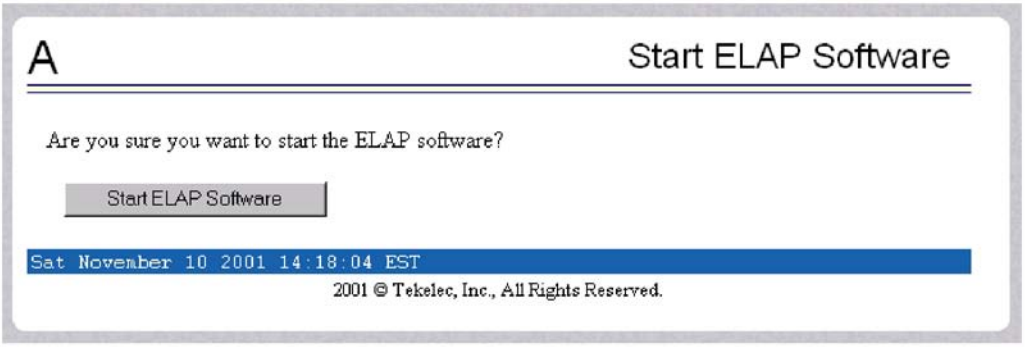
The Process Control menu provides the start and stop software actions.

- Start ELAP Software
- Stop ELAP Software

Start ELAP Software

The Process Control / Start ELAP Software menu option allows you start the ELAP software processes. The screen contains a button to confirm that you do want to start the software processes.

Figure 3-14. Start ELAP Software Screen



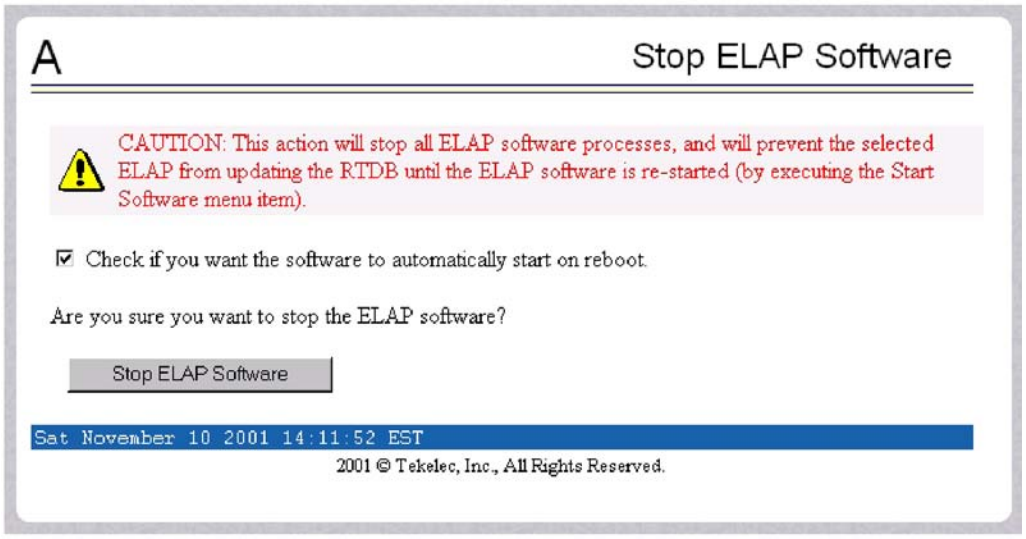
A dialog displays when the ELAP software starts successfully.

Figure 3-15. Successful Start of ELAP Software Screen

Stop ELAP Software

The Process Control / Stop ELAP Software screen allows the user stop the ELAP software processes. The screen contains a button to confirm that the user wants to stop the software processes. It also allows you choose whether the software is to restart automatically when the server reboots.

Figure 3-16. Stop ELAP Software Screen



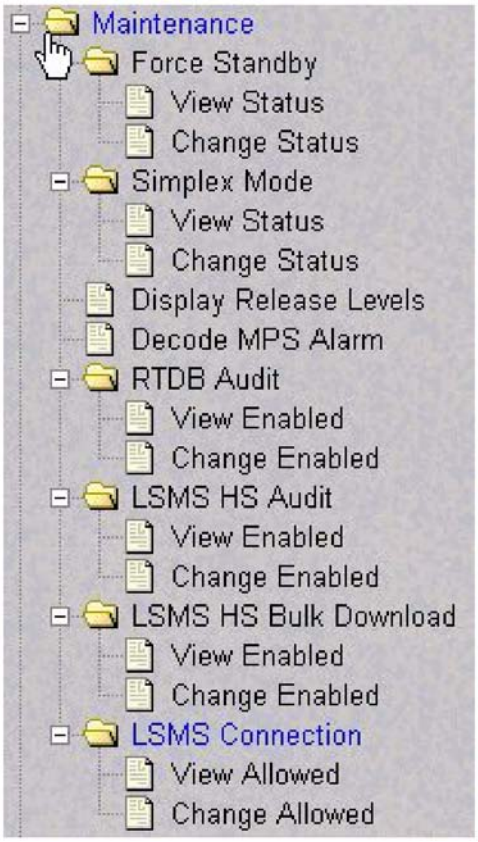
A dialog displays when the ELAP software is successfully stopped.

Figure 3-17. Successful Stop ELAP Software Screen

Maintenance Menu

The Maintenance Menu lets you perform various ELAP platform tasks shown in the Maintenance Menu.

Figure 3-18. Maintenance Menu



The Maintenance menu provides the following actions:

- Force Standby Menu
- Simplex Mode Menu
- Display Release Levels Screen
- Decode EAGLE 5 ISS MPS Alarm Screen
- RTDB Audit Menu
- LSMS High Speed Audit Menu
- LSMS High Speed Bulk Download Menu
- LSMS Connection Menu

Force Standby Menu

The Maintenance / Force Standby menu lets you view the ELAP state and change it by toggling into and out of forced standby state. See **Figure 3-19** .

Figure 3-19. Force Standby Menu

The Force Standby menu provides the following actions:

- View Status Screen
- Change Status Screen

View Status Screen

This Maintenance / Force Standby / View Status screen displays whether or not ELAP is currently in a forced standby state. See **Figure 3-20** .

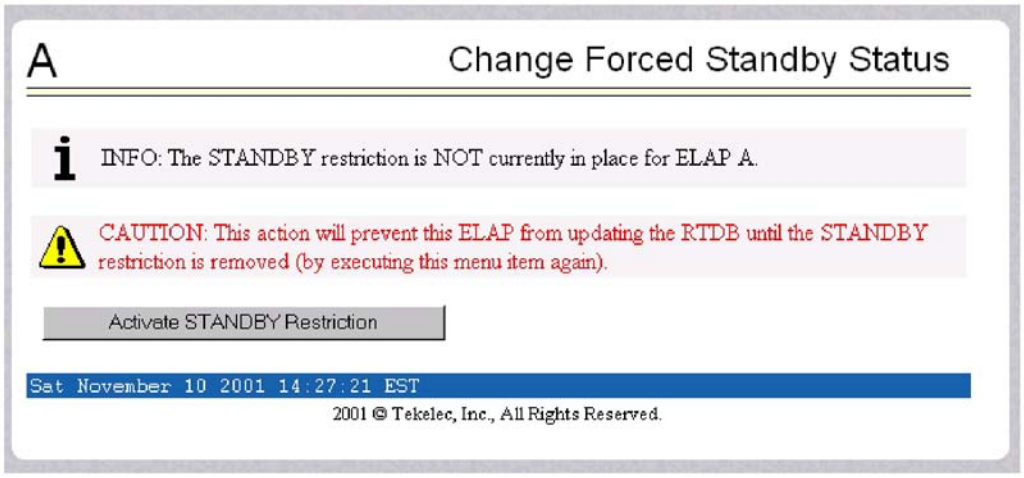
Figure 3-20. View Forced Standby Status Screen

Change Status Screen

The Maintenance / Force Standby / Change Forced Standby Status screen selection toggles the forced standby restriction on the selected ELAP. The current state of the selected ELAP is determined before the output of this screen. If the ELAP is not currently in forced standby mode, this screen lets the user force it into standby mode.

If the ELAP is currently in forced standby mode, the user can remove the standby restriction on the selected ELAP. See **Figure 3-21** .

Figure 3-21. Change Forced Standby Status Screen

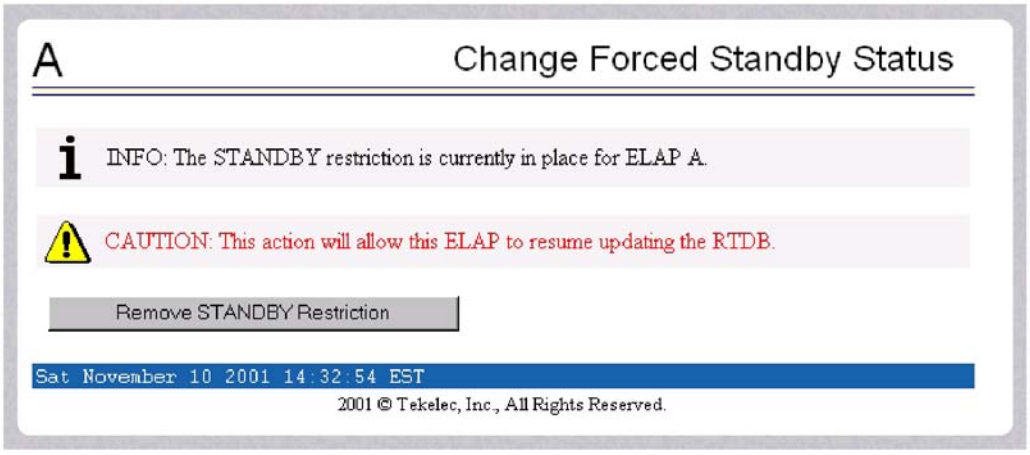


To put the current ELAP in forced standby mode, click the Activate STANDBY Restriction button. See **Figure 3-22** for the screen showing successful change of status.

Figure 3-22. Successfully Changing Forced Standby Status

To remove the forced standby mode, click the Change Status button and see the screen that initiates the removal of the forced standby state, shown by **Figure 3-23** .

Figure 3-23. Removing Changing Forced Standby Status



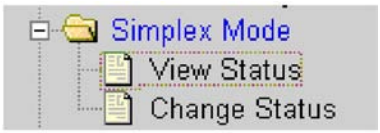
To finish removing the forced standby status, click the Remove STANDBY Restriction button. See **Figure 3-24** for the screen showing a successful change of status.

Figure 3-24. Removing Changing Forced Standby Status

Simplex Mode Menu

The Maintenance /Simplex Mode Menu provides the functionality to view as well as change (i.e toggle) whether or not the ELAP is in the simplex mode. See **Figure 3-25** for this menu.

Figure 3-25. Simplex Mode Menu



The Simplex Mode Menu provides the following functions:

- View Simplex Mode
- Change Simplex Mode

View Simplex Mode

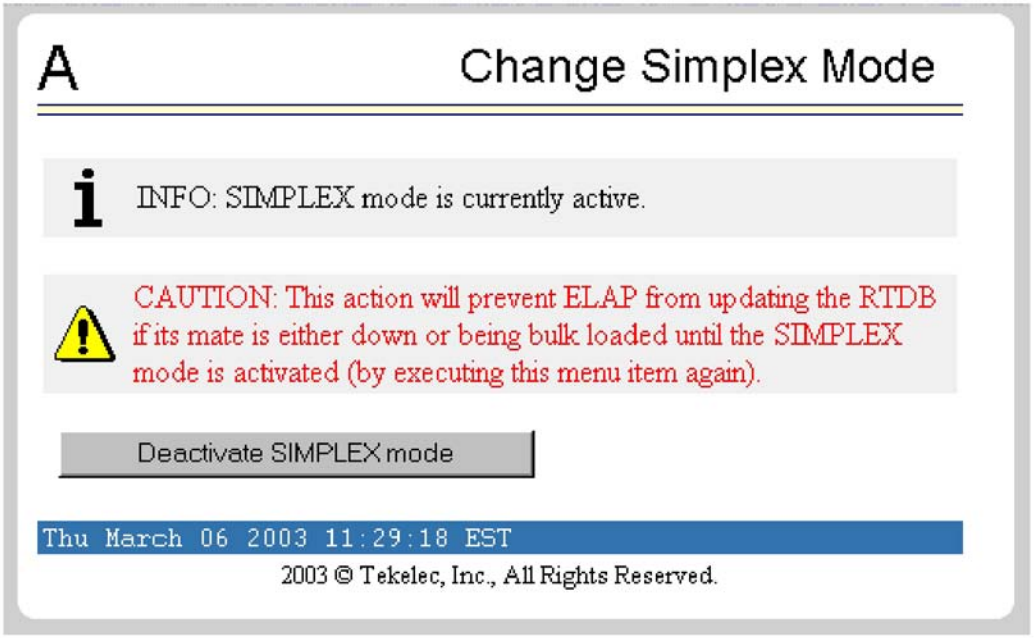
The Maintenance /Simplex Mode Menu/View Simplex Mode screen displays whether or not the ELAP is in the simplex mode state. See **Figure 3-26** for this menu.

Figure 3-26. View Simplex Mode Screen

Change Simplex Mode

The Maintenance /Simplex Mode Menu/Change Simplex Mode screen is used to activate or deactivate the simplex mode on the selected ELAP. The current state of the selected ELAP is shown on this screen. If the ELAP is currently in the duplex mode, this screen will enable the user to change it to the simplex mode. If the ELAP is currently in simplex mode, this screen will enable the user to remove the simplex mode condition on the selected ELAP. See **Figure 3-27** for this menu.

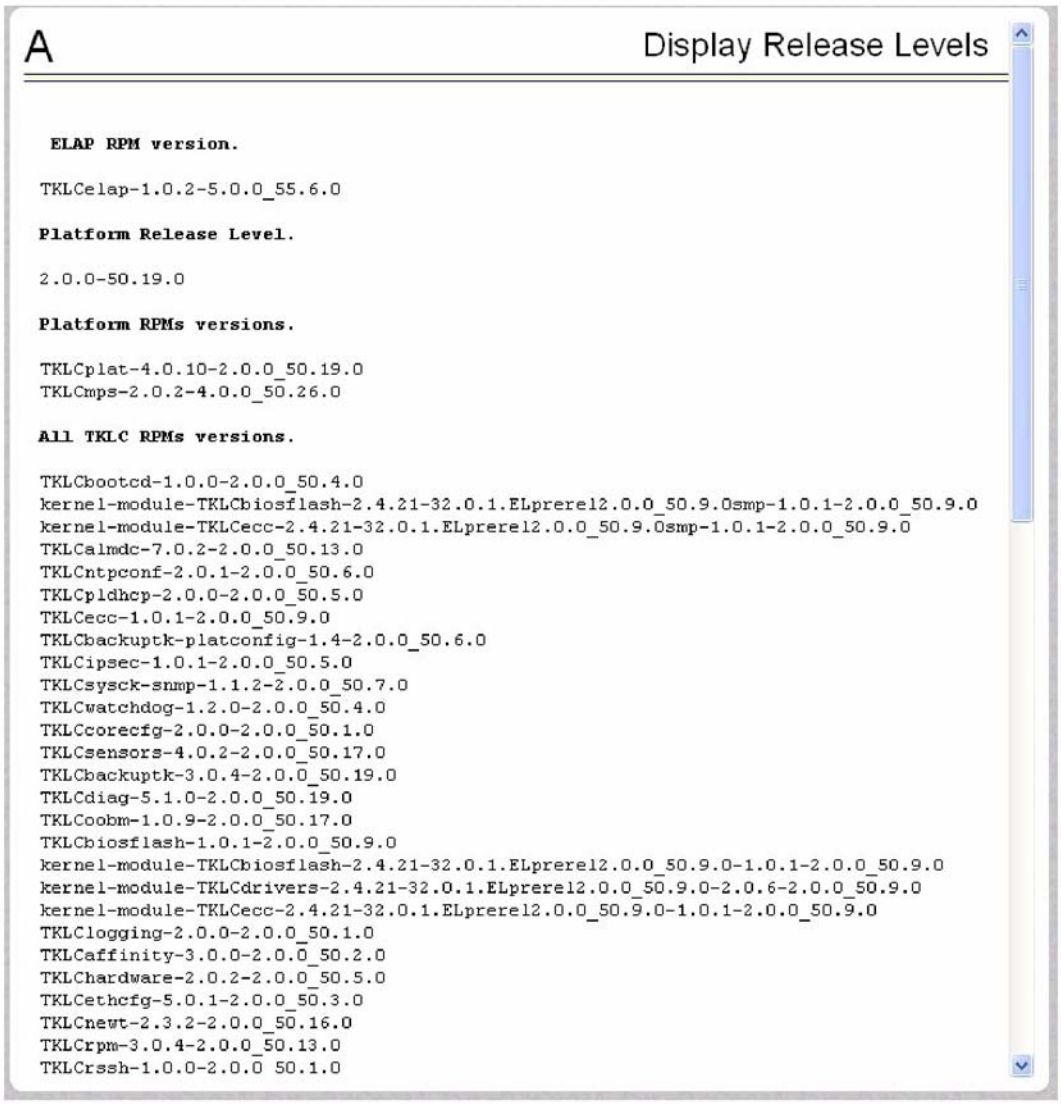
Figure 3-27. Change Simplex Mode Screen



Display Release Levels Screen

The Maintenance / Display Release Levels screen displays release information.

Figure 3-28. Maintenance / Display Release Levels Screen



Decode EAGLE 5 ISS MPS Alarm Screen

The Maintenance / Decode EAGLE 5 ISS MPS Alarm menu selection lets the user decode the EAGLE 5 ISS output of MPS alarms. The user enters the 16-character hexadecimal string from the EAGLE 5 ISS **`rept-stat-mps`** command. The strings are encoded from one of the following six categories, which are reported by UAM alarm data strings:

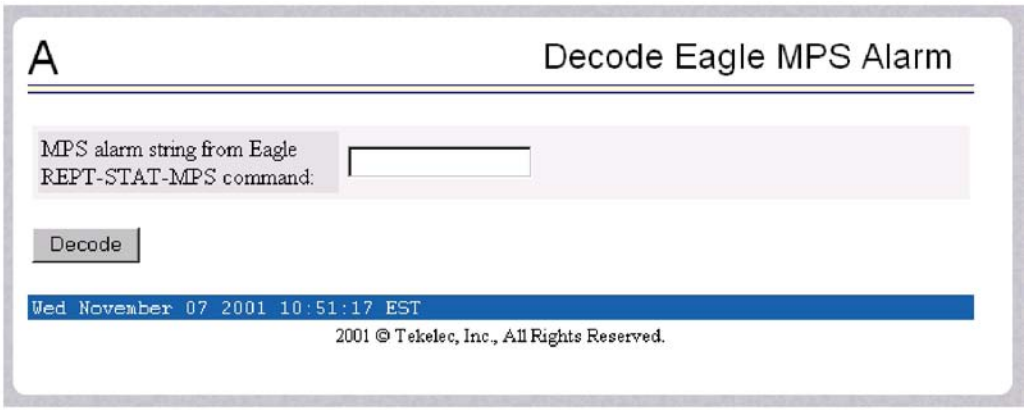
- Critical Platform Alarm (UAM #0370, alarm data h‘1000 . . .’)
- Critical Application Alarm (UAM #0371, alarm data h‘2000 . . .’)

- Major Platform Alarm (UAM #0372, alarm data h‘3000 . . .’)
- Major Application Alarm (UAM #0373, alarm data h‘4000 . . .’)
- Minor Platform Alarm (UAM #0374, alarm data h‘5000 . . .’)
- Minor Application Alarm (UAM #0375, alarm data h‘6000 . . .’)

The string included in the alarm messages is decoded into a category and a list of each MPS alarm that the hexadecimal string represents. The user should compare the decoded category with the source of the hex string as a sanity check. More details about the messages is in “System Health Check” *Tekelec 1100 AS MPS Platform Software and Maintenance Manual*.

The text for the alarms indicated by the alarm hex string is described in MPS Platform and ELAP Application Alarms . See **Figure 3-29** for the Decode EAGLE 5 ISS MPS Alarm screen.

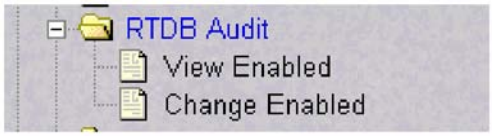
Figure 3-29. Decode EAGLE 5 ISS MPS Alarm Screen



RTDB Audit Menu

The Maintenance / RTDB Audit menu lets the user view and change the auditing of the selected ELAP. See **Figure 3-30** for the Maintenance / RTDB Audit menu.

Figure 3-30. RTDB Audit



The RTDB Audit menu provides these RTDB Audit tasks:

- View Enabled
- Change Enabled

View Enabled

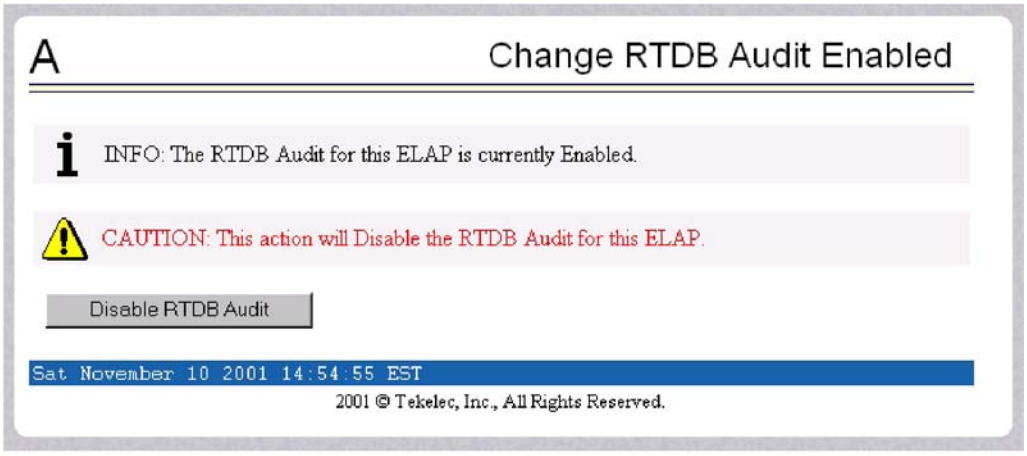
The Maintenance / RTDB Audit / View Enabled menu selection lets the user view the status of RTDB audit enabled, as shown in **Figure 3-31** .

Figure 3-31. View the RTDB Status Screen

Change Enabled

The Maintenance / RTDB Audit / Change Enabled screen turns auditing on and off for the RTDB that is on the selected ELAP. The user interface detects whether RTDB audit is enabled or disabled, and provides the associated screen to toggle the state. In **Figure 3-32** , the RTDB Audit is shown as Enabled.

Figure 3-32. Change the RTDB Audit Enabled Screen

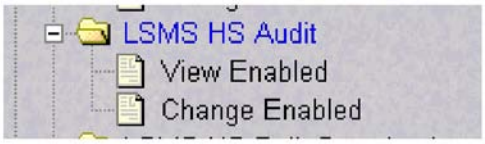


NOTE: RTDB audit and LSMS bulk download cannot be enabled at the same time. Enabling one toggles the other to a disabled state.

LSMS High Speed Audit Menu

The Maintenance / LSMS HS Audit menu lets the user view and change the auditing of the selected ELAP. See **Figure 3-33** for the Maintenance / High Speed Audit menu.

Figure 3-33. LSMS High Speed Audit



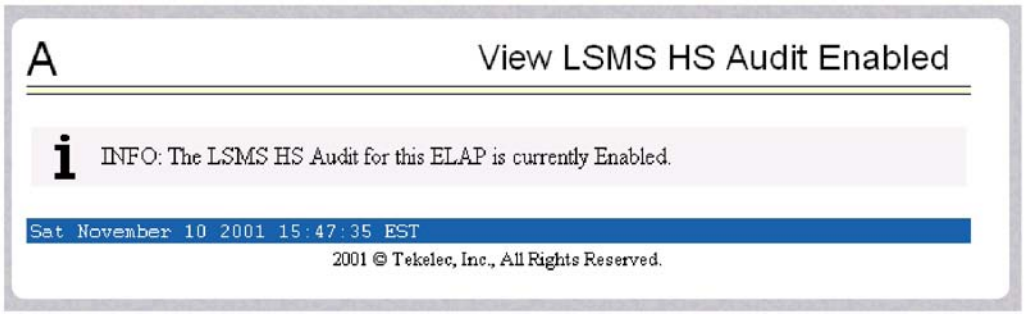
The LSMS High Speed Audit menu provides these actions.

- View Enabled
- Change Enabled

View Enabled

The Maintenance / LSMS HS Audit / View Enabled menu selection reports whether LSMS high speed auditing is enabled or disabled, as shown in **Figure 3-34** .

Figure 3-34. LSMS HS Audit View Enabled Screen

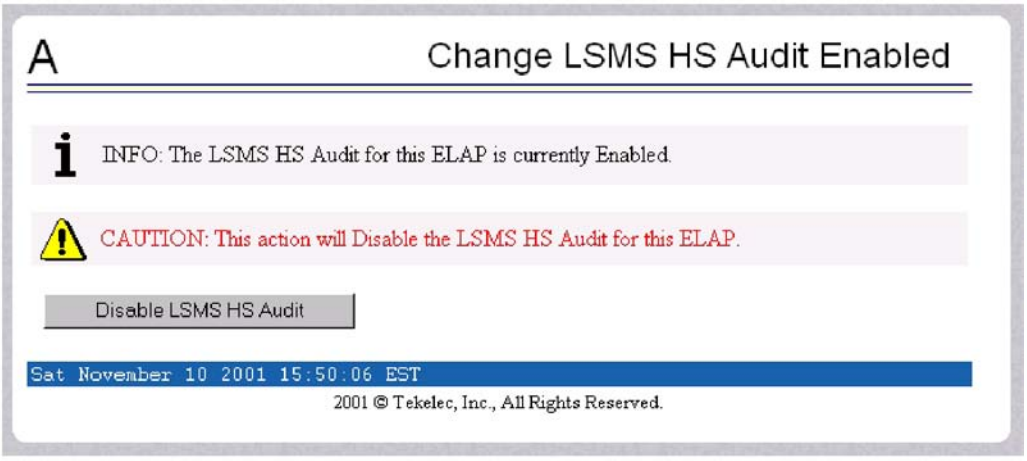


Change Enabled

The Maintenance / LSMS HS Audit / Change Enabled menu selection lets the user change the state of LSMS HS Auditing. The user interface detects the whether LSMS HS audit is engaged or disengaged, and provides the associated screen to toggle (that is, to alternate) the state.

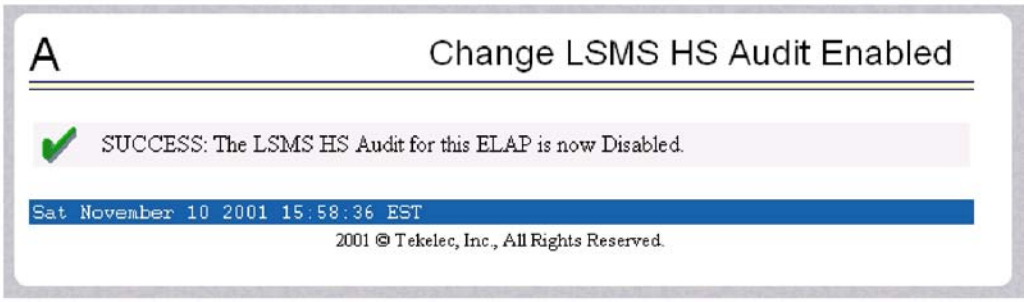
In **Figure 3-35** , the LSMS HS Audit is shown as engaged.

Figure 3-35. LSMS HS Audit Change Enabled Screen



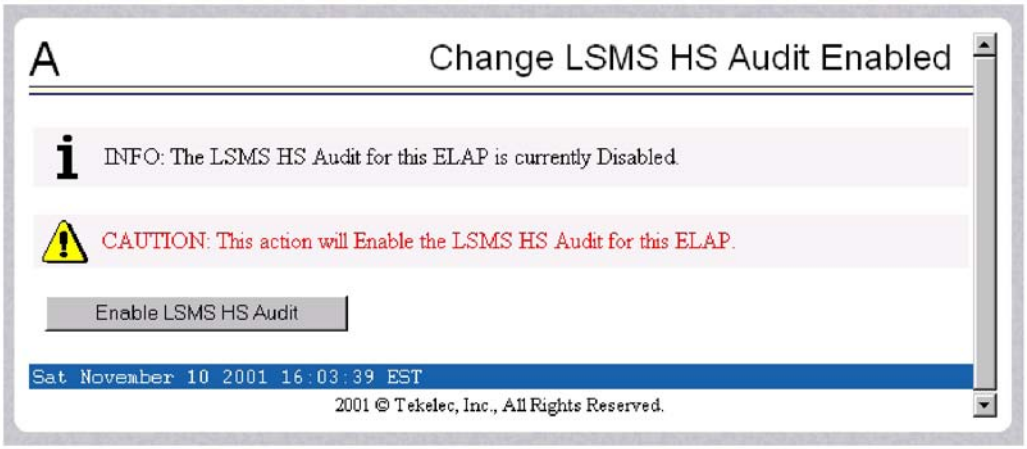
To put the change the status of the LSMS High Speed audit to Disabled, click the Disable LSMS HS Audit button. See **Figure 3-36** for the screen showing successful change of status.

Figure 3-36. Successfully Disabling LSMS HS Audit



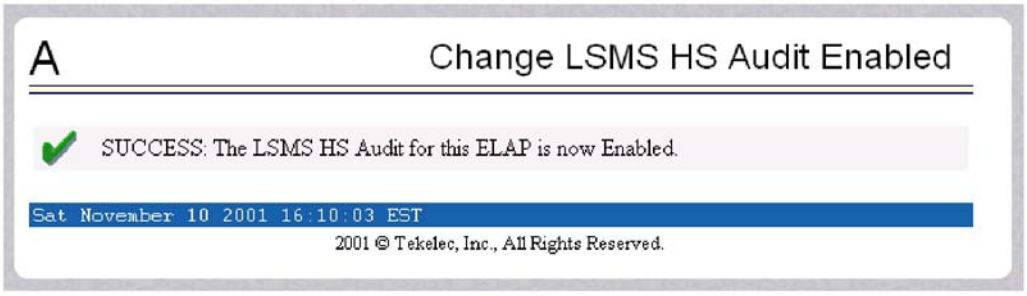
To restore the LSMS HS Audit to Enabled status, click the Change Enabled button on the menu. The new state is displayed in **Figure 3-37** .

Figure 3-37. Restoring LSMS HS Audit Enabled



To confirm the restoring of LSMS HS Audit to Enabled state, click the Enable LSMS HS Audit button, shown in **Figure 3-38** .

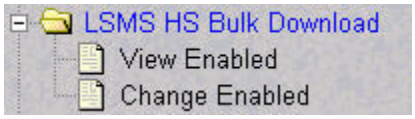
Figure 3-38. Confirming LSMS HS Audit Enabled



LSMS High Speed Bulk Download Menu

The Maintenance / LSMS HS Bulk Download menu lets the user view and change the state of high speed bulk downloading of the selected ELAP. See **Figure 3-39** for the Maintenance / High Speed Bulk Download menu.

Figure 3-39. LSMS High Speed Bulk Download



The LSMS High Speed Bulk Download menu provides these actions.

- View Enabled
- Change Enabled

View Enabled

The Maintenance / LSMS HS Bulk Download / View Enabled menu selection displays the state of the LSMS High Speed Bulk Download / LSMS High Speed Resync. The LSMS Bulk Download/LSMS HS Resync status is enabled, as shown in **Figure 3-40** .

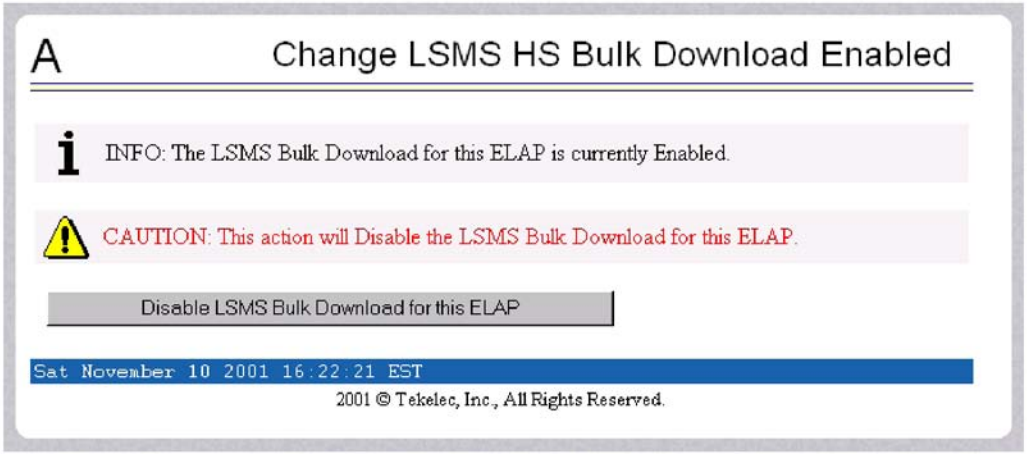
Figure 3-40. LSMS HS Bulk Download View Enabled Screen

Change Enabled

The Maintenance / LSMS HS Bulk Download / Change Enabled menu selection lets the user enable and disable the LSMS Bulk Download/LSMS HS Resync state. The user interface detects whether LSMS Bulk Download/ LSMS HS Resync is enabled or disabled, and provides the associated screen to toggle the state.

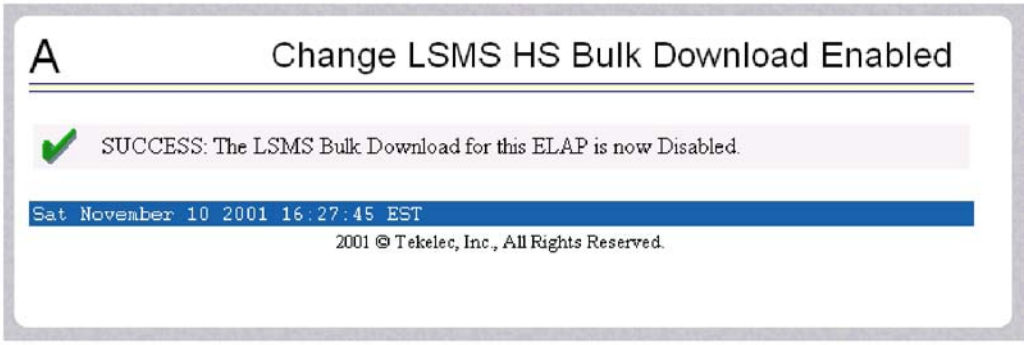
In **Figure 3-41** , the LSMS Bulk Download/LSMS HS Resync is shown as Enabled.

Figure 3-41. LSMS Bulk Download Change Enabled Screen



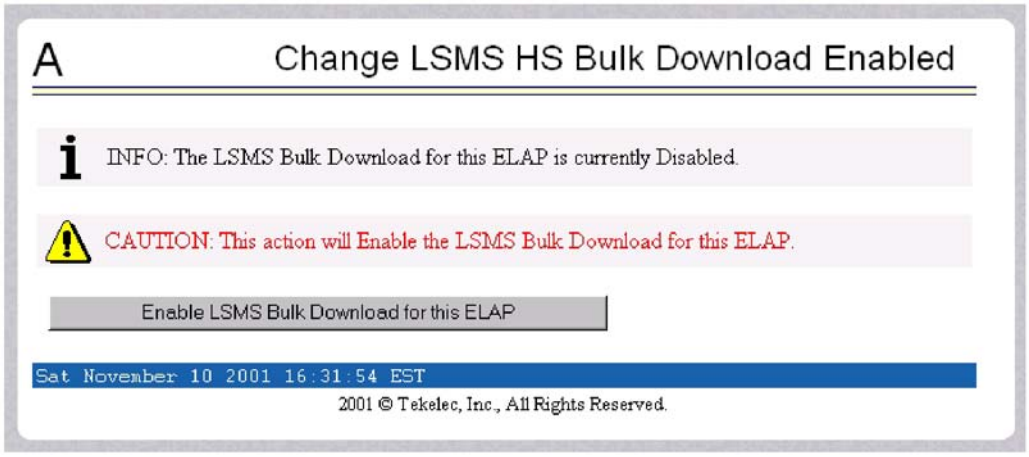
To change the status of the LSMS High Speed Bulk Download to Disabled, click the Disable LSMS Bulk Download for this ELAP button. See **Figure 3-42** for the screen showing successful change of status.

Figure 3-42. Successfully Disabling LSMS HS Bulk Download



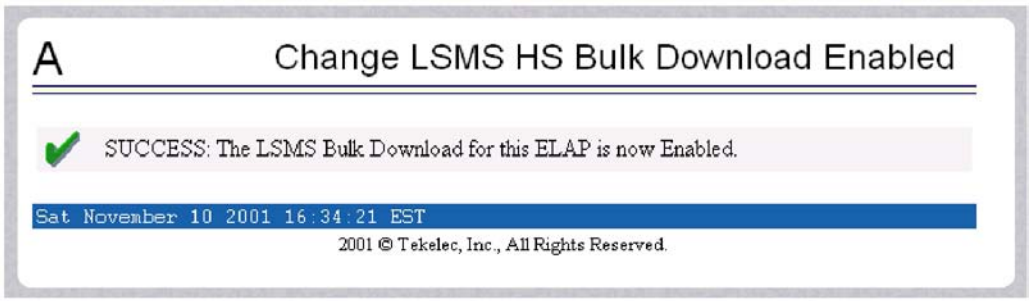
To restore the LSMS HS Bulk Download to Enabled status, click the Change Enabled button on the menu. The new state is displayed in **Figure 3-43** .

Figure 3-43. Restoring LSMS HS Bulk Download Enabled



To confirm the restoring of LSMS HS Bulk Download to Enabled state, click the Enable LSMS Bulk Download for this ELAP button, shown in **Figure 3-43** . When LSMS Bulk Download for the ELAP is successfully enabled, the screen in **Figure 3-44** confirms it is Enabled.

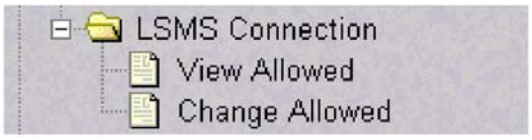
Figure 3-44. Confirming LSMS HS Bulk Download Enabled



LSMS Connection Menu

The Maintenance / LSMS Connection menu lets you view and change the state of the LSMS connection.

Figure 3-45. LSMS Connection



The LSMS Connection menu provides these actions:

- View Allowed
- Change Allowed

View Allowed

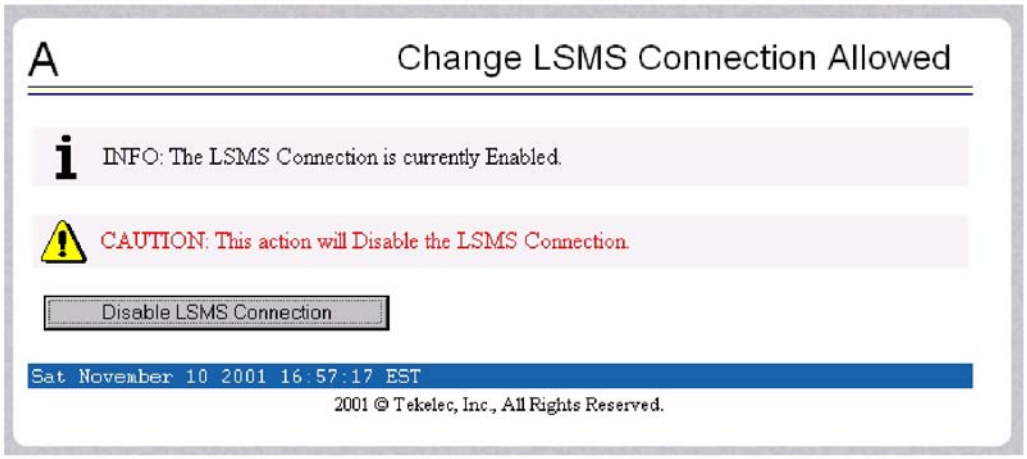
The Maintenance / LSMS Connection / View Allowed menu selection displays the state of the LSMS connection.

Figure 3-46. LSMS Connection View Allowed Screen

Change Allowed

The Maintenance / LSMS Connection / Change Allowed menu selection lets the user enable and disable the LSMS connection. The user interface detects the whether LSMS Connection is enabled or disabled, and provides the associated screen to toggle between (alternate) the states.

Figure 3-47. Change LSMS Connection Allowed Enabled

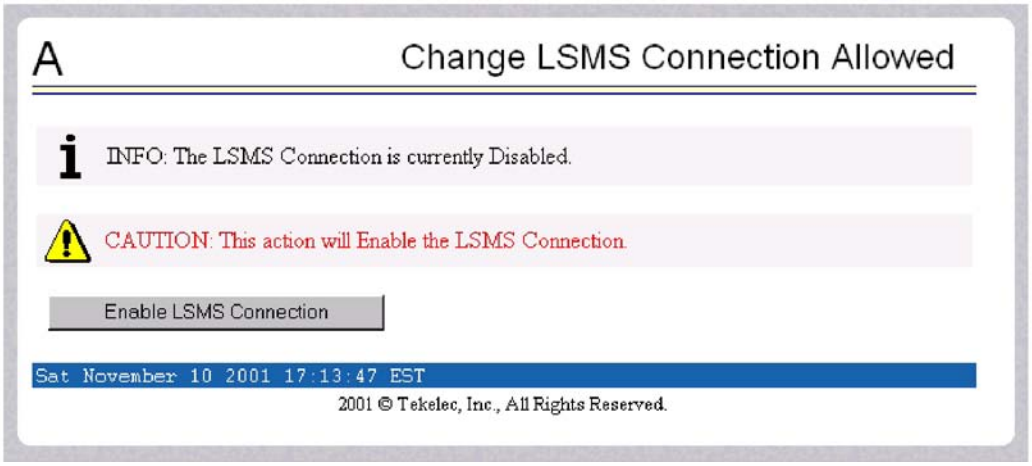


To disable the LSMS connection, click the **Disable LSMS Connection** button. A screen displays, confirming that the LSMS connection was successfully disabled.

Figure 3-48. Successfully Disabling LSMS HS Bulk Download

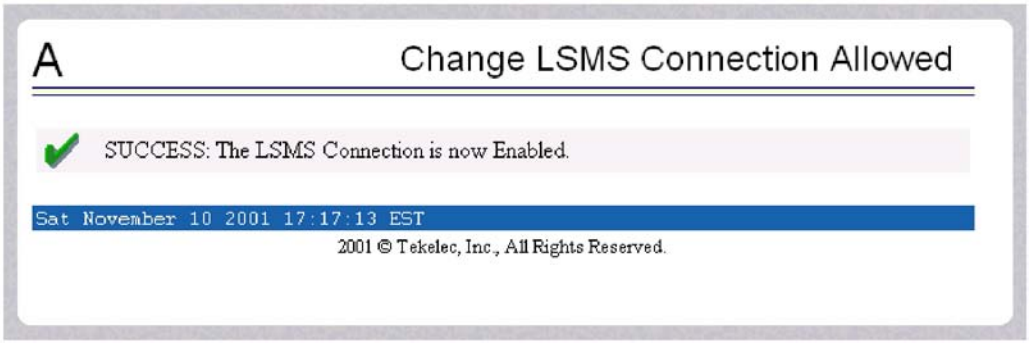
To restore the LSMS HS Bulk Download to Allowed status, click the **Change Allowed** button on the menu. .

Figure 3-49. Restoring LSMS Connection Allowed Enabled



To confirm the restore of LSMS connection to Enabled state, click the **Enable LSMS Connection** button. A screen displays, confirming that the LSMS Connection was successfully enabled.

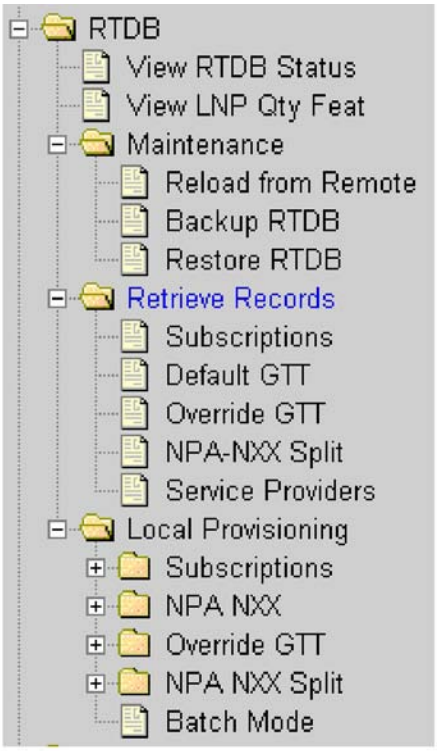
Figure 3-50. Confirming LSMS Connection Allowed Enabled



RTDB Menu

The RTDB (Real Time Database) Menu allows the user to interact with the RTDB for status, reloading, and updating. See the RTDB Menu in **Figure 3-51** .

Figure 3-51. RTDB Menu



The RTDB menu supports various ELAP tasks, including:

- View RTDB Status
- View LNP Qty Features
- Maintenance Menu
- Retrieve Records Menu
- Local Provisioning Menu

View RTDB Status

The RTDB / View RTDB Status screen displays the current level and birthday of the ELAP RTDBs. This selection displays the RTDB status information for both the selected ELAP and its mate. The status information reports the DB level and the DB birthday (date and time of the creation of the database). See **Figure 3-52** .

Figure 3-52. View RTDB Status Screen

View LNP Qty Features

The RTDB /View LNP QTY screen displays the enabled LNP quantity features and quantity enabled as provisioned on the EAGLE 5 ISS. See **Figure 3-53** .

This ELAP version only menu item selection displays the enabled LNP quantity features as provisioned on the EAGLE 5 ISS. User requires "View LNP Qty Features" action privilege to view this menu selection.

Figure 3-53. LNP QTY Features Screen

Maintenance Menu

The RTDB / Maintenance menu lets the user perform RTDB maintenance. See **Figure 3-54** for the RTDB / Maintenance menu.

Figure 3-54. Maintenance Menu

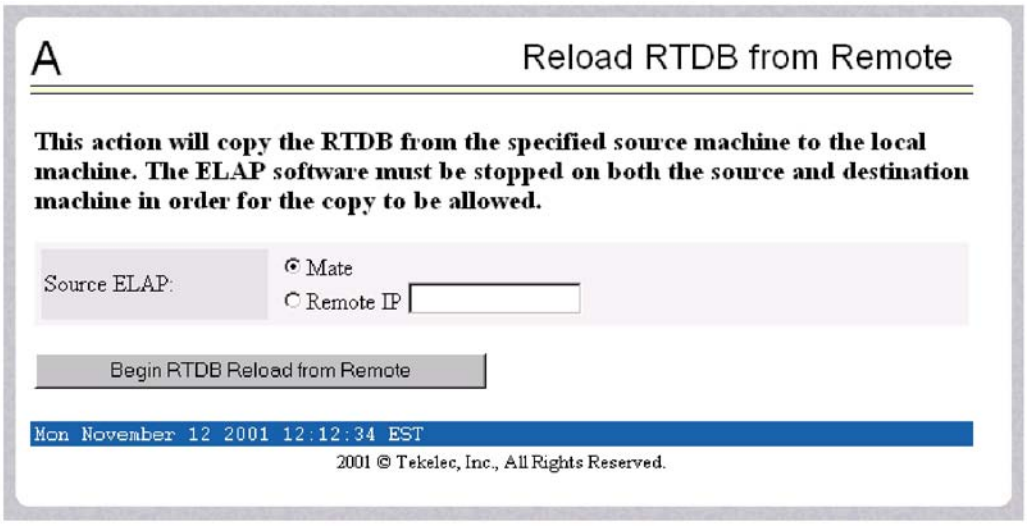
The Maintenance menu provides these actions:

- Reload from Remote
- Backup RTDB
- Restore RTDB

Reload from Remote

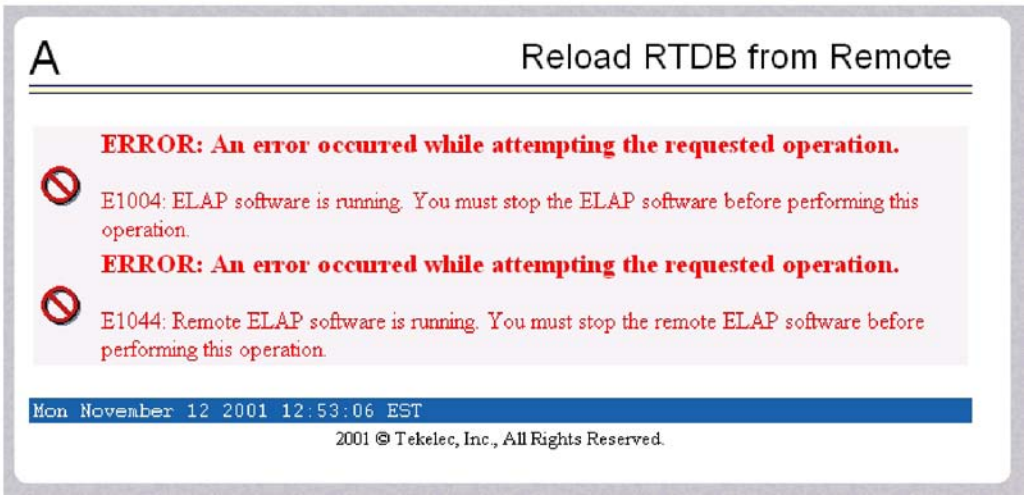
The RTDB / Maintenance / Reload RTDB from Remote screen copies the RTDB to the local machine from the mate or remote machine. See **Figure 3-55** .

Figure 3-55. Reload RTDB from Remote Screen



To reload the local RTDB, choose which source you want to reload, and click the Begin RTDB Reload from Remote button. If you attempt to do this while the ELAP is running, you receive the error message in **Figure 3-56** .

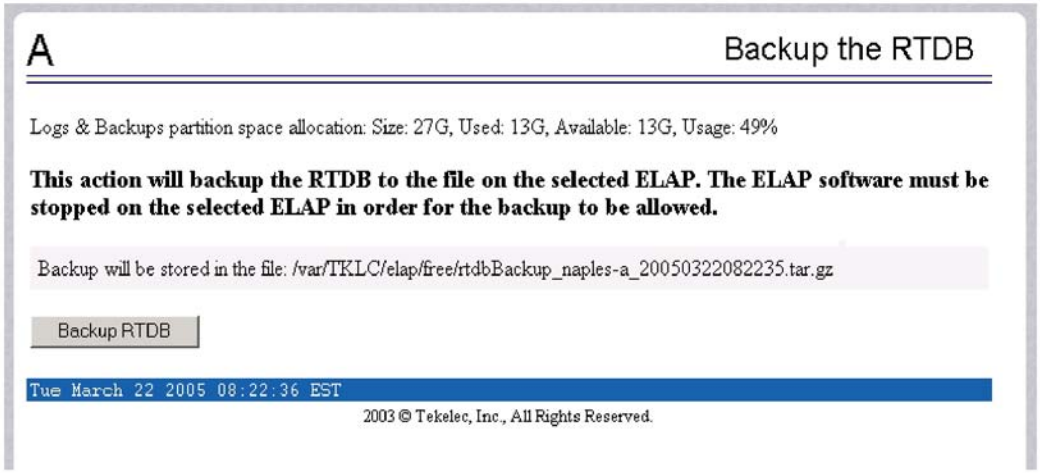
Figure 3-56. Error in Reloading RTDB from Remote Screen



Backup RTDB

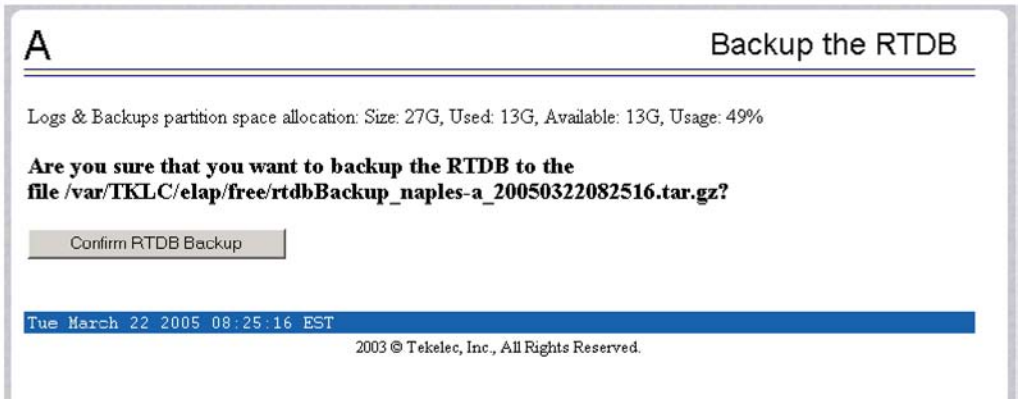
The RTDB / Maintenance / Backup the RTDB screen allows the user to backup the RTDB to a file. This file should then be transfered by Secure File Transfer Protocol (**`sftp`**) to a remote, safe location. The software must be down for the backup to be allowed to ensure that no updates are occurring. See **Figure 3-57** .

Figure 3-57. Backup the RTDB Screen



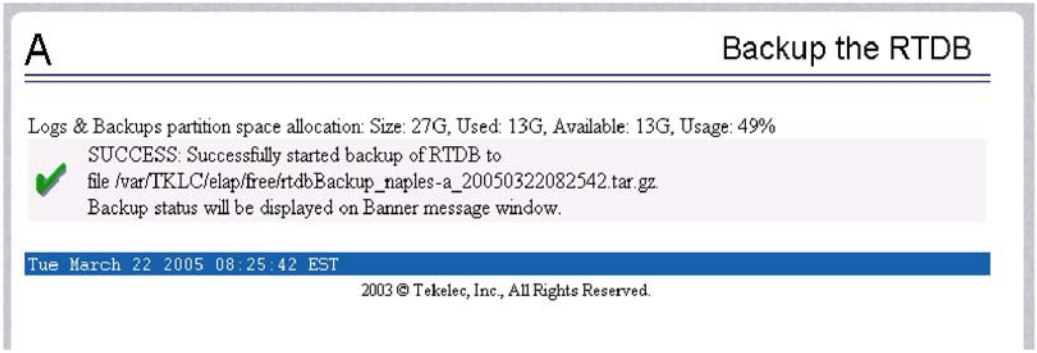
When you are ready to backup the RTDB, stop the selected ELAP software. Click the Backup RTDB button. You are shown a screen to confirm your backup choice in **Figure 3-58** .

Figure 3-58. Confirming the Backup the RTDB Screen



Confirm that you want to perform the backup by clicking the Confirm RTDB Backup button. **Figure 3-59** shows the successful startup of the RTDB backup.

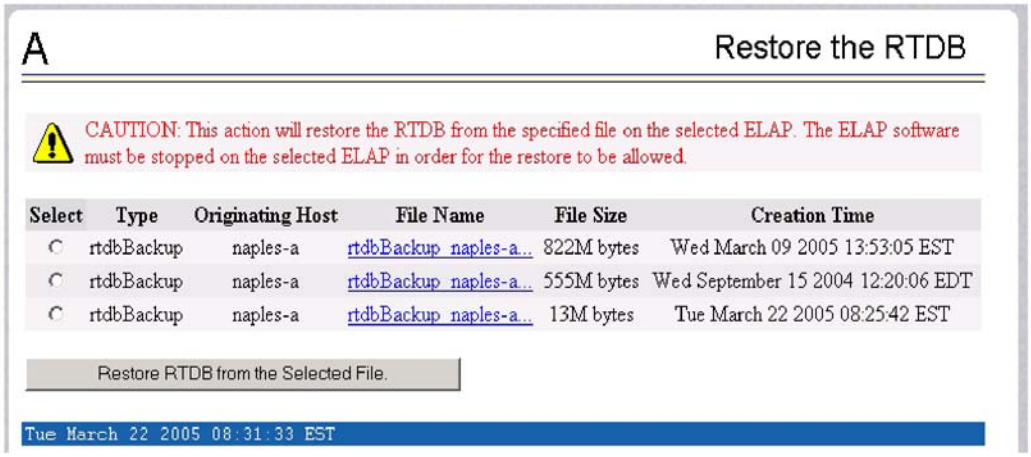
Figure 3-59. Successfully Starting the Backup the RTDB Screen



Restore RTDB

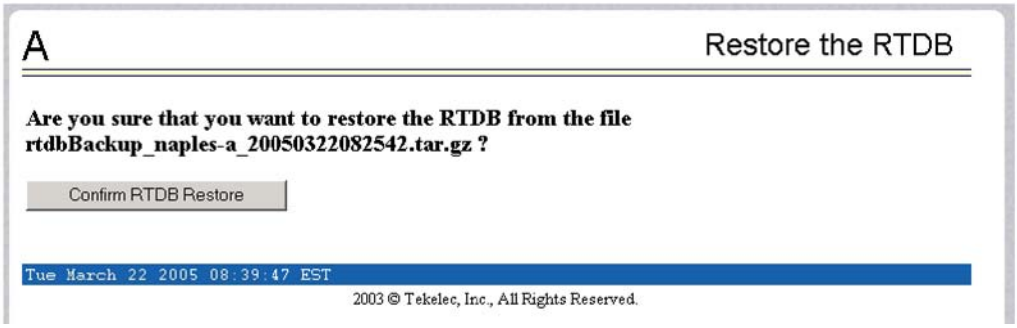
The RTDB / Maintenance / Restore the RTDB screen allows the user to restore the RTDB from an RTDB backup file. The software must be down for the backup to be allowed to ensure that no updates are occurring. Follow the procedure in the *Tekelec 1100 AS MPS Platform Software and Maintenance Manual* to restore the RTDB form a backup file. See **Figure 3-60** .

Figure 3-60. Restore the RTDB



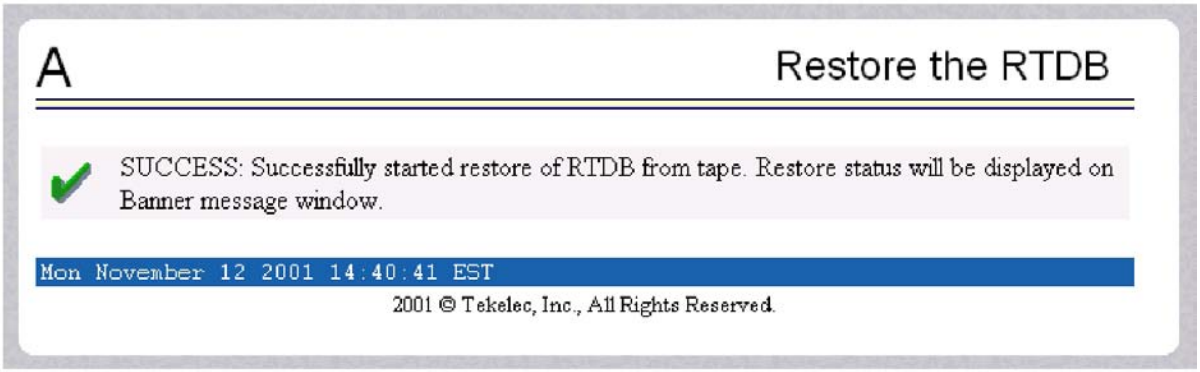
When you are ready to restore the RTDB, prepare the backup media and stop the selected ELAP software. Select the appropriate file and click the Restore RTDB from the Selected File button. You are shown a screen to confirm your restoration choice in **Figure 3-61** .

Figure 3-61. Confirming the Restoration of the RTDB



Confirm that you want to perform the backup by clicking the Confirm RTDB Restore button. **Figure 3-62** shows the successful restoration of the RTDB.

Figure 3-62. Successfully Starting the RTDB Restoration



Retrieve Records Menu

The RTDB / Retrieve Records menu allows the user to retrieve a single subscription record, a single default GTT record, a single override GTT record, a single NPA NXX record, and a service provider record or list all service providers. See **Figure 3-63** for an example of the Retrieve Records menu.

Figure 3-63. Retrieve Records Menu

The RTDB / Retrieve Records menu provides these actions:

- Subscriptions
- Default GTT
- Override GTT
- NPA NXX Split
- Service Providers

Subscriptions

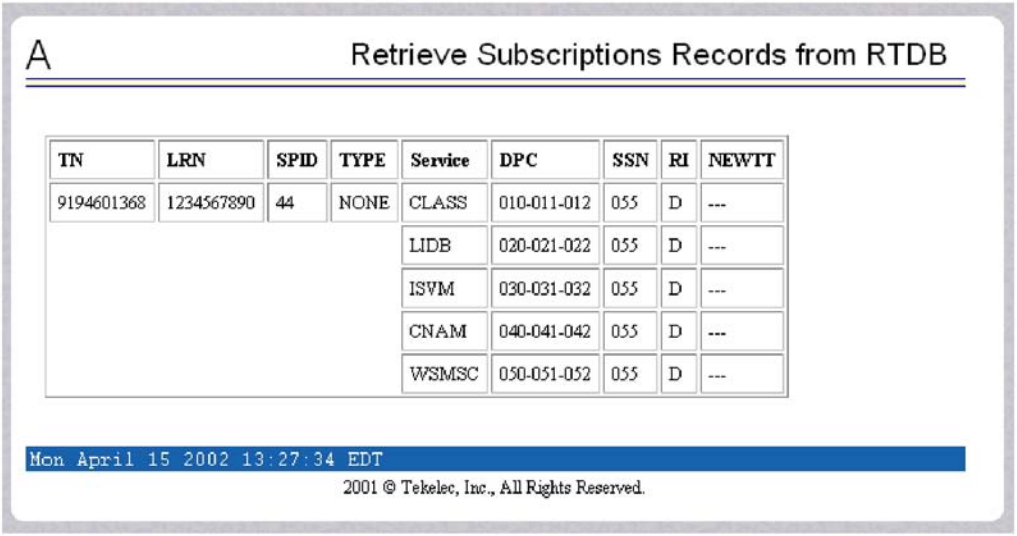
The RTDB / Retrieve Records / Subscriptions menu option lets the user retrieve a single subscription record using a 10-digit subscription as the key. See **Figure 3-64** for the Retrieve Subscription screen.

Figure 3-64. Retrieve Subscriptions Screen

Enter the single ten-digit subscription number in the TN field, and click the Retrieve button.

See **Figure 3-65** for a sample response from the Retrieve Subscription screen.

Figure 3-65. Sample of Retrieve Subscriptions Output

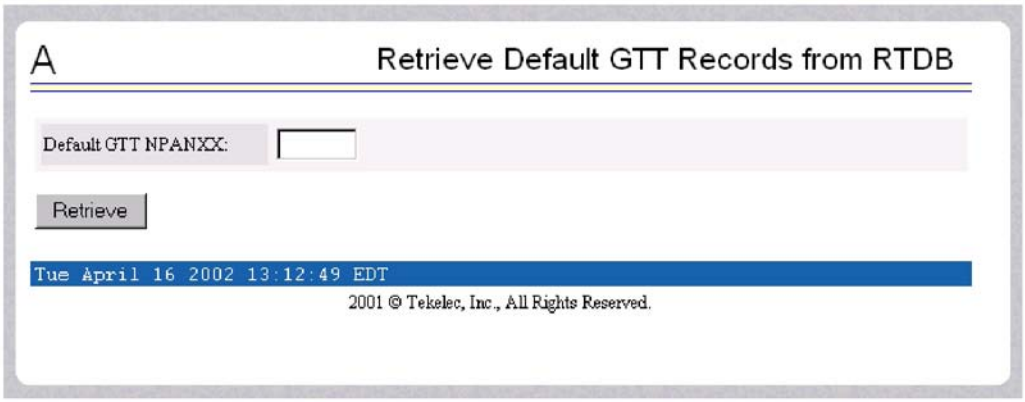


Output Field Descriptions		
Field	**Description**	**Range**
TN	Telephone Number (10 character subscription)	0000000000 - 9999999999 or 0000000*** - 9999999***
LRN	Location Routing Number	0000000000 - 9999999999
SPID	Service Provider ID	4 character alphanumeric
TYPE	LNP Type	NONE, POOL
Service	LNP Service	CLASS, LIDB, ISVM, CNAM, WSMSC
DPC	Destination Point Code	xxx-yyy-zzz where:
		xxx: 000 - 254
		yyy: 000 - 254
		zzz: 000 - 254
SSN	Subsystem Number	000 - 254
RI	Routing Indicator	G, D
NEWTT	New Translation Type	000 - 254

Default GTT

The RTDB / Retrieve Records / Retrieve Default GTT Records from RTDB screen lets you retrieve a single default GTT record using a six-digit NPA NXX number as the key. See **Figure 3-66** for the Retrieve Default GTT Records from GTT screen.

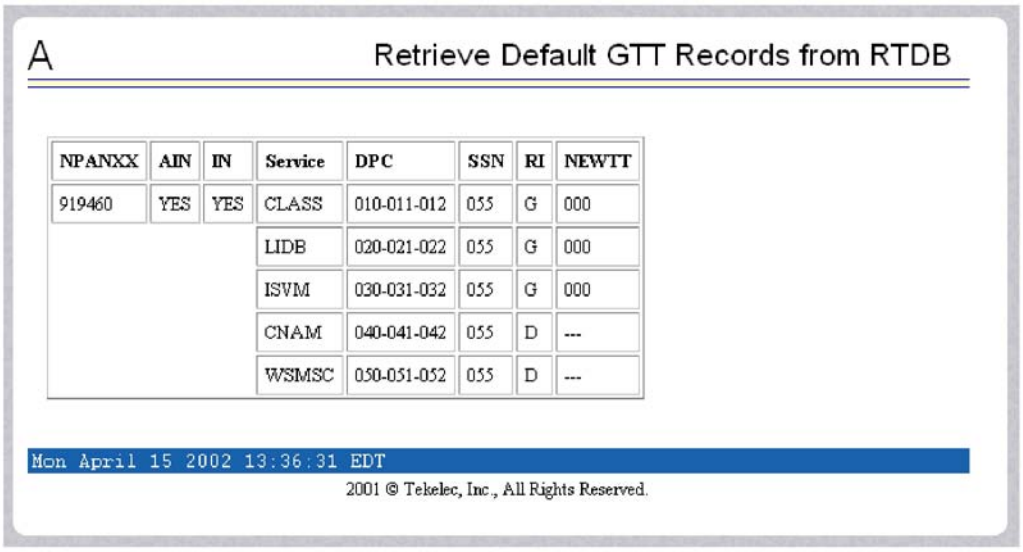
Figure 3-66. Retrieve Default GTT from RTDB



Enter the single NPA NXX number in the Default GTT NPANXX field, and click the Retrieve button.

See **Figure 3-67** for a sample response from the Retrieve Default GTT screen.

Figure 3-67. Sample of Retrieve Default GTT Output



Output Field Descriptions		
Field	**Description**	**Range**
NPANXX	6-digit default GTT	000000 - 999999
AIN	Use Local AIN	YES, NO
IN	Use Local IN	YES, NO
Service	LNP Service	CLASS, LIDB, ISVM, CNAM, WSMSC

DPC	Destination Point Code	xxx-yyy-zzz where:	
		xxx:	000 - 254
		yyy:	000 - 254
		zzz:	000 - 254
SSN	Subsystem Number	000 - 254	
RI	Routing Indicator	G, D	
NEWTT	New Translation Type	000 - 254	

Override GTT

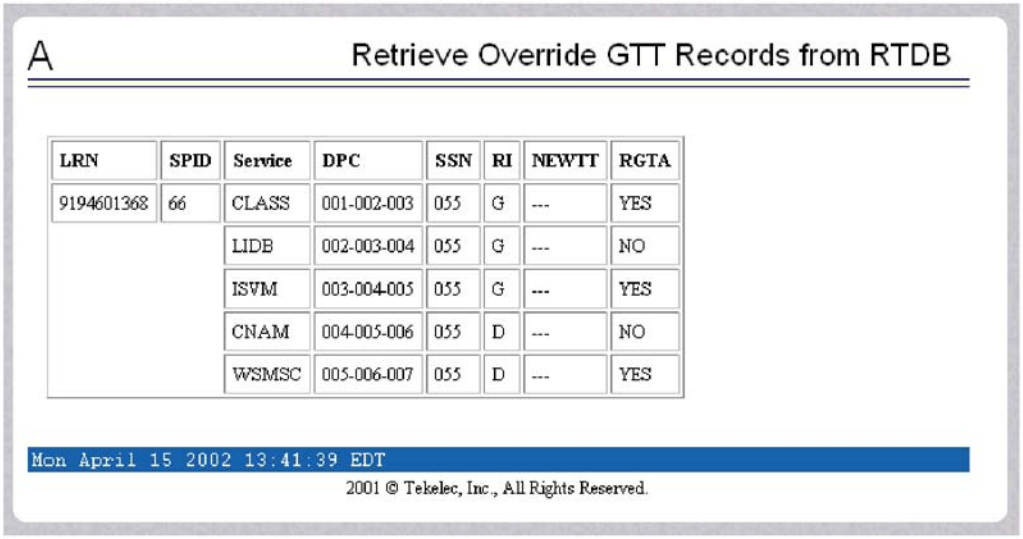
The RTDB / Retrieve Records / Override GTT screen lets the user retrieve a single override GTT record using a 10-digit LRN number as the key. See **Figure 3-68** for the Retrieve Override GTT from RTDB screen.

Figure 3-68. Retrieve Override GTT Screen

Enter the single Location Routing Number in the LRN field, and click the Retrieve button.

See **Figure 3-69** for a sample response from the Retrieve Override GTT screen.

Figure 3-69. Sample of Retrieve Override GTT Output

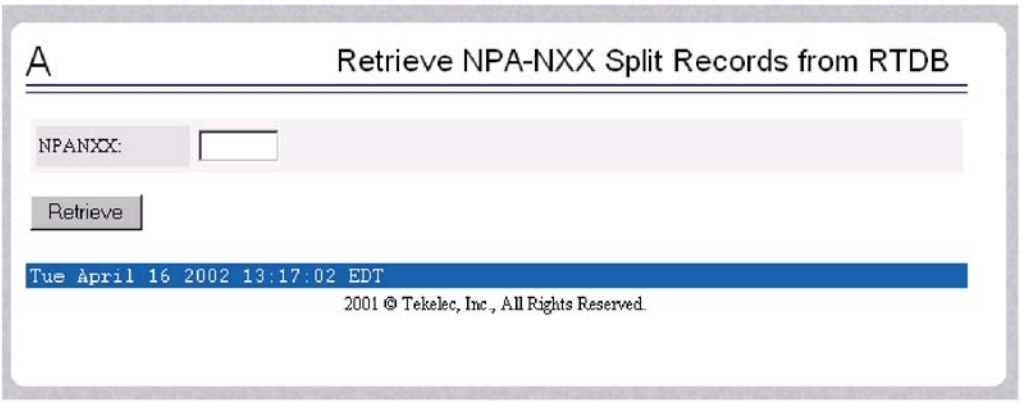


Output Field Descriptions		
Field	**Description**	**Range**
LRN	Location Routing Number	0000000000 - 9999999999
SPID	Service Provider ID	4 character alphanumeric
Service	LNP Service	CLASS, LIDB, ISVM, CNAM, WSMSC
DPC	Destination Point Code	xxx-yyy-zzz where:
		xxx: 000 - 254
		yyy: 000 - 254
		zzz: 000 - 254
SSN	Subsystem Number	000 - 254
RI	Routing Indicator	G, D
NEWTT	New Translation Type	000 - 254
RGTA	Replace Global Title Address with LRN	YES, NO

NPA NXX Split

The RTDB / Retrieve Records / NPA NXX Split screen lets the user retrieve a single split NPA NXX record using a 6-digit NPA NXX number as the key. See **Figure 3-70** for the Retrieve NPA NXX Split Records from RTDB screen.

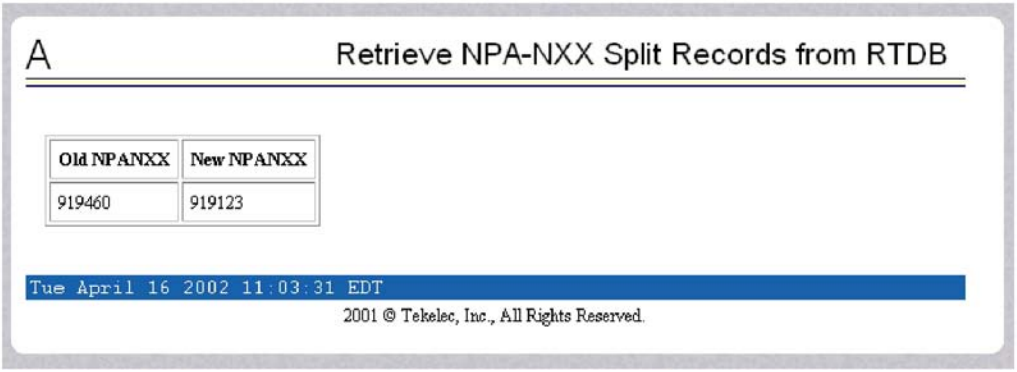
Figure 3-70. Retrieve NPA NXX Split Screen



Enter the single NPA NXX split record number in the Old NPANXX field, and click the Retrieve button.

See **Figure 3-71** for a sample response from the Retrieve NPA NXX Split screen.

Figure 3-71. Sample of Retrieve NPA NXX Split Output



Output Field Descriptions		
Field	**Description**	**Range**
Old NPA NXX	6-digit default GTT	000000 - 999999
New NPA NXX	6-digit default GTT	000000 - 999999

Service Providers

The RTDB / Retrieve Records / Service Providers from RTDB screen lets you retrieve a single service provider record or list all the service providers in the database. See **Figure 3-72** for the Retrieve Service Providers Records from RTDB screen.

Figure 3-72. Retrieve Service Providers Screen

Enter the number in the Service Provider ID field, and click the Retrieve button.

See **Figure 3-73** for a sample response from the Retrieve Service Provider Records from RTDB screen.

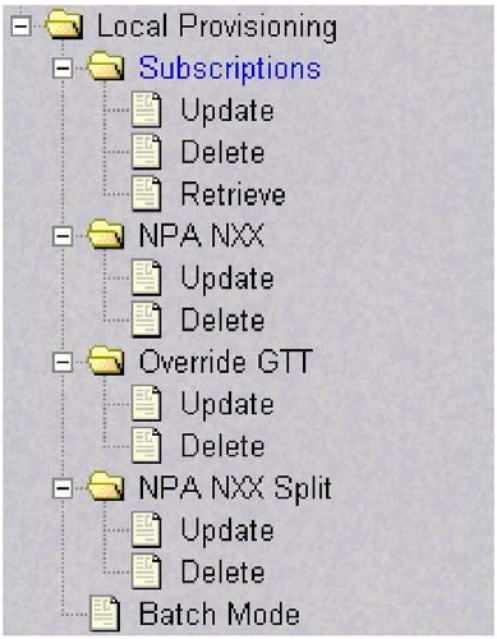
Figure 3-73. Sample of Retrieve Service Providers Output

Output Field Descriptions		
Field	**Description**	**Range**
SP	Service Provider	4 character alphanumeric

Local Provisioning Menu

The RTDB / Local Provisioning menu contains options that let the user provision LNP data directly to the RTDB. This menu contains options for Subscriptions, NPA NXX, Override GTT, and NPA NXX Split. See **Figure 3-74** for the Local Provisioning screen.

Figure 3-74. Local Provisioning Menu



Local Provisioning Utility

The Local Provisioning Utility (LPU) handles customer data received locally. The LPU processes Local Provisioning commands.

If an equipment or communications failure causes the LSMS to be unable to connect to either the local or remote JRS through the JRS's LPU port, the LPU masquerades as an LSMS. This masquerade results in the LPU processing commands in the absence of an LSMS connection. When such a failure happens, the LPU takes control of both JRS LSMS ports and sends a timestamp request to the local side, which allows LPU to connect to the local JRS's LPU port. It controls both ports to eliminate the possibility of LSMS reconnecting to the other port and causing synchronization problems.

The Retrieve Records and Local Provisioning commands have a checkbox option:

```
Process command even if connection to remote LSMS port not possible (use option with care).
```

The user checks this option to allow the LPU to masquerade by connecting to only the local JRS's LSMS port.

CAUTION: Manually applying updates to the ELAP RTDB using the LPU can result in LSMS and ELAP databases that are not synchronized (contain different data).

The RTDB / Local Provisioning menu provides these actions:

- Subscriptions
- NPA NXX Menu
- Override GTT Menu
- NPA NXX Split Menu

- Batch Mode

Subscriptions

The RTDB / Local Provisioning / Subscriptions menu options lets you update, delete, and retrieve LNP data directly to the RTDB. See **Figure 3-75** for the Local Provisioning /Subscriptions menu.

Figure 3-75. Local Provisioning / Subscriptions Menu

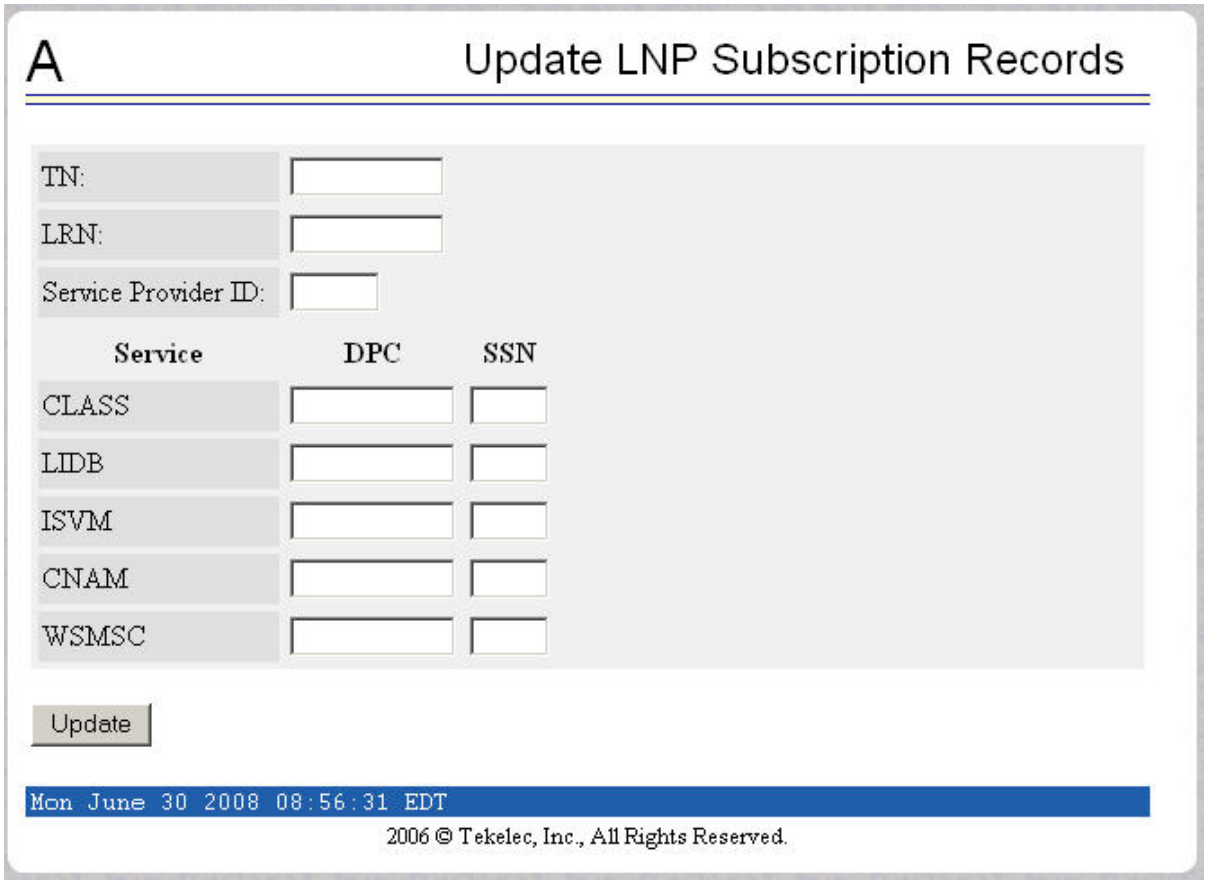
The RTDB / Local Provisioning /Subscriptions menu provides these actions:

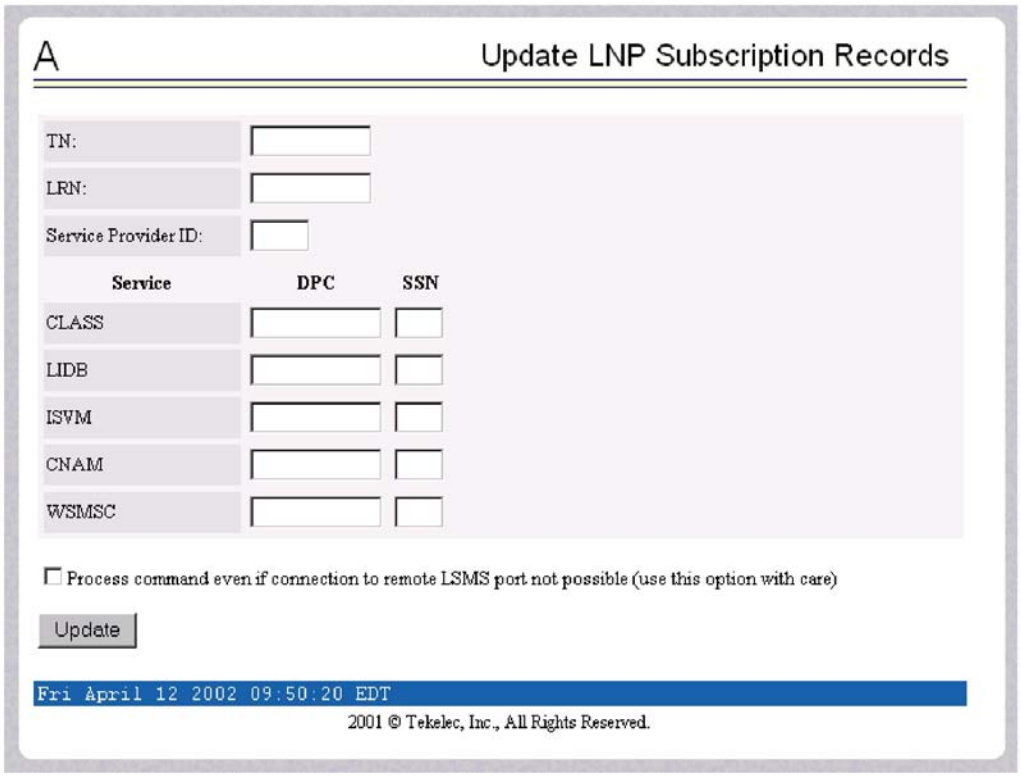
- Subscriptions / Update
- Subscriptions / Delete
- Subscriptions / Retrieve

Subscriptions / Update

The RTDB / Local Provisioning /Subscriptions / Update LNP Subscription Records screen lets the user update values for a specific subscription using a 10-digit subscription number as a key. See **Figure 3-76** for the RTDB / Local Provisioning / Subscriptions / Update LNP Subscription Records screen.

Figure 3-76. Update LNP Subscriptions Records



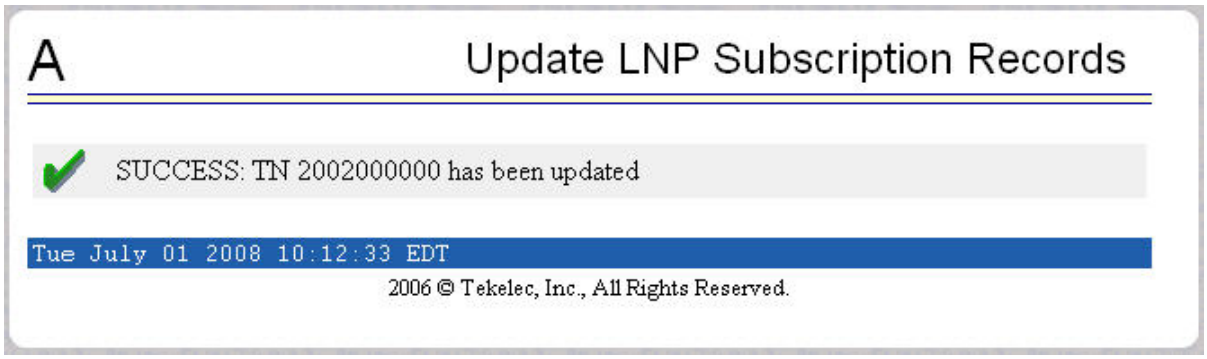


Enter the required information in the fields shown, and click the Update button.

NOTE: Do not check the 'Process command even if connection to remote LSMS port not possible' button unless you thoroughly understand the material in Introduction .

See **Figure 3-77** for a list of sample responses from the Update Subscriptions option screen.

Figure 3-77. Sample of Updating LNP Subscription Records Output

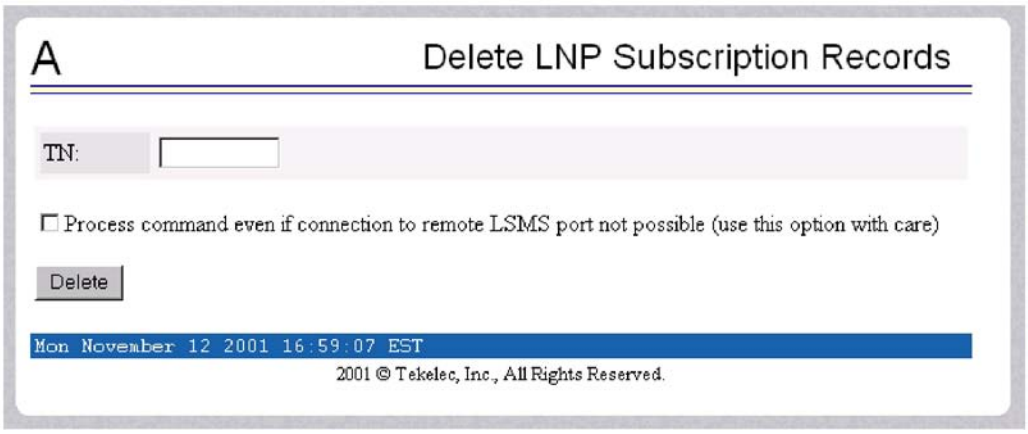


- Connected to local LSMS port on X.X.X.X
- Connected to remote LSMS port on Y.Y.Y.Y
- Connected to LPU port on Z.Z.Z.Z
- Could not connect to LPU port. Do you wish to connect and try to send the command again? [N]:
- Could not connect to local LSMS port
- Could not connect to remote LSMS port. Do you wish to connect and try to send the command again? [N]:

Subscriptions / Delete

The RTDB / Local Provisioning /Subscriptions / Delete LNP Subscription Records screen lets the user delete a specific subscription record using a 10-digit subscription number as a key. See **Figure 3-78** for the RTDB / Local Provisioning / Subscriptions / Delete LNP Subscription Records screen.

Figure 3-78. Delete LNP Subscripting



Enter the single ten-digit subscription number in the TN field, and click the Retrieve button.

NOTE: Do not check the 'Process command even if connection to remote LSMS port not possible' button unless you thoroughly understand the material in Introduction .

See **Figure 3-79** for a list of sample responses from the Delete Subscriptions option screen.

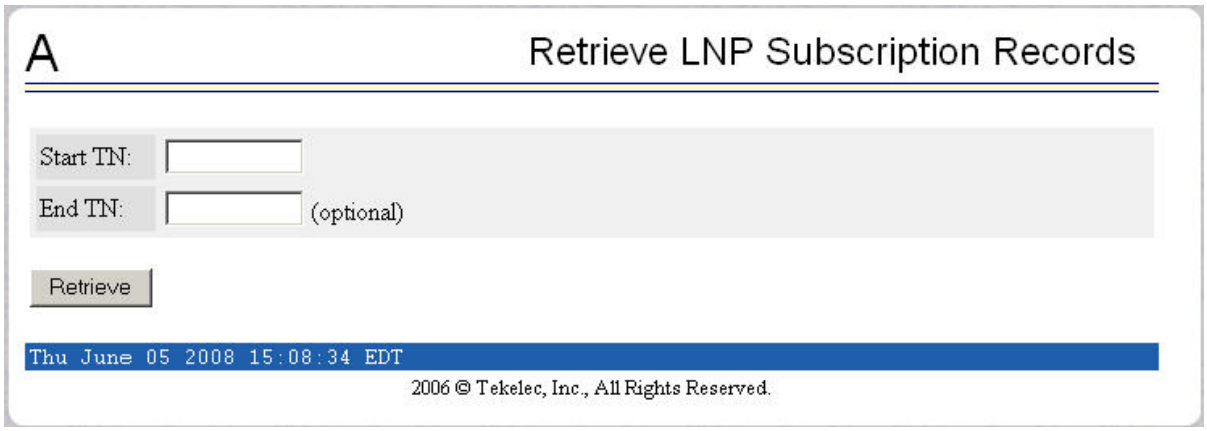
Figure 3-79. Sample of Delete Subscription Output

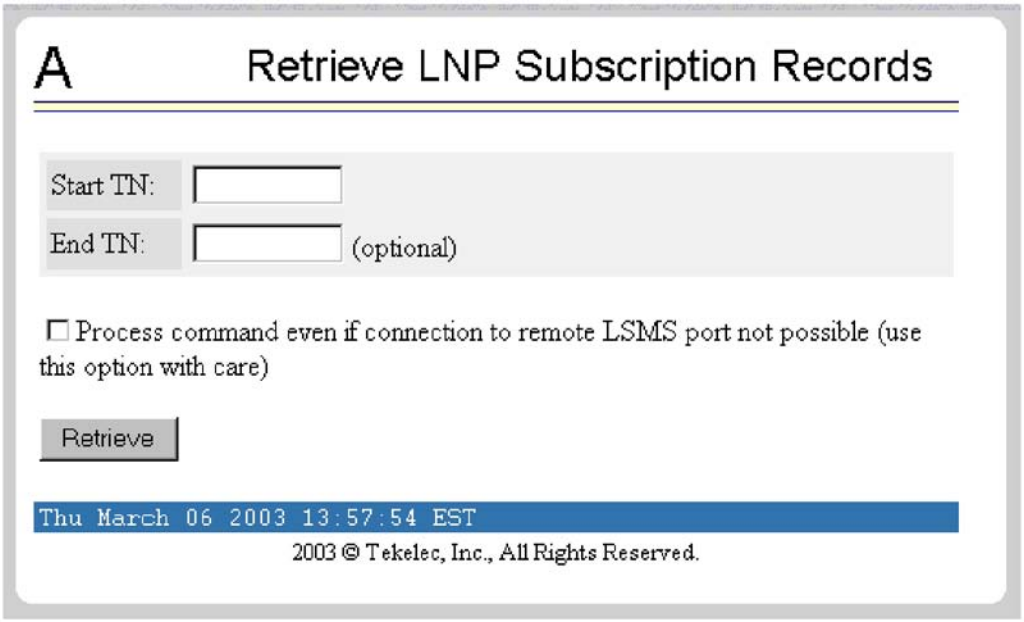
- Connected to local LSMS port on X.X.X.X
- Connected to remote LSMS port on Y.Y.Y.Y
- Connected to LPU port on Z.Z.Z.Z
- Could not connect to LPU port. Do you wish to connect and try to send the command again? [N]:
- Could not connect to local LSMS port
- Could not connect to remote LSMS port. Do you wish to connect and try to send the command again? [N]:

Subscriptions / Retrieve

The RTDB / Local Provisioning /Subscriptions / Retrieve LNP Subscription Records screen lets the user retrieve a specific subscription record using a 10-digit subscription number as a key. See **Figure 3-80** for the Local Provisioning / Subscriptions / Retrieve LNP Subscription Records screen.

Figure 3-80. Retrieve LNP Subscripting



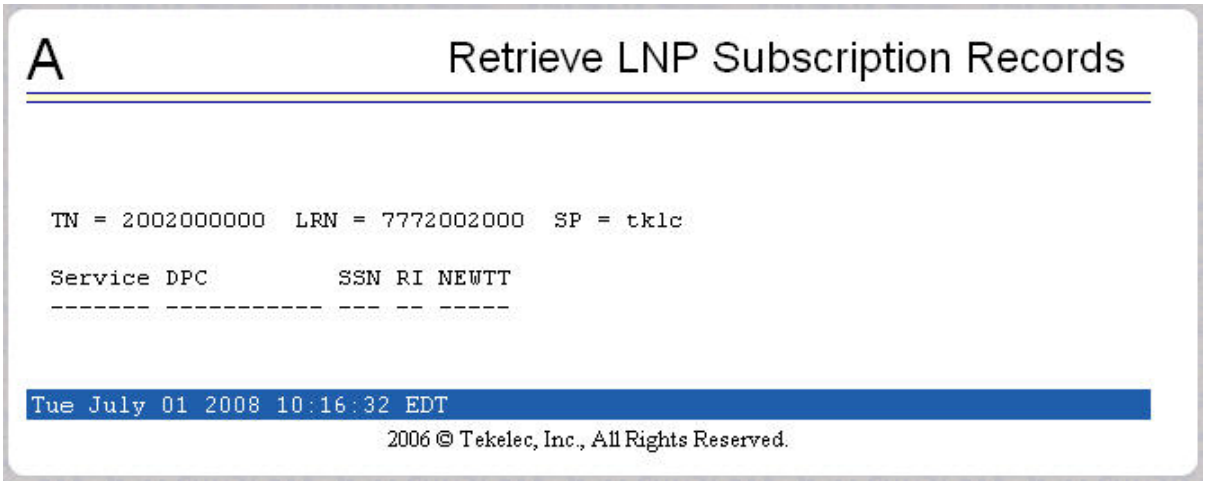


Enter the single ten-digit subscription number in the TN field, and click the Retrieve button.

NOTE: Do not check the 'Process command even if connection to remote LSMS port not possible' button unless you thoroughly understand the material in Introduction .

See **Figure 3-81** for a list of sample responses from the Retrieve Subscriptions option screen.

Figure 3-81. Sample of Retrieve Subscription Output

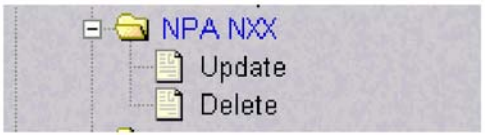


- Connected to local LSMS port on X.X.X.X
- Connected to remote LSMS port on Y.Y.Y.Y
- Connected to LPU port on Z.Z.Z.Z
- Could not connect to LPU port. Do you wish to connect and try to send the command again? [N]:
- Could not connect to local LSMS port
- Could not connect to remote LSMS port. Do you wish to connect and try to send the command again? [N]:

NPA NXX Menu

The RTDB / Local Provisioning / NPA NXX menu lets you update and delete a single NPA NXX record directly to the RTDB. See **Figure 3-82** for the RTDB / Local Provisioning / NPA NXX screen.

Figure 3-82. RTDB / Local Provisioning / NPA NXX Menu



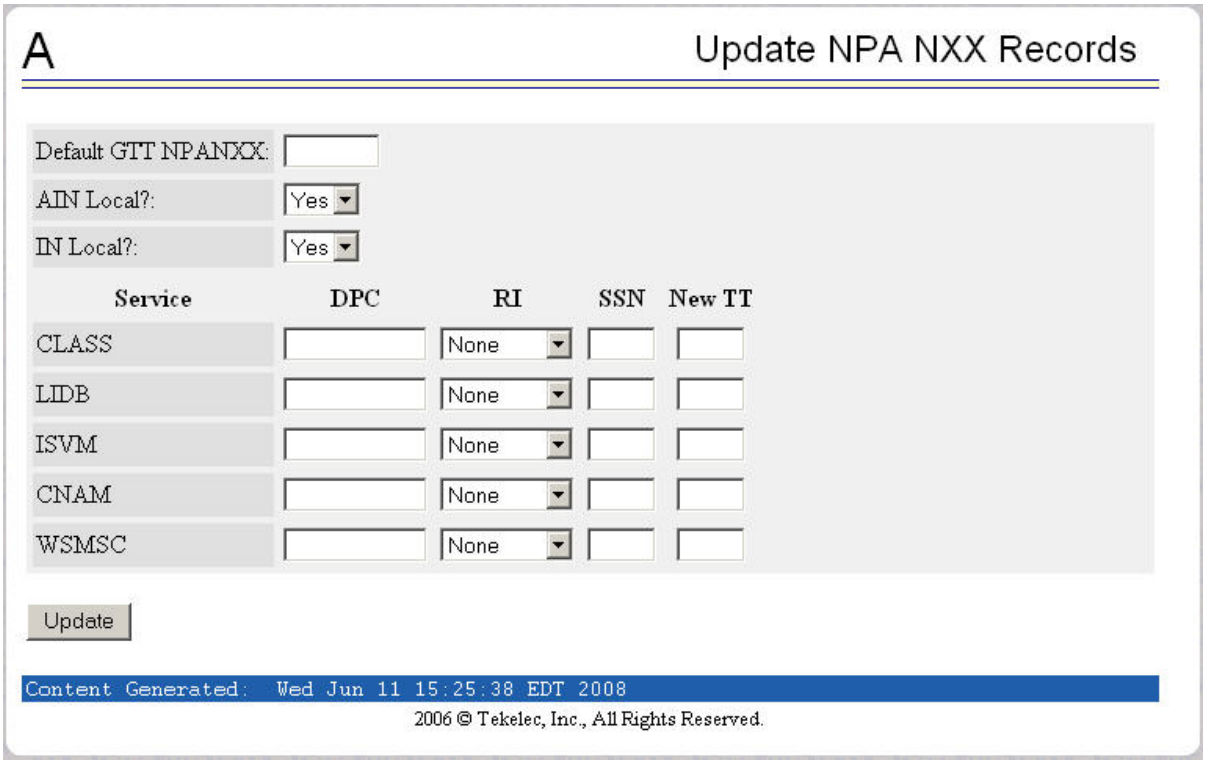
The RTDB / Local Provisioning / NPA NXX menu provides these actions:

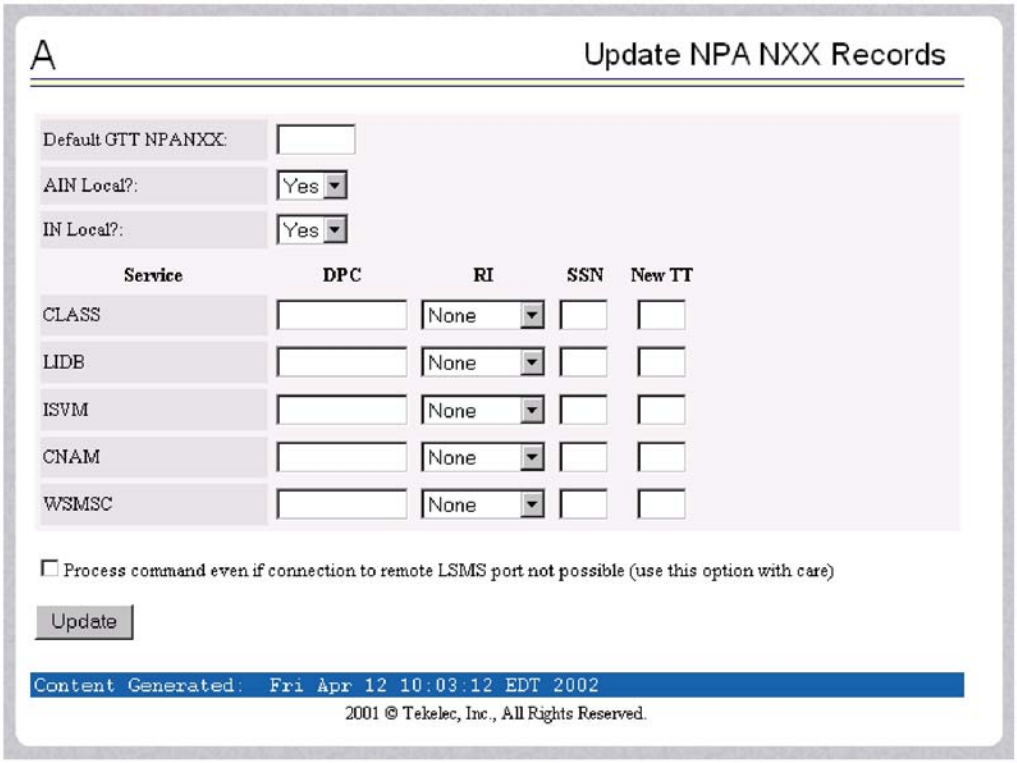
- NPA NXX / Update
- NPA NXX / Delete

NPA NXX / Update

The RTDB / Local Provisioning / NPA NXX / Update NPA NXX Records screen lets you update values for a specific NPA NXX record using a 6-digit subscription number as a key. See **Figure 3-83** for the Local Provisioning / Subscriptions / Update NPA NXX Records screen.

Figure 3-83. Update NPA NXX Records





Enter the required information in the fields shown, and click the **Update** button.

NOTE: Do not check the 'Process command even if connection to remote LSMS port not possible' button unless you thoroughly understand the material in Local Provisioning Utility .

See Figure 3-84 for a list of sample responses from the Update NPA NXX Records option screen.

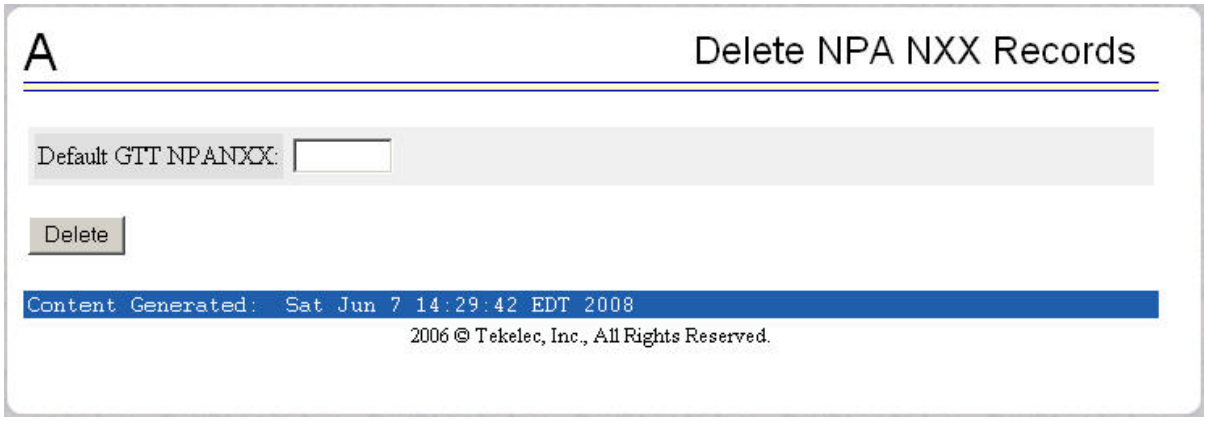
Figure 3-84. Samples of Update NPA NXX Records Output

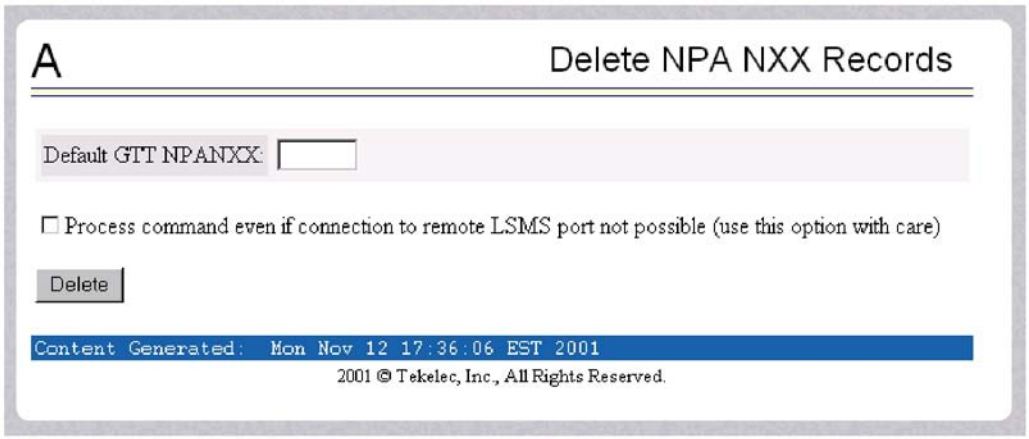
- `Connected to local LSMS port on X.X.X.X`
- `Connected to remote LSMS port on Y.Y.Y.Y`
- `Connected to LPU port on Z.Z.Z.Z`
- `Could not connect to LPU port. Do you wish to connect and try to send the command again? [N]:`
- `Could not connect to local LSMS port`
- `Could not connect to remote LSMS port. Do you wish to connect and try to send the command again? [N]:`

NPA NXX / Delete

The RTDB / Local Provisioning / NPA NXX / Delete NPA NXX Records screen lets you delete values for a specific NPA NXX record using a 6-digit subscription number as a key. See Figure 3-85 for the RTDB / Local Provisioning / NPA NXX / Delete NPA NXX Records screen.

Figure 3-85. Delete NPA NXX Records





Enter the single NPA NXX number in the **Default GTT NPANXX** field, and click the **Delete** button.

NOTE: Do not check the 'Process command even if connection to remote LSMS port not possible' button unless you thoroughly understand the material in Local Provisioning Utility .

See **Figure 3-86** for a list of sample responses from the Update NPA NXX Records option screen.

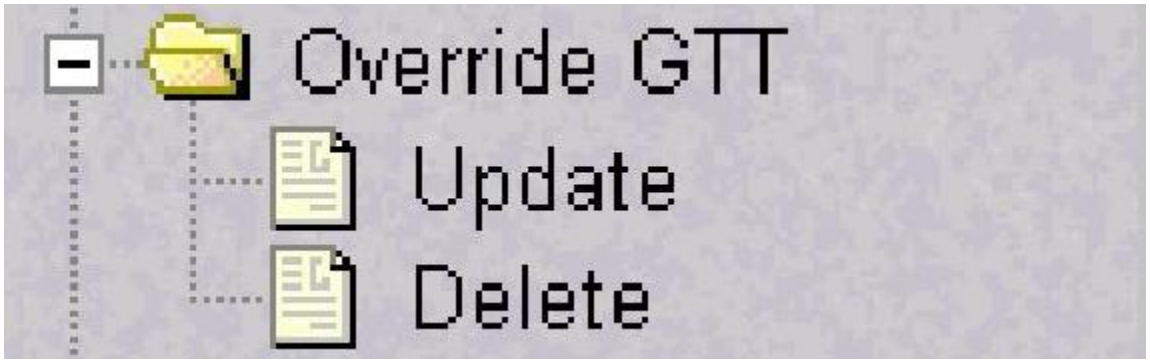
Figure 3-86. Samples of Delete NPA NXX Records Output

- `Connected to local LSMS port on X.X.X.X`
- `Connected to remote LSMS port on Y.Y.Y.Y`
- `Connected to LPU port on Z.Z.Z.Z`
- `Could not connect to LPU port. Do you wish to connect and try to send the command again? [N]:`
- `Could not connect to local LSMS port`
- `Could not connect to remote LSMS port. Do you wish to connect and try to send the command again? [N]:`

Override GTT Menu

The RTDB / Local Provisioning / Override GTT menu lets you update and delete a single LRN (Location Routing Number) record directly to the RTDB. See **Figure 3-87** for the RTDB / Local Provisioning / Override GTT menu.

Figure 3-87. RTDB / Local Provisioning / Override GTT Menu



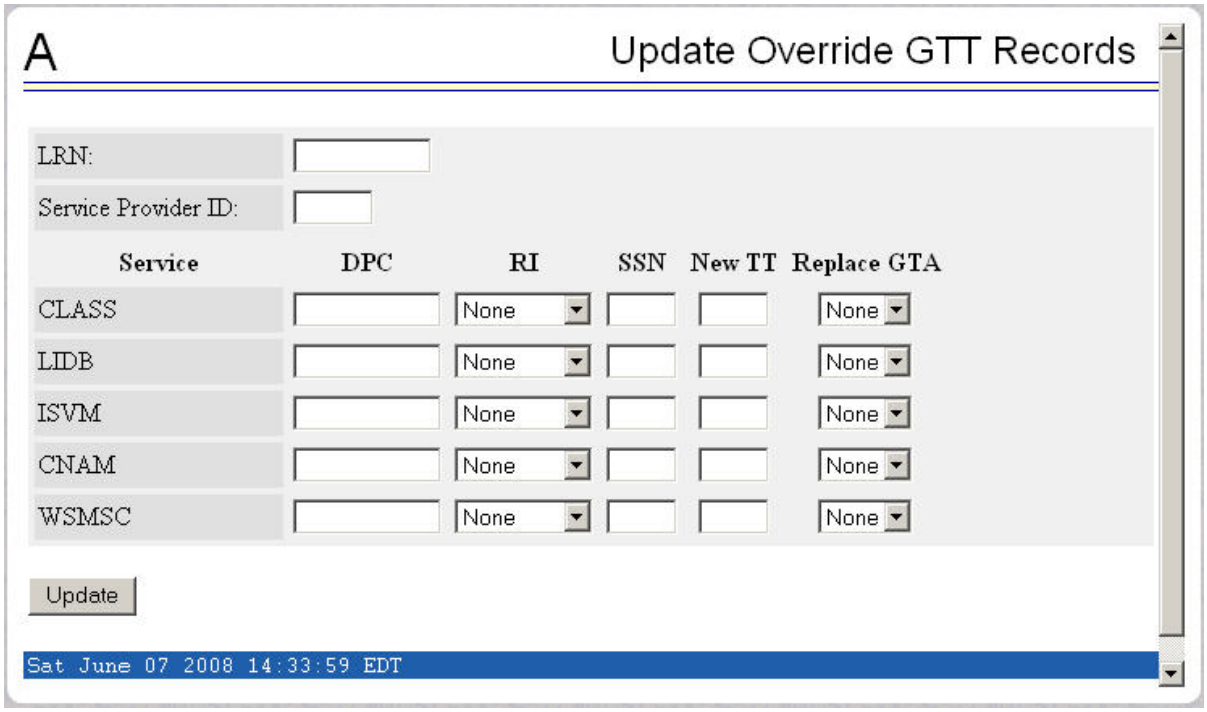
The RTDB / Local Provisioning / Override GTT menu provides these actions:

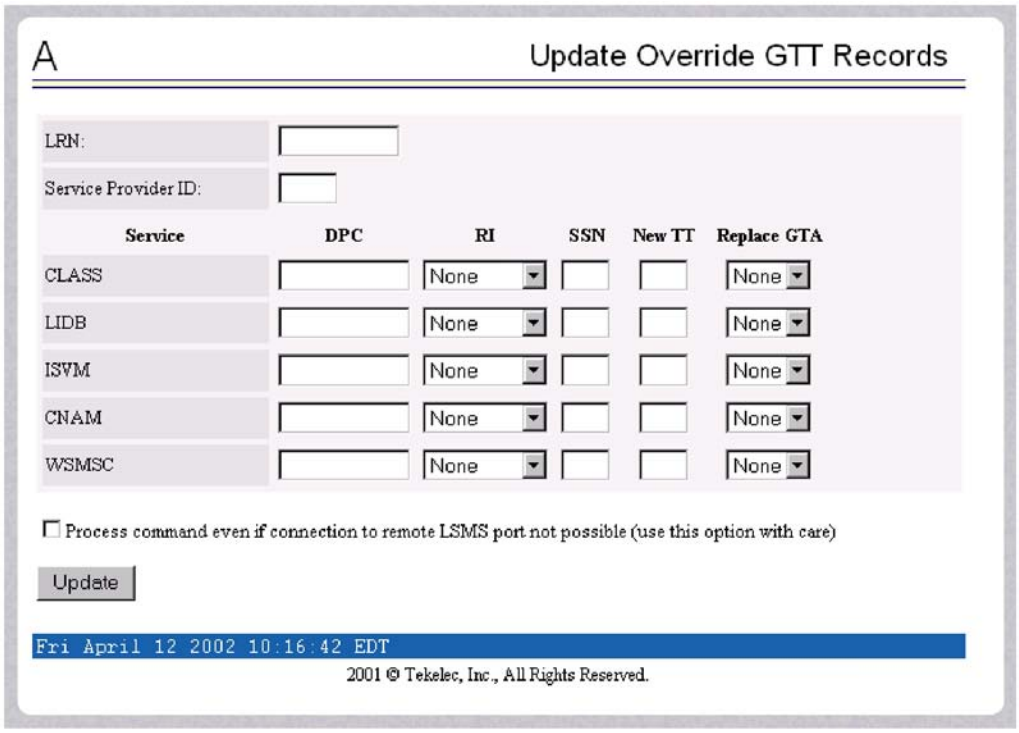
- Override GTT / Update
- Override GTT / Delete

Override GTT / Update

The RTDB / Local Provisioning / Override GTT / Update Override GTT Records screen lets the user update values for a specific LRN record using a 10-digit LRN number as a key. See **Figure 3-88** for the Local Provisioning / Override GTT / Update Override GTT Records screen.

Figure 3-88. Update Override GTT Records





Enter the required information in the fields shown, and click the **Update** button.

NOTE: Do not check the 'Process command even if connection to remote LSMS port not possible' button unless you thoroughly understand the material in Local Provisioning Utility .

See **Figure 3-89** for a list of sample responses from the Update Override GTT Records option screen.

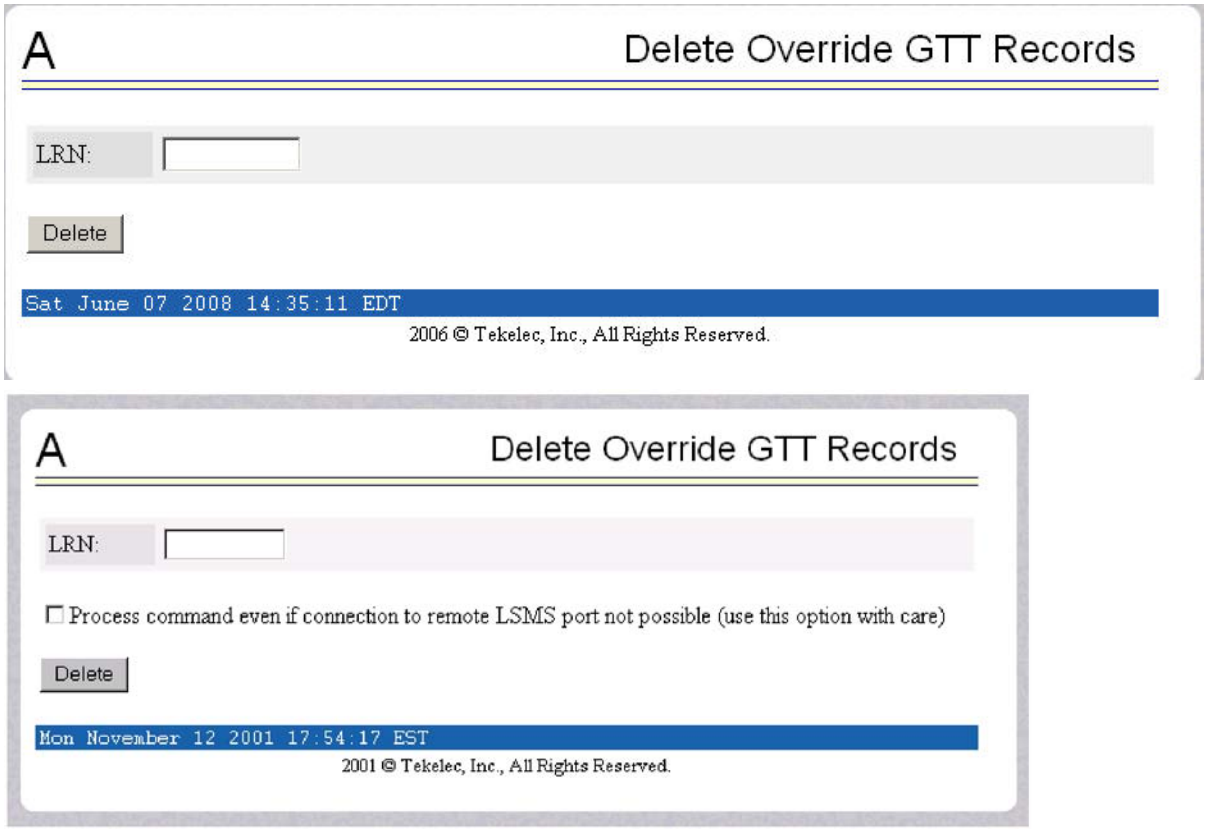
Figure 3-89. Samples of Update Override GTT Record Output

- Connected to local LSMS port on X.X.X.X
- Connected to remote LSMS port on Y.Y.Y.Y
- Connected to LPU port on Z.Z.Z.Z
- Could not connect to LPU port. Do you wish to connect and try to send the command again? [N]:
- Could not connect to local LSMS port
- Could not connect to remote LSMS port. Do you wish to connect and try to send the command again? [N]:

Override GTT / Delete

The RTDB / Local Provisioning / Override GTT / Delete Override GTT Records screen lets you delete a specific LRN record using a 10-digit LRN number as a key. See **Figure 3-90** for the Local Provisioning / Subscriptions / Delete Override GTT Records screen.

Figure 3-90. Delete Override GTT Record



Enter the specific Location Routing Number in the **LRN** field, and click the **Delete** button.

NOTE: Do not check the 'Process command even if connection to remote LSMS port not possible' button unless you thoroughly understand the material in Local Provisioning Utility .

See **Figure 3-91** for a list of sample responses from the Delete Override GTT Record option screen.

Figure 3-91. Samples of Delete Override GTT Record Output

- Connected to local LSMS port on X.X.X.X
- Connected to remote LSMS port on Y.Y.Y.Y
- Connected to LPU port on Z.Z.Z.Z
- Could not connect to LPU port. Do you wish to connect and try to send the command again? [N]:
- Could not connect to local LSMS port
- Could not connect to remote LSMS port. Do you wish to connect and try to send the command again? [N]:

NPA NXX Split Menu

The RTDB / Local Provisioning / NPA NXX Split menu lets you update and delete a single Split NPA NXX record directly to the RTDB. See **Figure 3-92** for the RTDB / Local Provisioning /Subscriptions / NPA NXX screen.

Figure 3-92. RTDB / Local Provisioning / NPA NXX Split Menu

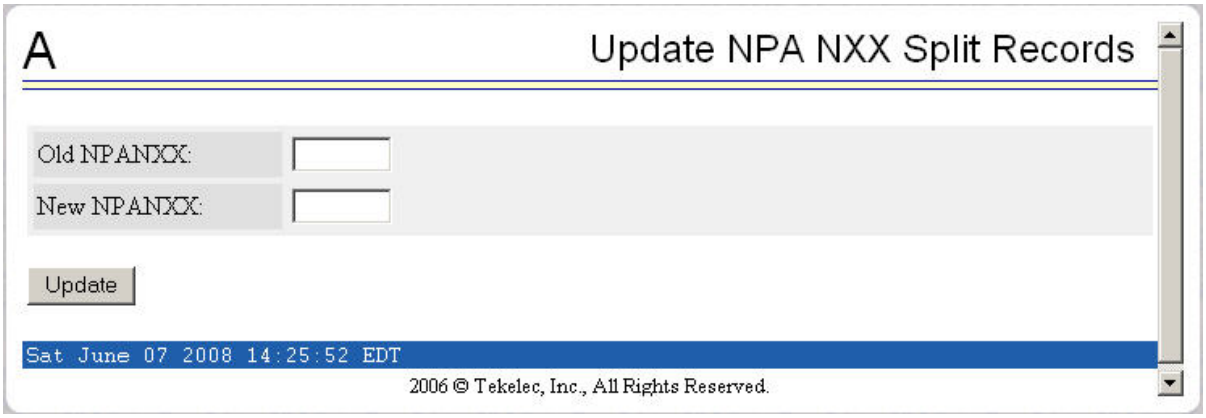
The RTDB / Local Provisioning / NPA NXX Split menu provides these actions:

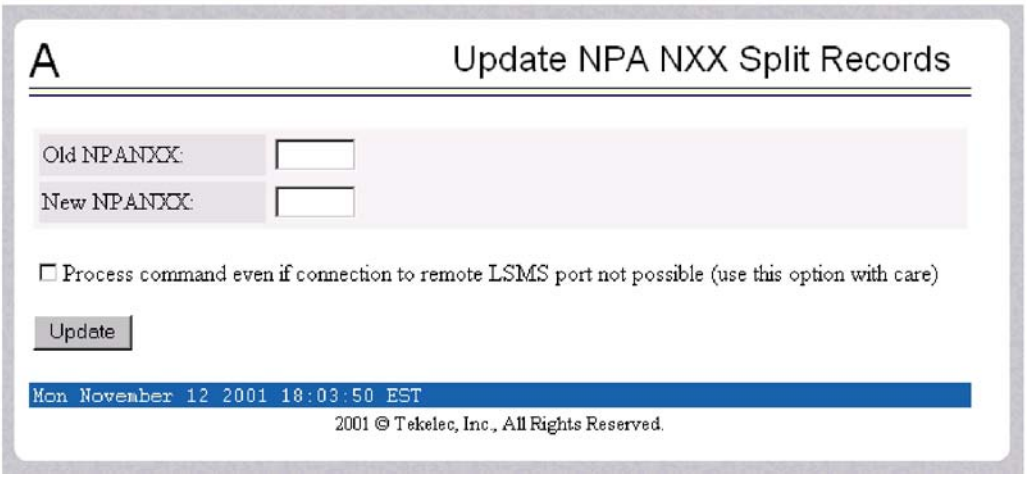
- NPA NXX Split / Update
- NPA NXX Split / Delete

NPA NXX Split / Update

The RTDB / Local Provisioning / NPA NXX Split / Update NPA NXX Split Records screen lets you update values for a single Split NPA NXX record using a 6-digit NPA NXX number as a key.

Figure 3-93. Update NPA NXX Split Records





Enter the required information in the fields shown, and click the **Update** button.

NOTE: Do not check the 'Process command even if connection to remote LSMS port not possible' button unless you thoroughly understand the material in Local Provisioning Utility .

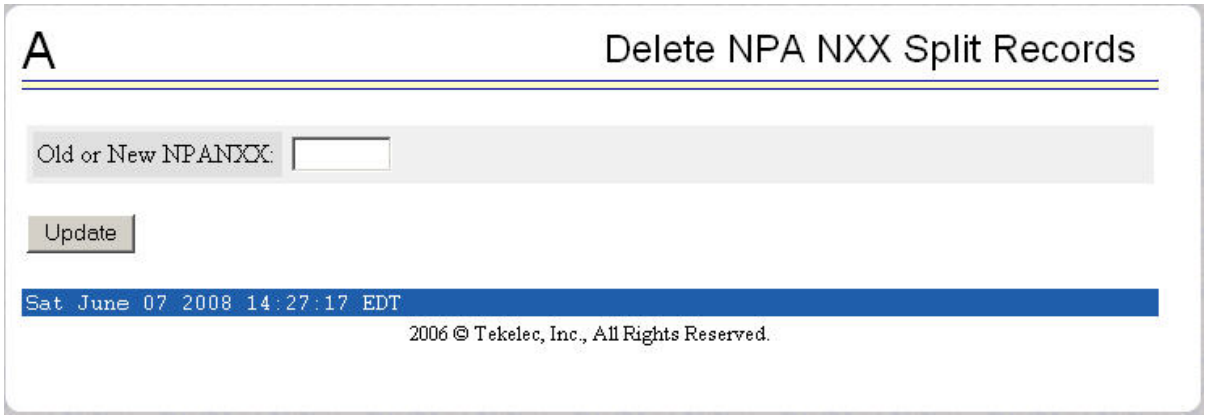
Figure 3-94. Samples of Update NPA NXX Split Record Output

- Success - New NPA NXX: 910345
- Connected to local LSMS port on X.X.X.X
- Connected to remote LSMS port on Y.Y.Y.Y
- Connected to LPU port on Z.Z.Z.Z
- Could not connect to LPU port. Do you wish to connect and try to send the command again? [N]:
- Could not connect to local LSMS port
- Could not connect to remote LSMS port. Do you wish to connect and try to send the command again? [N]:

NPA NXX Split / Delete

The RTDB / Local Provisioning / NPA NXX Split / Delete screen lets the user delete a single Split NPA NXX record using a 6-digit NPA NXX number as a key.

Figure 3-95. Delete NPA NXX Split Record



Enter the single Split NPA NXX record using a 6-digit NPA NXX number in the **Old or New NPANXX** field, and click the **Update** button.

NOTE: Do not check the 'Process command even if connection to remote LSMS port not possible' button unless you thoroughly understand the material in Local Provisioning Utility .

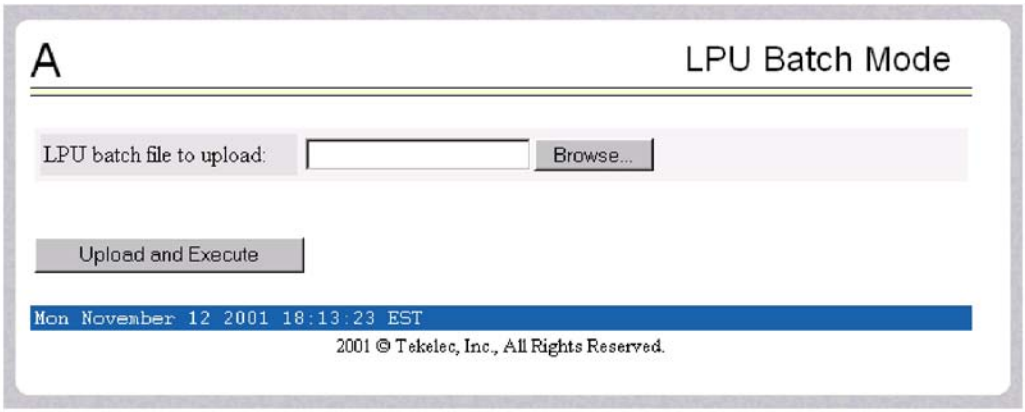
Figure 3-96. Samples of Delete NPA NXX Split Record Output

- `Connected to local LSMS port on X.X.X.X`
- `Connected to remote LSMS port on Y.Y.Y.Y`
- `Connected to LPU port on Z.Z.Z.Z`
- `Could not connect to LPU port. Do you wish to connect and try to send the command again? [N]:`
- `Could not connect to local LSMS port`
- `Could not connect to remote LSMS port. Do you wish to connect and try to send the command again? [N]:`

Batch Mode

The RTDB / Local Provisioning / Batch Mode screen lets you upload an LPU batch file for local provisioning. See **Figure 3-97** for the RTDB / Local Provisioning / Batch Mode screen.

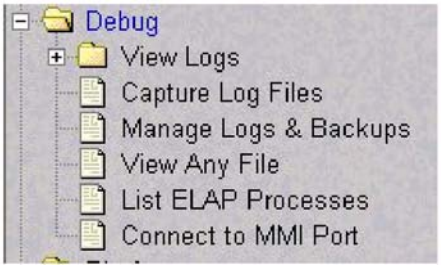
Figure 3-97. RTDB/Local Provisioning/Batch Mode Screen



Debug Menu

The Debug Menu allows the user to view logs, list running processes, and access the EAGLE 5 ISSMMI port.

Figure 3-98. Debug Menu



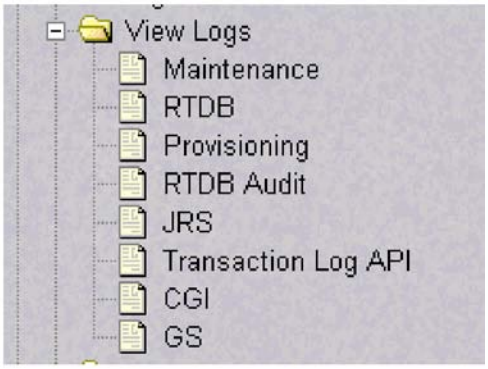
The Debug menu provides the following actions:

- LINK
- Capture Log Files
- LINK
- LINK
- List ELAP Software Processes
- LINK

View Logs Menu

The Debug / View Logs menu allows the user to view such logs as the Maintenance, RTDB, Provisioning, RTDB audit, and UI logs. See the View Logs menu in **Figure 3-99** .

Figure 3-99. View Logs Menu



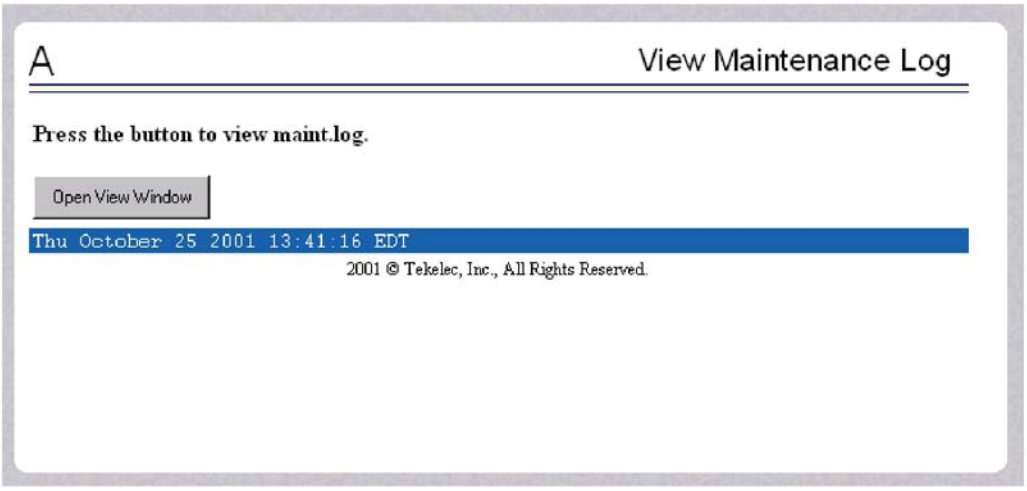
The View Logs menu provides the following actions:

- Maintenance Log
- RTDB, Provisioning, RTDB Audit, JRS, Transaction Log API, CGI and GS Logs

Maintenance Log

When you click Debug / View Logs / Maintenance in **Figure 3-99** , you see the View Maintenance Log screen, shown in **Figure 3-100** . Press the Open View Window button to activate the View Window viewer and see the Maintenance Log.

Figure 3-100. View Maintenance Log Screen



Selecting the Maintenance Log in this window displays the requested log in the log viewer window. For details about using this utility, see ELAP Log Viewer .

RTDB, Provisioning, RTDB Audit, JRS, Transaction Log API, CGI and GS Logs

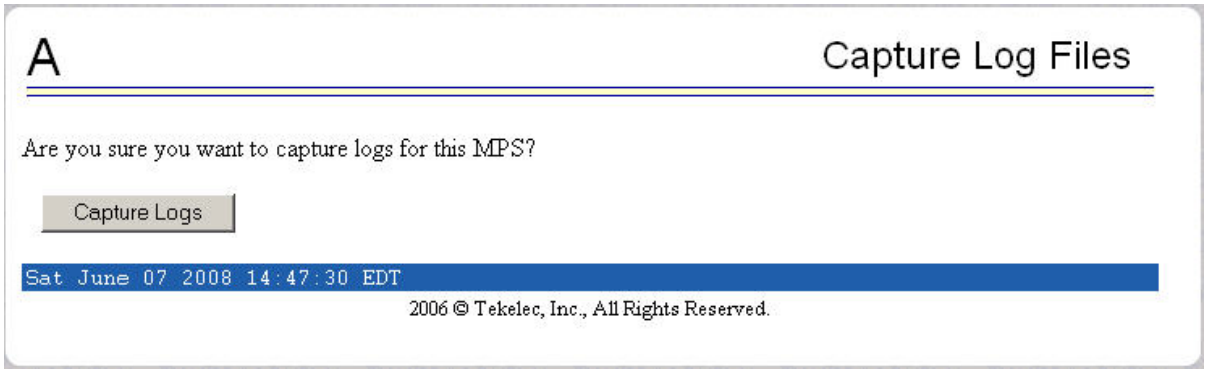
When you choose to view any of the Debug / View Logs files, the process is the same as for the Maintenance Log described previously. The selection you choose causes a screen similar to the View Maintenance Log screen in **Figure 3-100** . Press the Open View Window button to activate the View Window viewer for the log file you have selected in the View Logs menu.

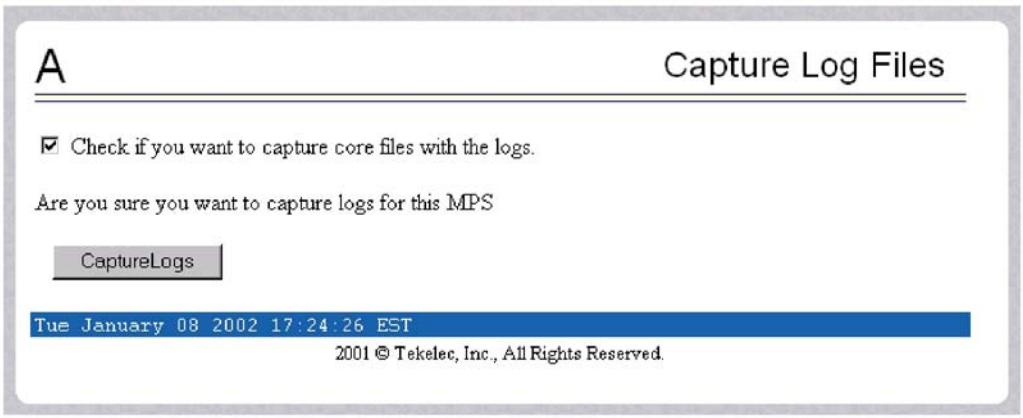
Opening any log in this window displays the requested log in the log viewer window. All log files are viewed with the same file viewing utility. For details about this utility, see ELAP Log Viewer .

Capture Log Files

The Debug / Capture Log Files screen allows the user to make a copy of the logs for the current MPS. Optionally, you can capture files with the logs.

Figure 3-101. Capture Log Files





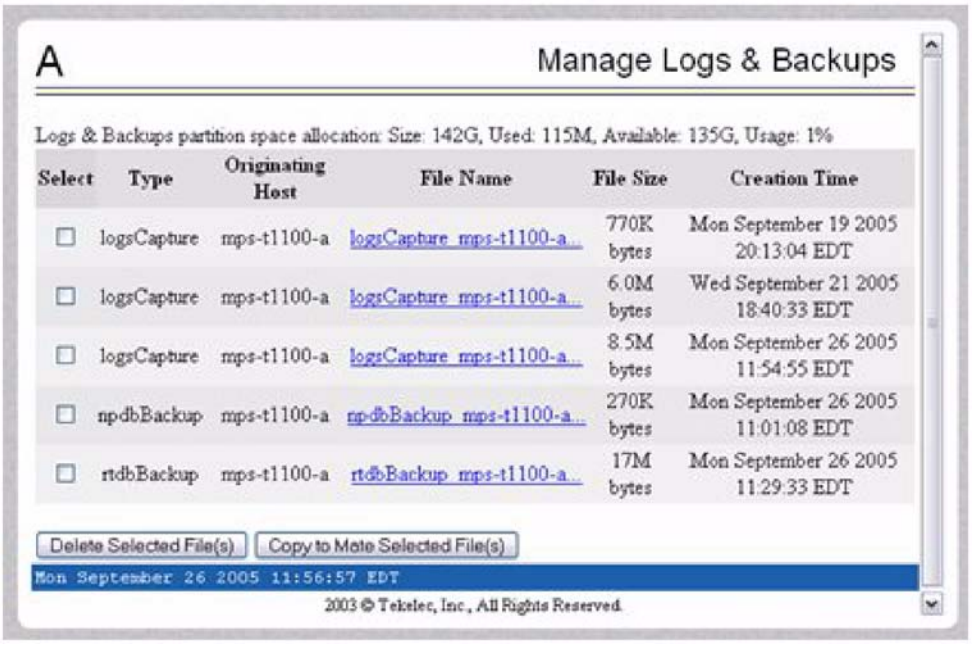
When you click the Capture Logs button, the copy of the log files occurs, and a successful completion displays the message in **Figure 3-102** .

Figure 3-102. Example of Successfully Capturing Log Files

Manage Log Files

The Debug / Manage Log Files screen displays the captured log files and allows the user to delete the copies no longer wanted. See **Figure 3-103** for the Manage Log Files screen.

Figure 3-103. Manage Log Files



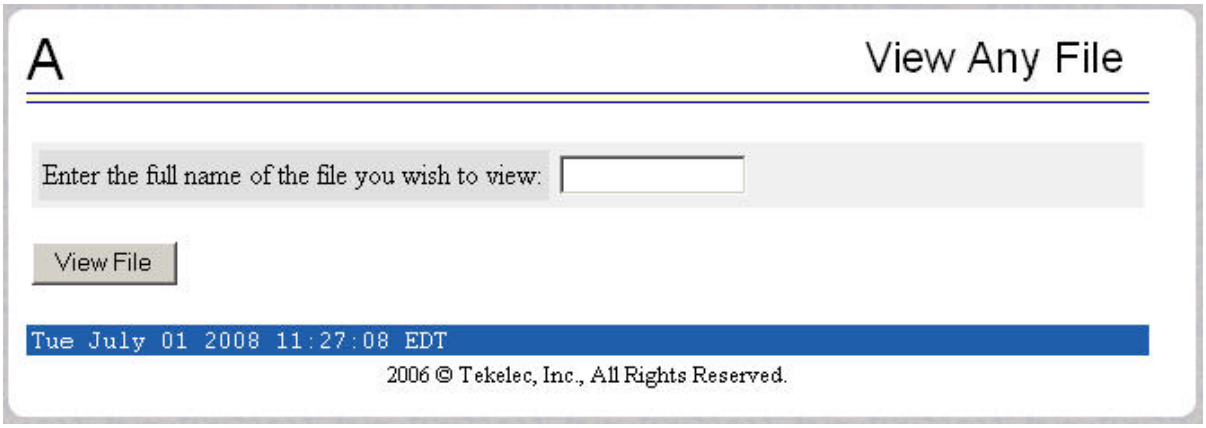
In the Manage Log Files screen, you can remove a log file by clicking the appropriate file under the Selete column and then the Delete Selected File(s) button. A successful removal message appears in **Figure 3-104** .

Figure 3-104. Example of Successfully Deleting a Log File

View Any File

The Debug / View Any File screen allows the user to view any file on the system using the Log Viewer. When the user enters a file, the Log Viewer is invoked. See the View Any File screen in **Figure 3-105** .

Figure 3-105. View Any File Screen

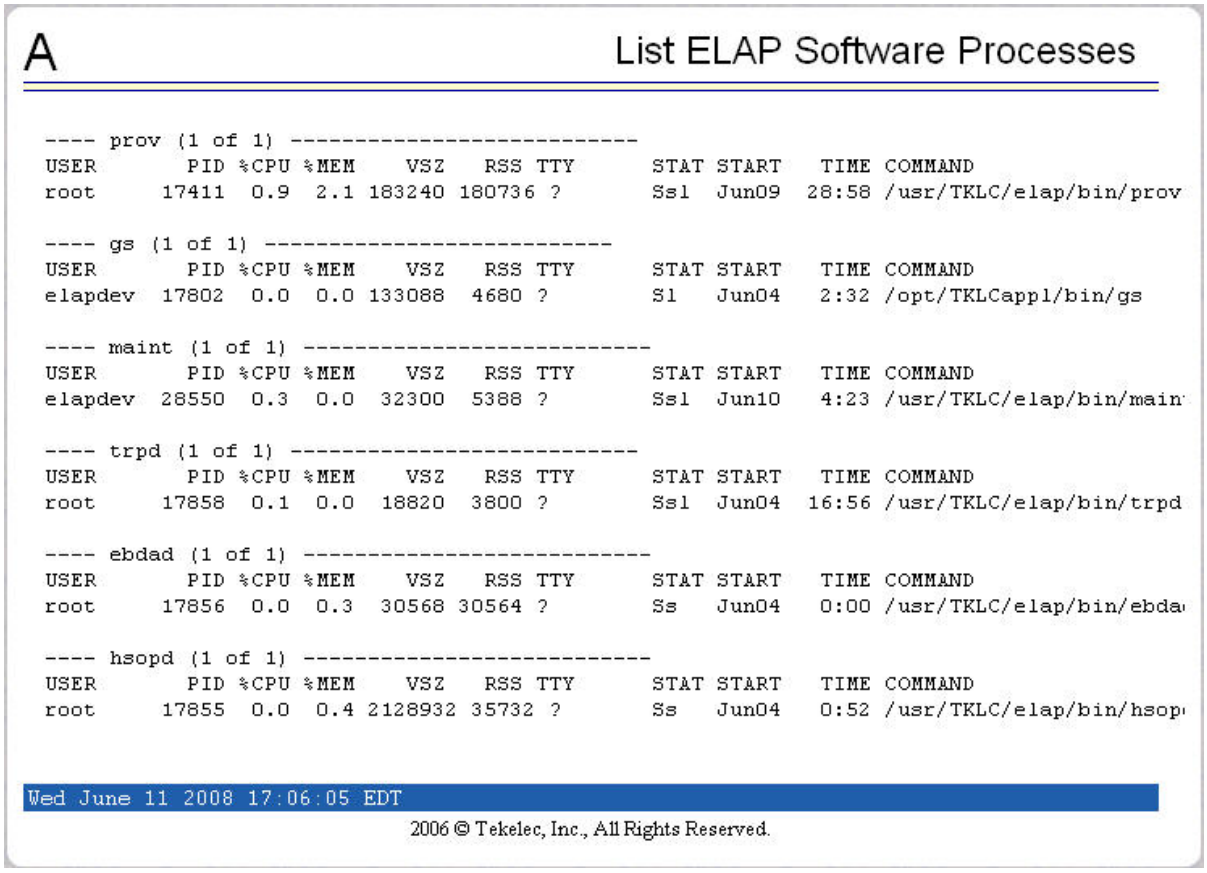


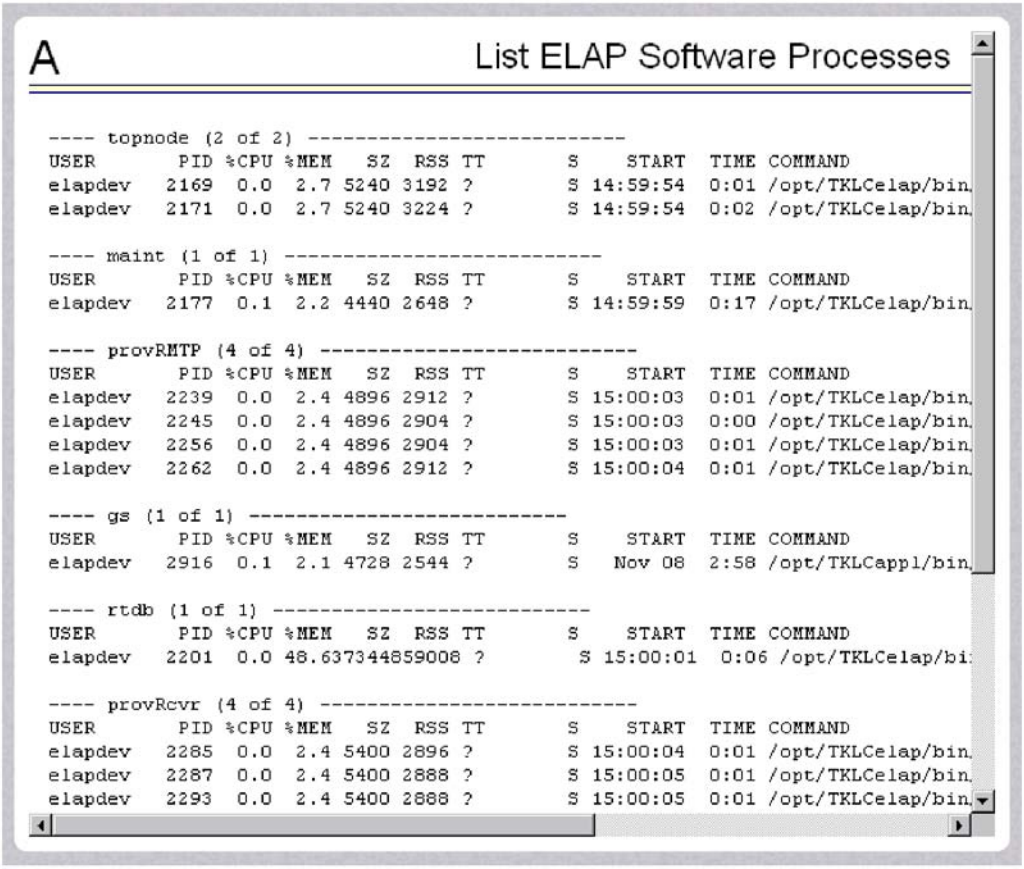
Opening any file in this window displays the requested file in the file viewer window. All files are viewed with the same file viewing utility. For details about this utility, see ELAP Log Viewer .

List ELAP Software Processes

The Debug / List ELAP Software Processes screen shows the ELAP processes started when the ELAP boots or with the "Start ELAP software" prompt. The **`/usr/ucb/ps -auxw`** command generates this list. (The operating system's manual page for the ps command thoroughly defines the output for this command.) **Figure 3-106** shows an example of the format of the process list.

Figure 3-106. View Any File Screen



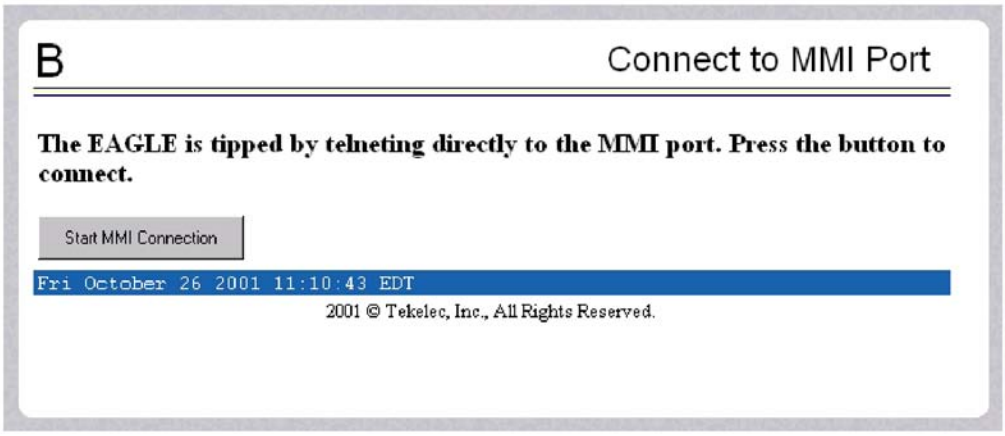


When you have finished with this screen, you can click the **Back** button on the browser or select another menu item to perform.

Connect to EAGLE 5 ISS MMI Port

The Debug / Connect to EAGLE 5 ISS MMI Port screen lets the user interact with the EAGLE 5 ISS through the MMI port only from ELAP B. See the *Commands Manual* for a detailed listing of EAGLE 5 ISS commands and the input and output from the EAGLE 5 ISS MMI port. **Figure 3-107** shows the Connect to MMI Port screen.

Figure 3-107. Connect to MMI Port Screen

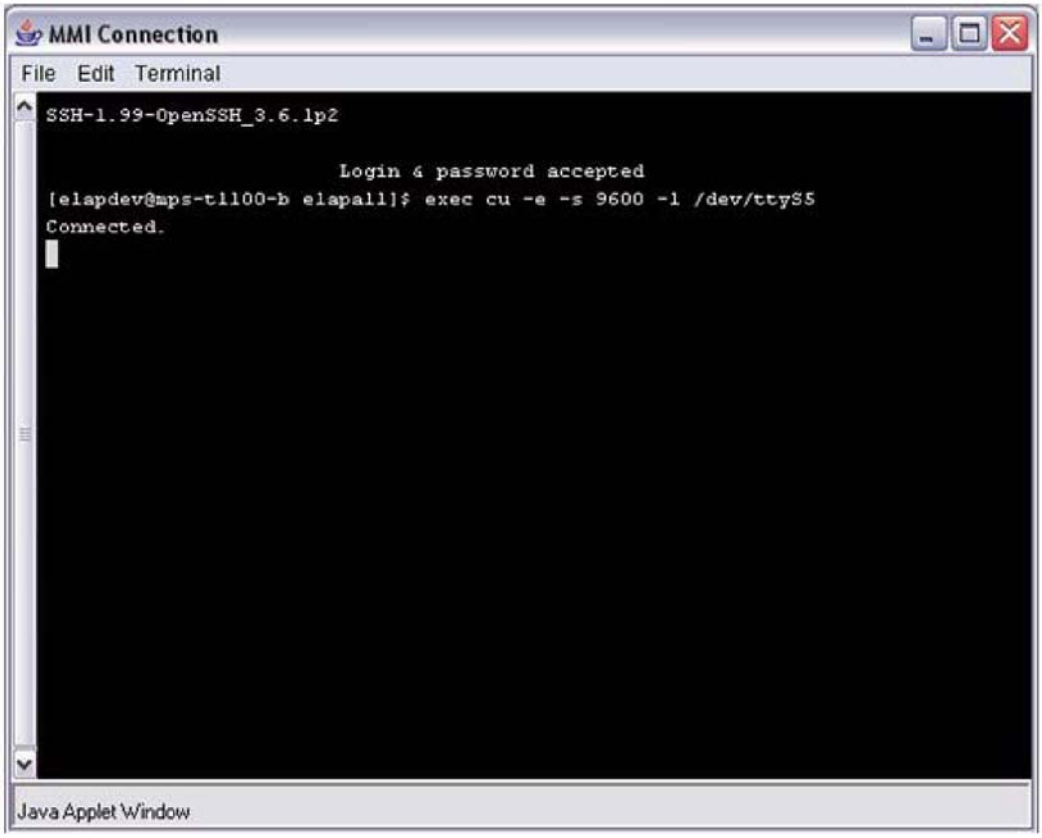


Press the Start MMI Connection button, and the SSH User Authentication window appears. Enter the User name (elapdev) and password to connect. **Figure 3-108** has an example of the SSH User Authentication screen.

Figure 3-108. SSH User Authentication Screen

After a successful login, a new window appears with the MMI connection. Refer to the *Commands Manual* for details about the **`chg-trm`** and **`rtrv-trm`** commands. **Figure 3-109** has an example of the MMI window.

Figure 3-109. MMI Connection Window



The window starts a **ssh** session during which you can issue EAGLE 5 ISS commands. You can close the session by:

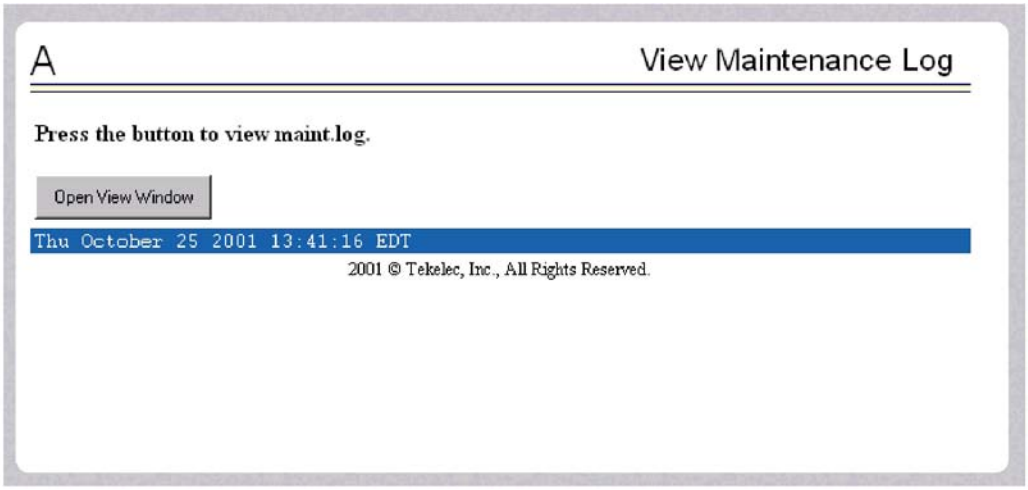
- Using the tilde character and the period (for example: **~.**) or
- Closing the window under the File menu, or
- Clicking on the X icon in the upper right corner of the window.Remember that the MMI port is on only ELAP B, and you can connect to the port only when you are on ELAP B. If you were to forget and attempt to perform this command from ELAP A, you see the error screen in **Figure 3-110** .

Figure 3-110. Error in Connecting to MMI Port from ELAP A

ELAP Log Viewer

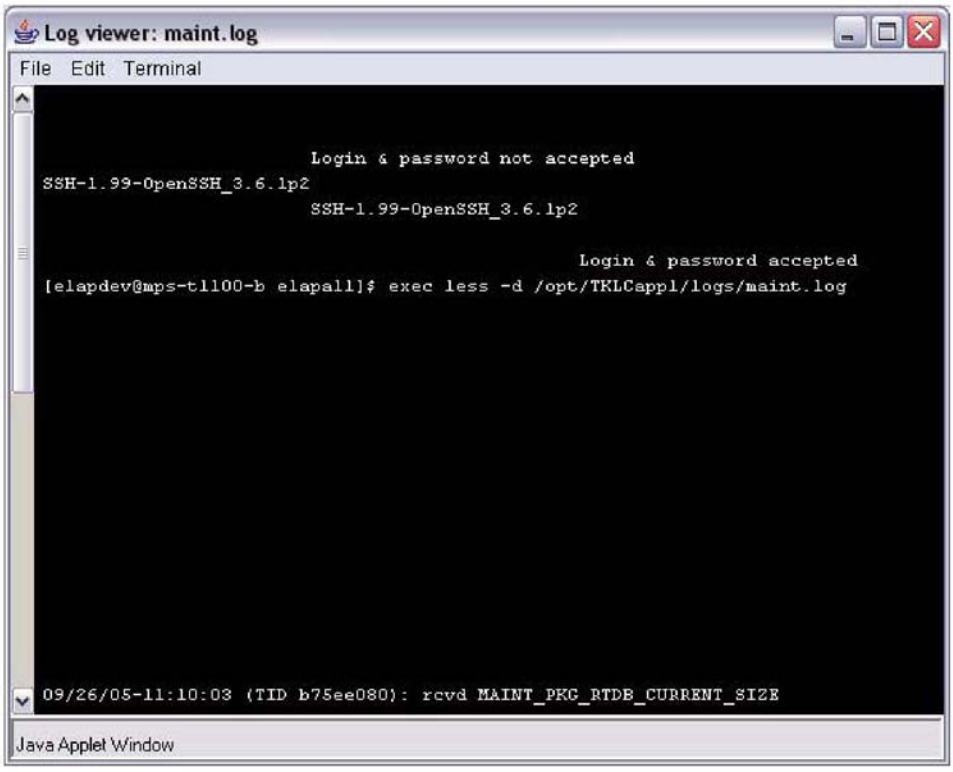
Viewing any log file involves using the Log Viewer. Menu options using the log viewer first display a request screen in the workspace, shown in **Figure 3-111** .

Figure 3-111. Typical Log Viewer Request Screen



Invoke the log viewer by pressing the Open View Window button. This opens the SSH User Authentication window. A user name and Password word are required to login. Then the log viewer appears in its own window so you can continue using the user interface while viewing the selected file. See **Figure 3-112** for a sample Log Viewer window.

Figure 3-112. Log Viewer Window Example



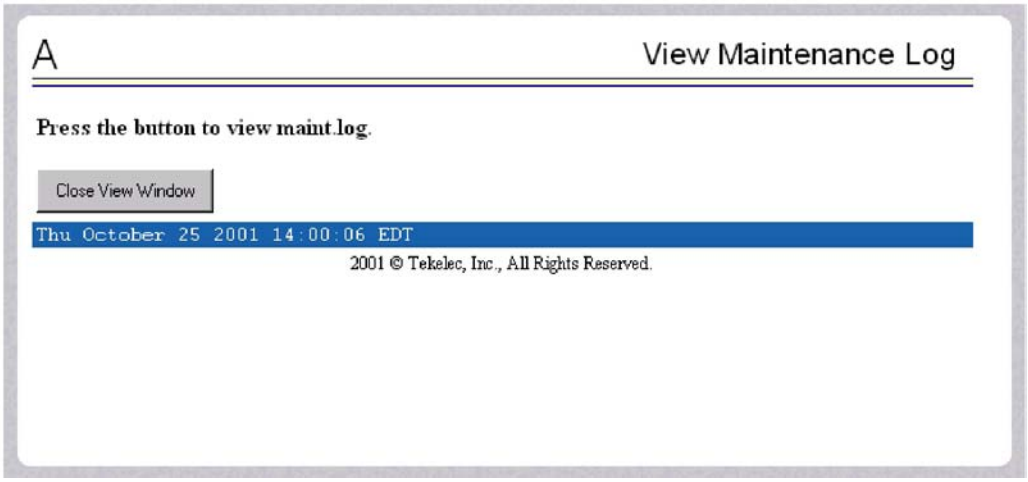
Use the commands in **Table 3-1** to navigate through the file displayed by the log viewer:

Table 3-1. Log Viewer Navigation Commands

Command	Action
<return>	Scroll down 1 line
<space>	Scroll down 1 page
b	Scroll up 1 page
G	Go to bottom of file
/ ***{pattern}***	Search for ***{pattern}*** from current position in file
n	Repeat search
q	Exit log viewer

When you have finished viewing a log file, close the Log Viewer window by clicking the Close View Window button, shown in **Figure 3-113** .

Figure 3-113. Closing the Log Viewer Window



Platform Menu

The Platform Menu allows the user to perform various platform-related functions, including running health checks, back ups, upgrades, shut downs, etc., shown in Platform Menu.

Figure 3-114. Platform Menu

The Platform menu provides these actions:

- Run Health Check Screen
- List All Running Processes
- LINK
- Eject the CD
- Reboot the MPS
- Halt the MPS
- LINK

Run Health Check Screen

The Platform / Run Health Check screen allows the user to execute the health check routine on the selected ELAP. The *Tekelec 1100 AS MPS Platform Software and Maintenance Manual*describes the health check (also called system health check and syscheck) in detail.

The first screen presented in the workspace frame lets the user select the “normal” or “verbose” mode of output detail. **Figure 3-115** shows the Run Health Check screen that begins the execution of this diagnostic tool.

Figure 3-115. Run Health Check Screen

The ELAP system health check utility performs multiple tests of the server. For each test, check and balances verify the health of the MPS server and platform software. Refer to the *Tekelec 1100 AS MPS Platform Software and Maintenance Manual*, for the functions performed and how to interpret the results of the normal outputs (**Figure 3-116**) and verbose outputs (**Figure 3-117**).

Figure 3-116. Normal Health Check Output

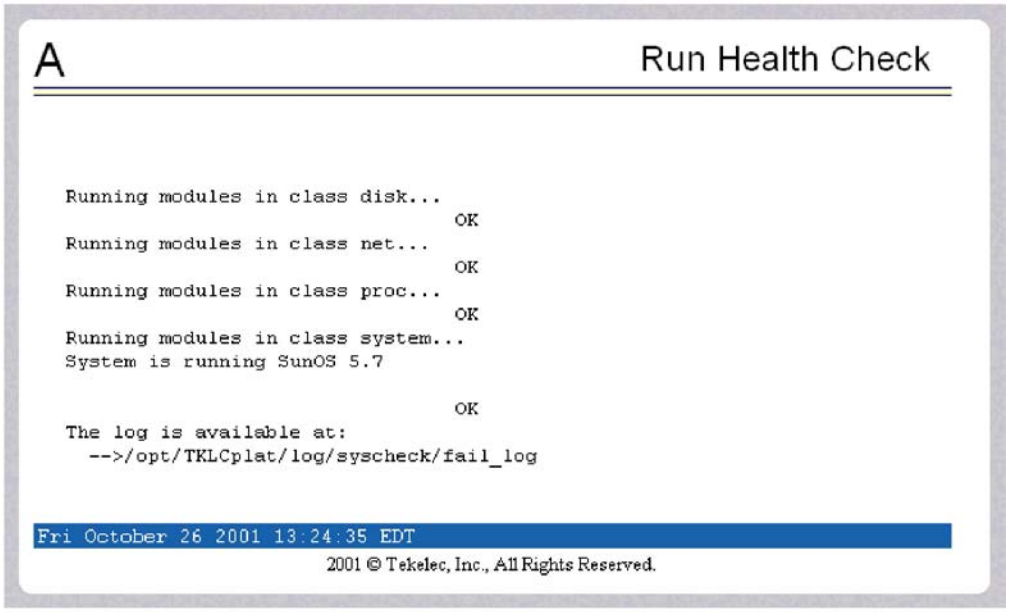
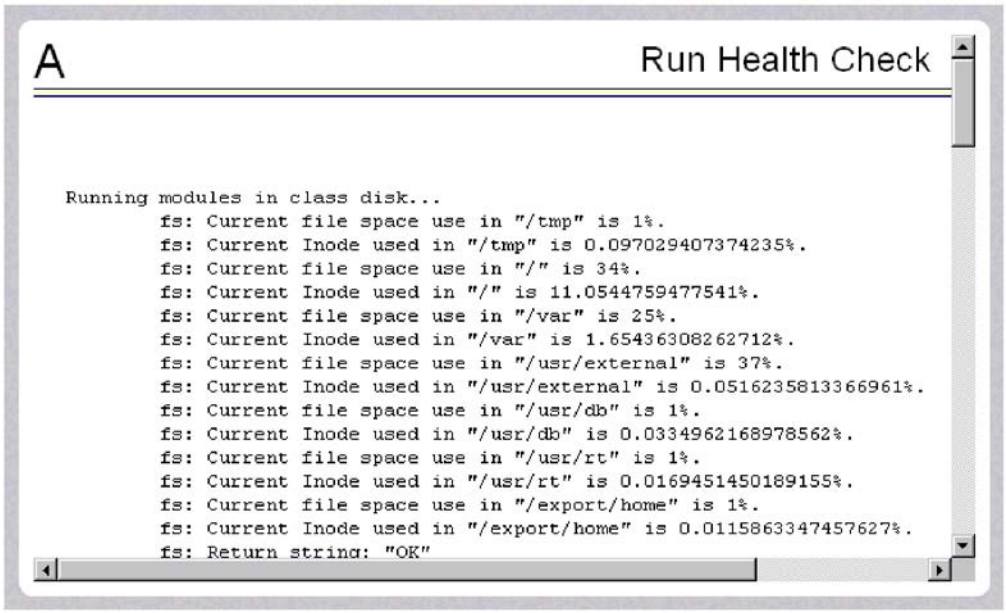


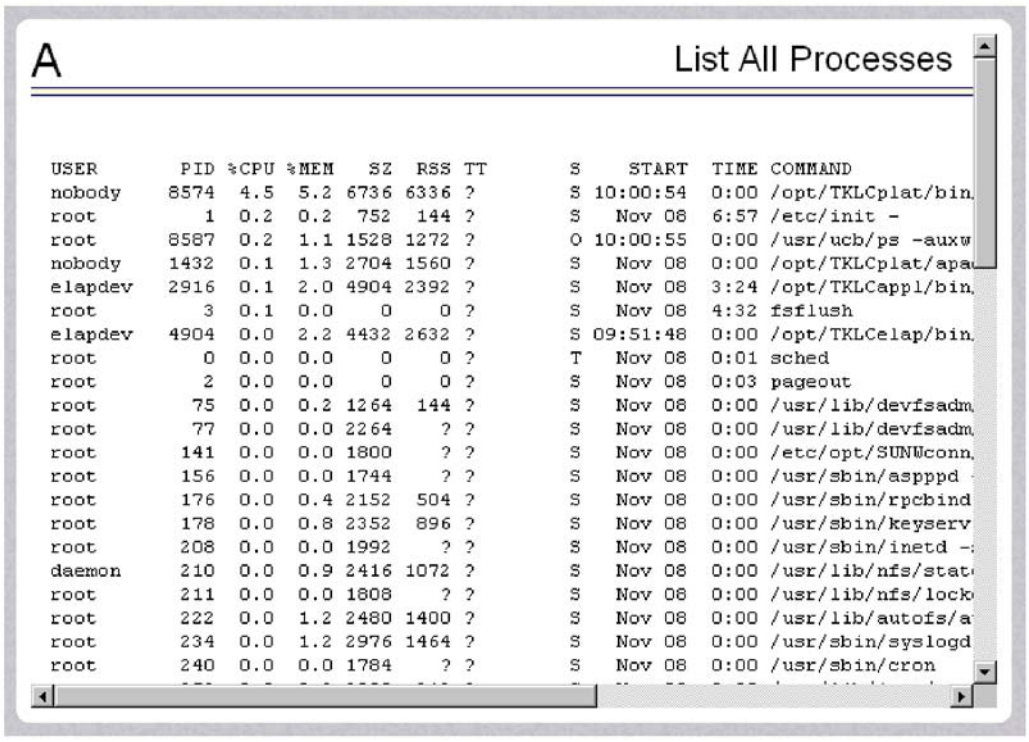
Figure 3-117. Portion of Verbose Health Check Output



List All Running Processes

The Platform / List All Running Processes screen lists all processes running on the selected ELAP. The **`/bin/ps auxw`** command generates this list. The operating system's manual page for the **`ps`** command thoroughly defines the output for this command. **Figure 3-118** shows an example of the process list.

Figure 3-118. List All Running Processes Screen

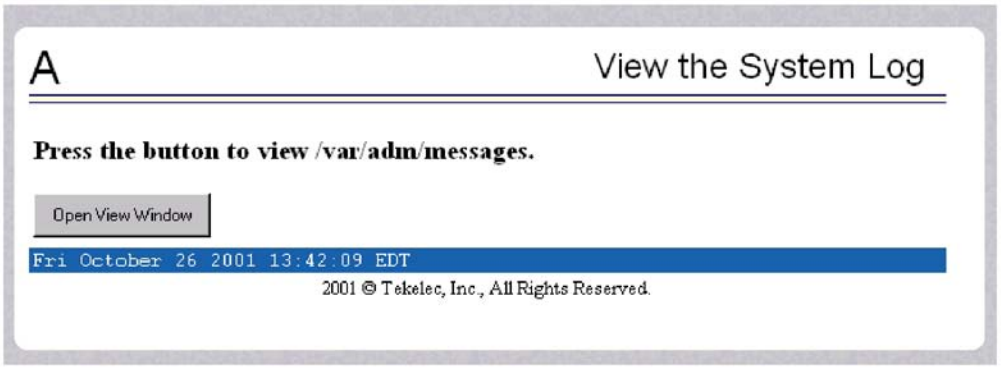


NOTE: The exact processes shown will not be the same on your ELAP servers. The output from this command is unique for each ELAP, depending on the ELAP software processes, the number of active ELAP user interface processes, and other operational conditions.

View System Log

The Platform / View System Log screen allows the user to display the System Log. Each time a system maintenance activity occurs, an entry is made in the System Log. When the user chooses this menu selection, the View the System Log screen appears, as shown in **Figure 3-119** .

Figure 3-119. View the System Log Screen



When the user clicks the Open View Window button, the system shows the System Log in the Log Viewer window. (The use of the Log Viewer is described ELAP Log Viewer .) See **Figure 3-120** for an example of the System Log output.

Figure 3-120. View System Log Format Example

```
May  6 15:39:08 mate unix: WARNING: interrupt level 4 not serviced
May  7 10:13:00 mate unix: WARNING: interrupt level 4 not serviced
```

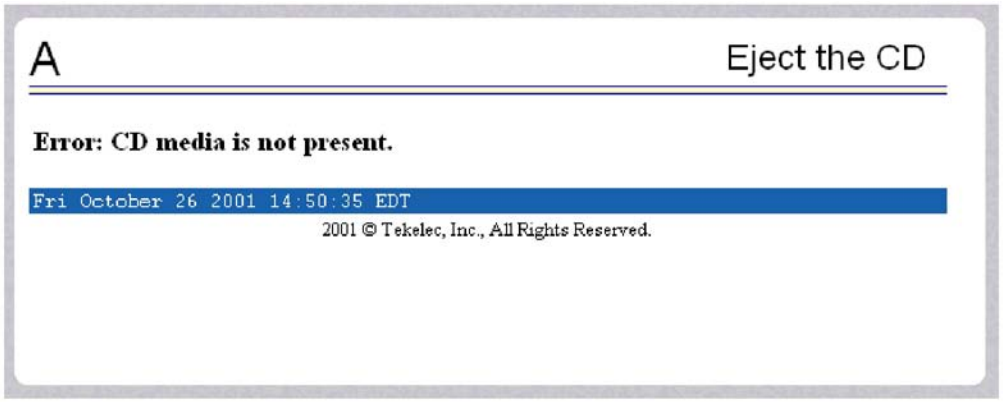
Eject the CD

The Platform / Eject the CD screen allows the to user to eject the CD on the selected CD device on the selected ELAP server. **Figure 3-121** shows the Eject CD screen.

Figure 3-121. Eject the CD Screen

Figure 3-122 shows an example of an error reporting that CD media is missing.

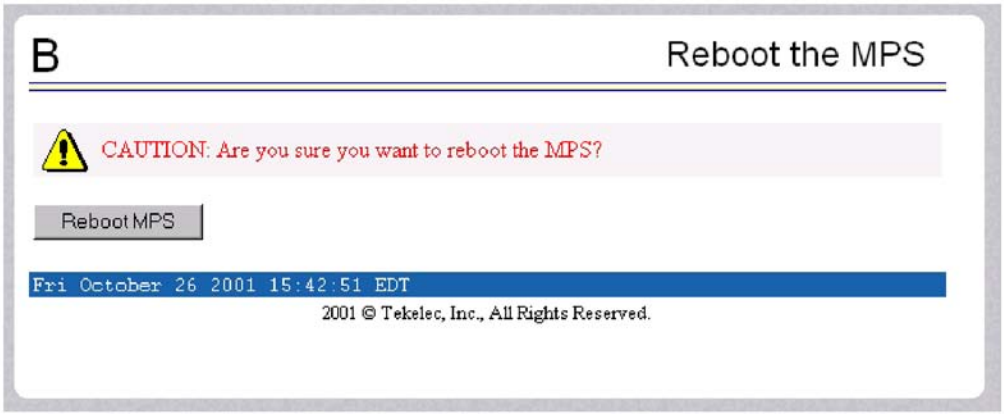
Figure 3-122. Eject CD Screen Error Message



Reboot the MPS

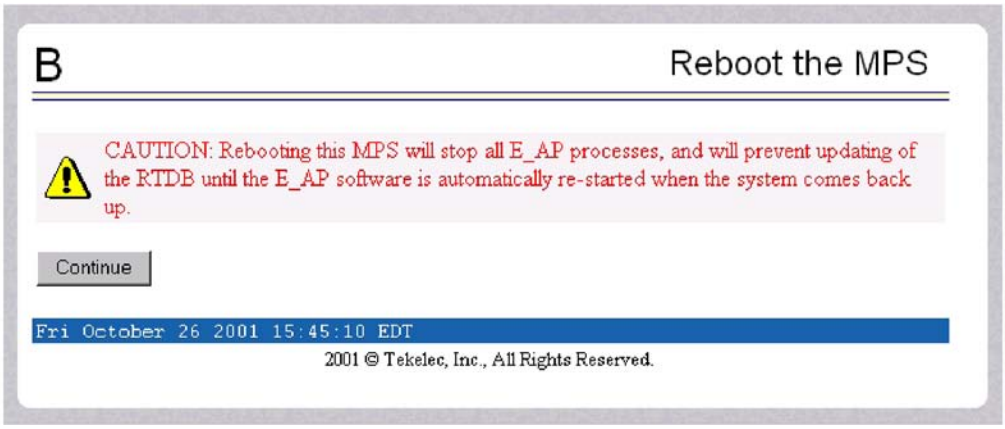
The Platform / Reboot the MPS screen allows the user to reboot the selected ELAP. All ELAP software processes running on the selected ELAP are shut down normally. Figure 3-123 shows the Reboot the MPS screen.

Figure 3-123. Reboot the MPS Screen



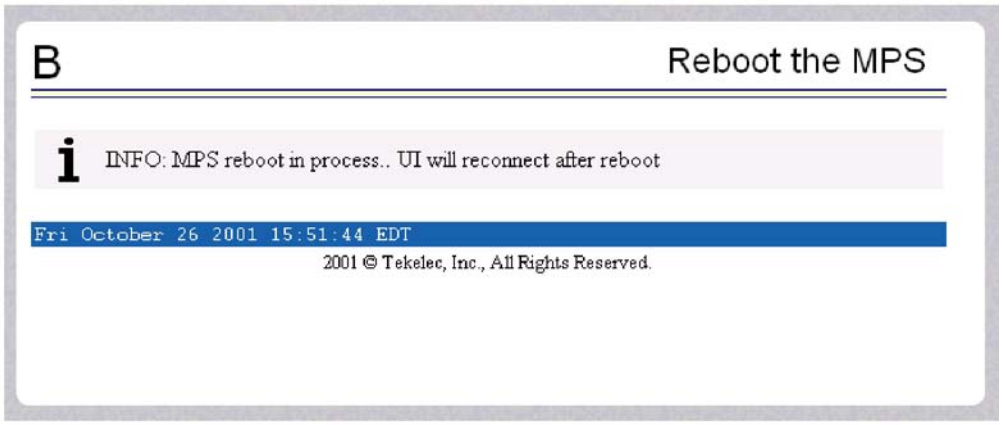
When you click the Reboot MPS button, a cautionary message appears, informing the user that this action causes ELAP to stop all activity and to prevent the RTDB from being updated with new subscriber data. See **Figure 3-124** .

Figure 3-124. Caution about Rebooting the MPS



When you are certain that you want to reboot, click the Continue button. Another screen informs you that MPS is being rebooted and that the User Interface will be reconnected when the reboot is completed, as shown in **Figure 3-125** .

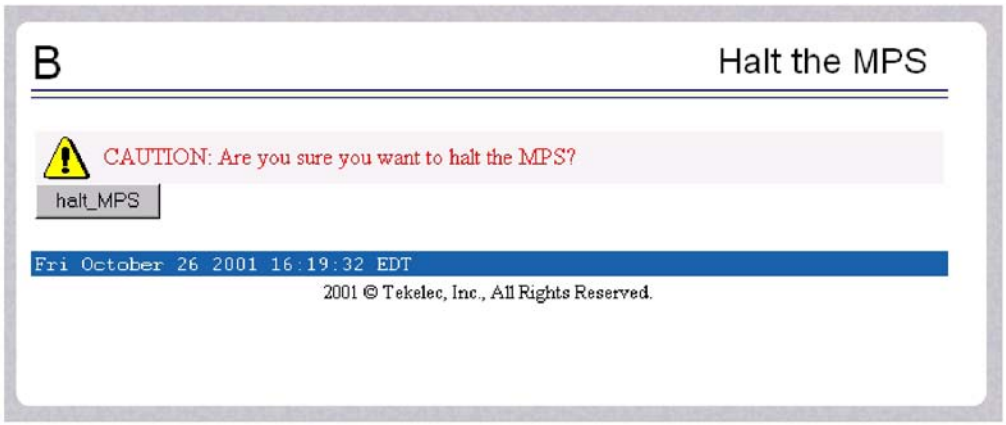
Figure 3-125. Rebooting the MPS in Process



Halt the MPS

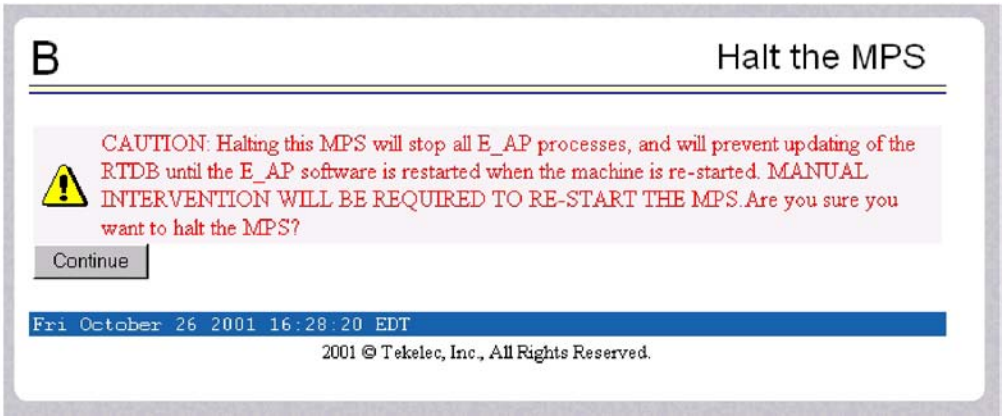
The Platform / Halt the MPS screen allows the user to halt the selected ELAP. All ELAP software processes running on the selected ELAP are shut down normally. Halt the MPS Screen shows the Halt the MPS screen.

Figure 3-126. Halt the MPS Screen



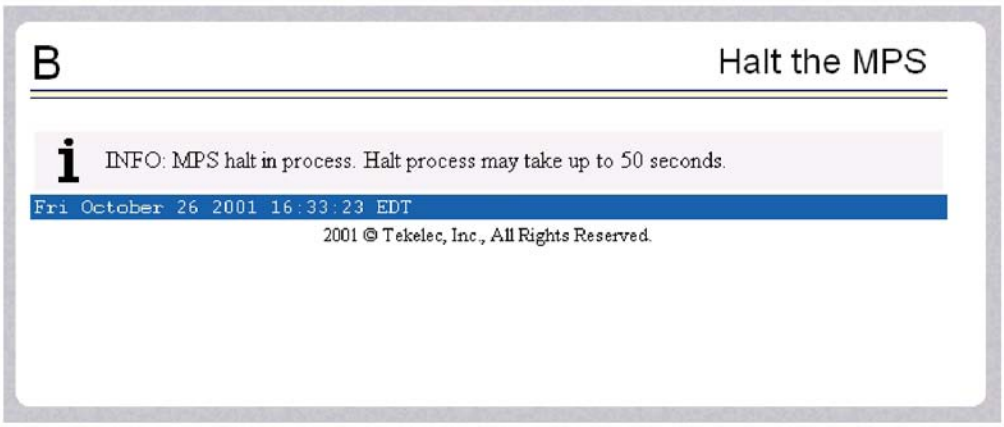
To perform this action, click the halt_MPS button. Next a cautionary message appears, informing the user that this action causes ELAP to stop all activity and to prevent the RTDB from being updated with new subscriber data. See Caution about Halting the MPS.

Figure 3-127. Caution about Halting the MPS



When you are certain that you want to halt the MPS, click the Continue button. Another screen informs you that MPS is being halted and that the process may require up to 50 seconds. See Rebooting the MPS in Process.

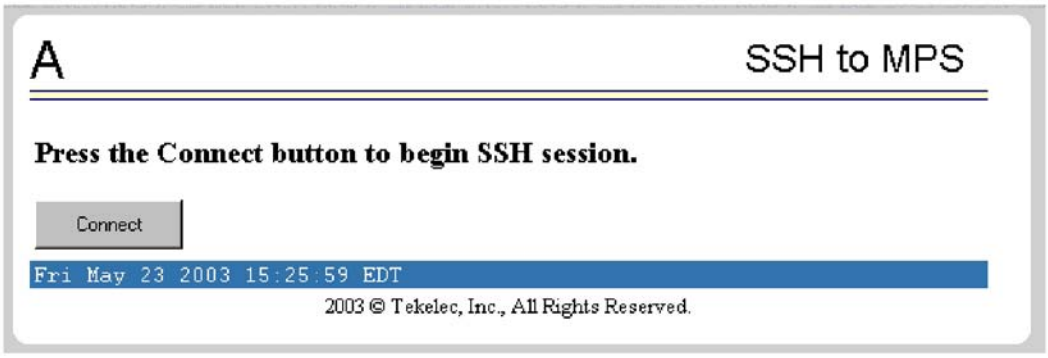
Figure 3-128. Rebooting the MPS in Process



SSH to MPS

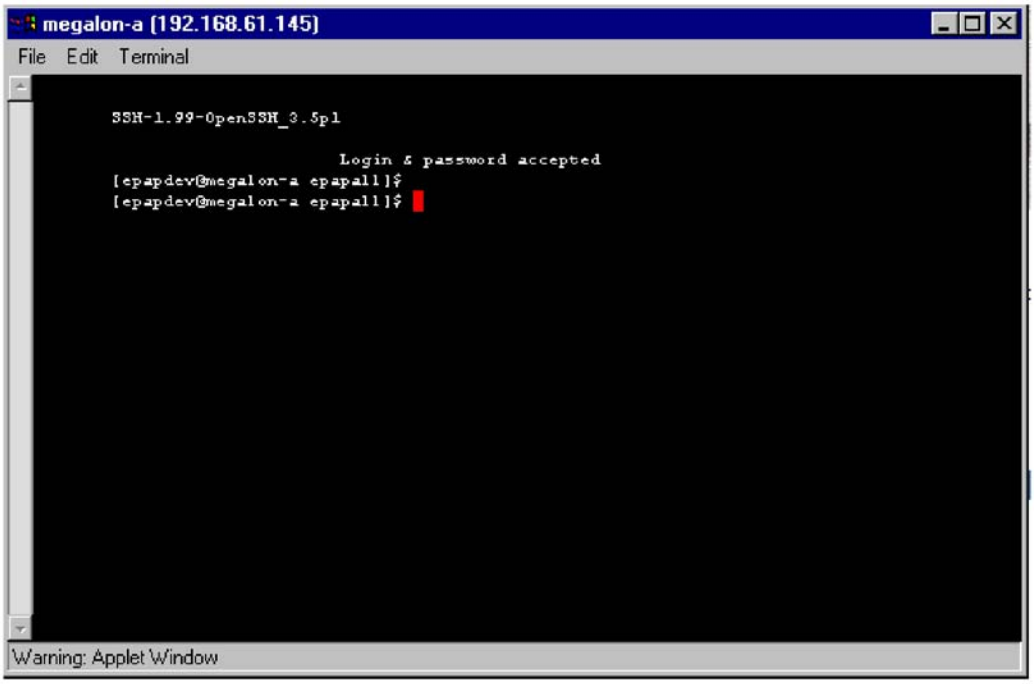
The Platform / SSH to MPS screen allows the user to have a **SSH** window to the user interface user. Clicking on the Connect button, shown in **Figure 3-129** , opens the SSH User Authentication window. A user name and Password word are required to login.

Figure 3-129. SSH to MPS Screen



Press the Connect button, and see the **SSH** window with which you can perform **SSH** communications, as shown in **Figure 3-130** .

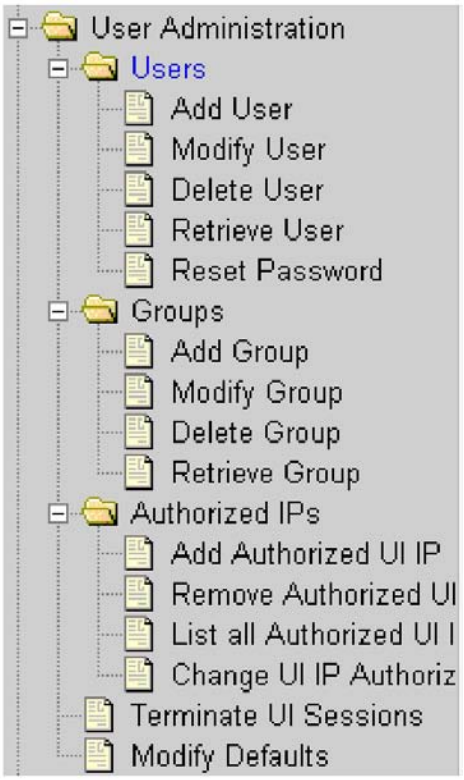
Figure 3-130. Example of a SSH Window



User Administration Menu

The User Administration menu allows the user to perform various platform tasks, including administering users and groups, terminating active sessions, and modifying system defaults. The user interface allows for many users with multiple and varied configurations of permissions. It is designed for convenience and ease of use while supporting complex user set-ups where required.

Figure 3-131. User Administration Menu



When a user successfully logs into the UI , he is considered to have a session open. These rules apply to session management and security.

- Idle Port Logout: If no messages are exchanged with the UI client session for a configurable amount of time, the session is automatically closed on the server side. The default length of the timeout is a system-wide value, configurable by the administrator. The administrator can also set a different timeout length for an individual user, if desired.

- Multiple Sessions per User: The administrator can turn off multiple sessions allowed per user on a global system-wide basis.

- Revoke/Restore User: The administrator can revoke a userid. A revoked userid remains in the database but can no longer log in. Likewise, the administrator can restore a userid that was previously revoked.

- Manage Unused UserIDs: The ELAP UI automatically revokes userids that are not accessed within a specified number of days. The number of days is a system-wide value that is definable by the administrator.

- Login Tracking: When a user successfully logs in, the UI displays the time of the last successful login and the number of failed login attempts for that userid.

- Intrusion Alert: When the number of successive failed login attempts from a specific IP address reaches **5** (five), the ELAP automatically writes a message to the UI security log and displays a message on the banner applet to inform any administrator logged in at that time.

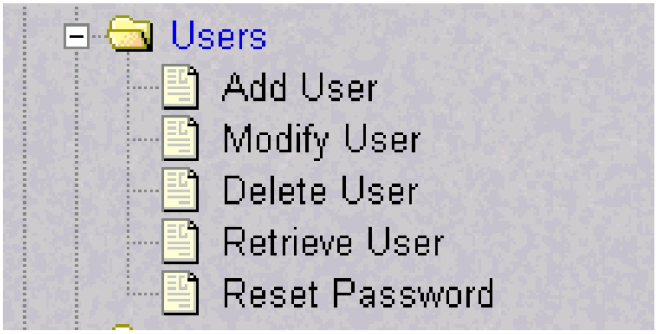
- Revoke Failed User: The UI automatically revokes any user who has N successive login failures within 24 hours. N is a system-wide configurablnumber, with a default of **3** (three). This restriction is turned off if N is set to 0 by the administrator.

The User Administration menu performs administration functions for users and groups, and handles terminating active sessions and modifying system defaults. See these topics discussed:

Users Menu

The User Administration / Users menu allows the system administrator to administer users functions such as add, modify, delete, retrieve, and reset user password. See the Users menu in **Figure 3-132** .

Figure 3-132. User Menu



A user is someone who has been given permission with system administrator authority to log in to the user interface. The administrator creates these user accounts and associates them with the groups to which they belong. A user automatically has access to all actions allowed to the groups he is a member. In addition to the user's groups, the administrator can set other user-specific permissions or restrictions to any user’s set of individual permissions.

The ELAP user interface comes pre-defined with user interface users in order to provide a seamless transition to the user interface. This is done by duplicating the Unix user logins and permissions that existe on the text-based UI. In addition, The default password for a new **`uiadmin`** is **`uiadmin`**. See **Table 3-2** for login names.

Table 3-2. ELAP UI Logins

Login Name	Access Granted
elapmaint	Maintenance menu and all submenus
elapdatabase	Database menu and all submenus
elapdebug	Debug menu and all submenus

Login Name	Access Granted
elapplatform	Platform menu and all submenus
uiadmin	User Administration menu
elapall	All of the above menus
elapconfig	Configuration menu and all submenus (text-based UI)

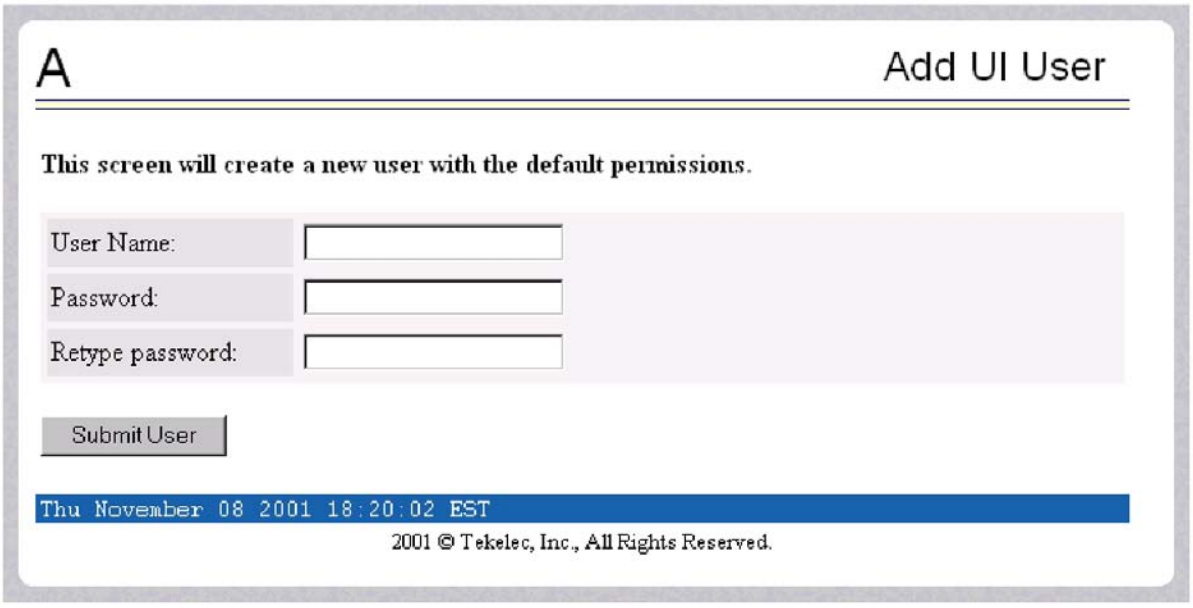
The Users menu performs the following actions:

- Add User
- Modify User
- Delete User
- Retrieve User
- Reset User Password

Add User

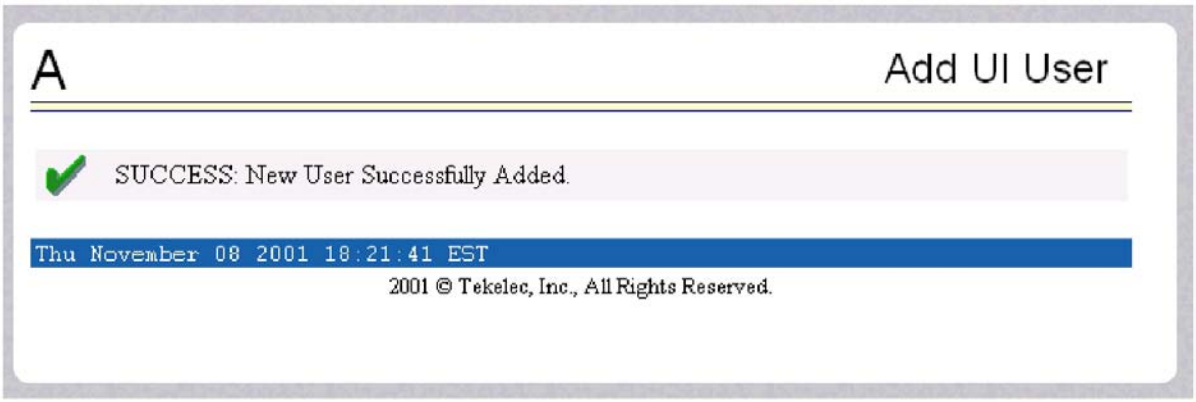
The User Administration / Users / Add User screen lets you add a new user interface user name and a default password. **Figure 3-133** shows the Add UI User screen.

Figure 3-133. Add User Screen



See **Figure 3-134** for the screen confirmation of the newly added user.

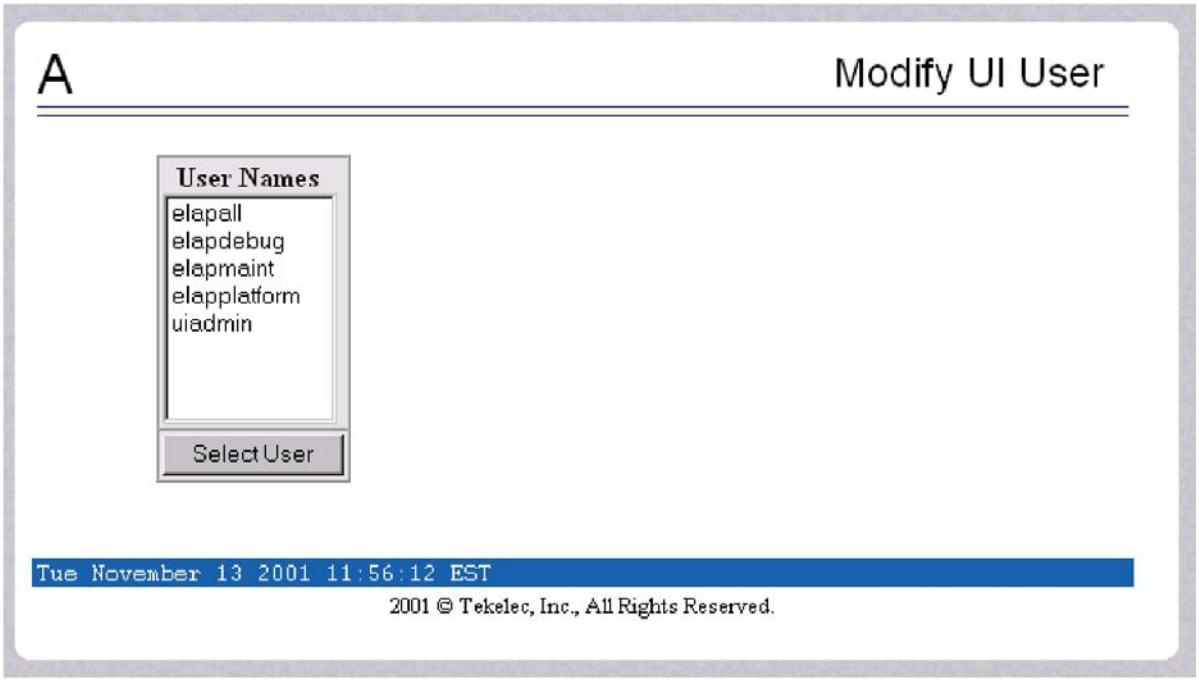
Figure 3-134. Success in Adding UI User



Modify User

The User Administration / Users / Modify User screen lets you change a user permission profile. The administrator must first select a user name from the list of current users, as shown in **Figure 3-135** .

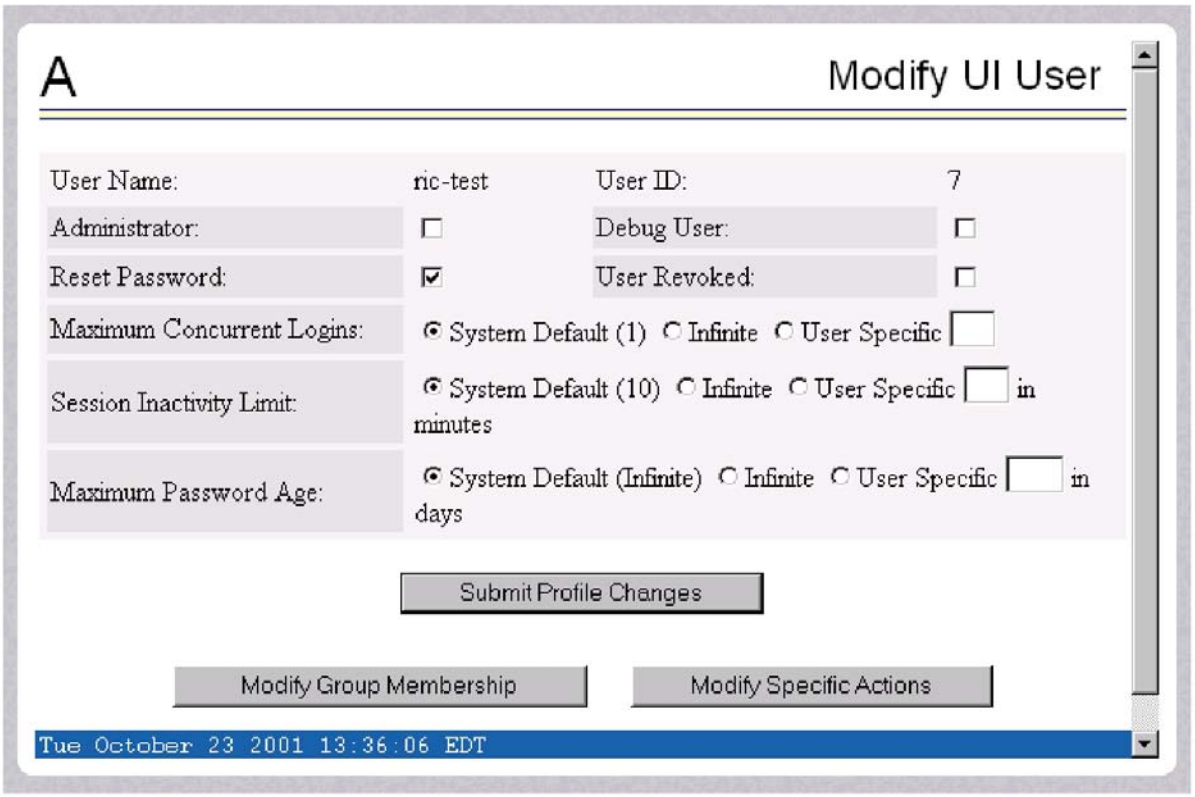
Figure 3-135. Select a User for Modification Screen



After you select a User Name in the screen above, the screen to specify the user permissions appears, as shown in **Figure 3-136** . In that screen, you can view and specify the permissions allowed to the user.

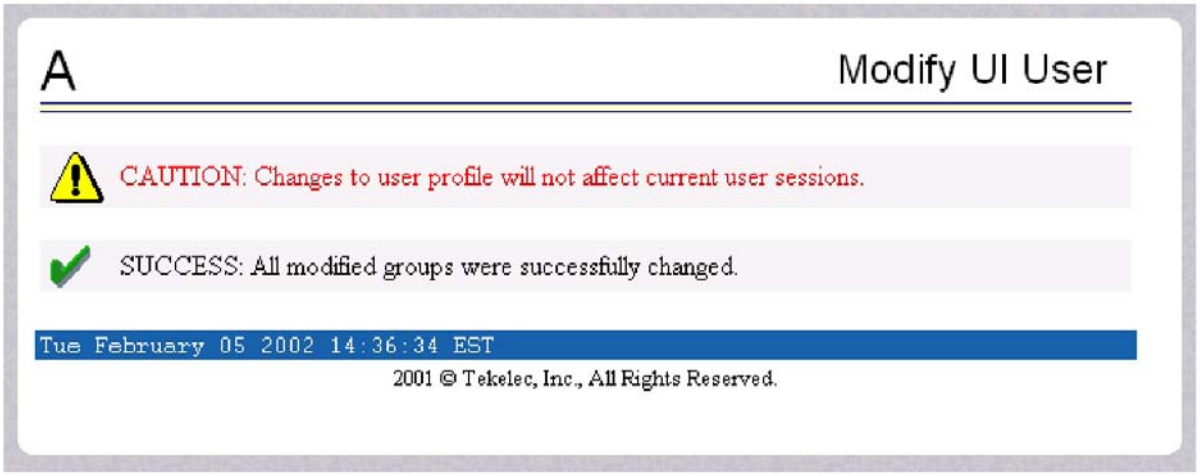
You can directly specify the number of concurrent log-ins, an inactivity time limit, and a password age limit. In addition, you can modify group membership data and specific actions that the user is permitted. See **Figure 3-136** to see how to specify user modifications.

Figure 3-136. Specify the Modify UI User Screen



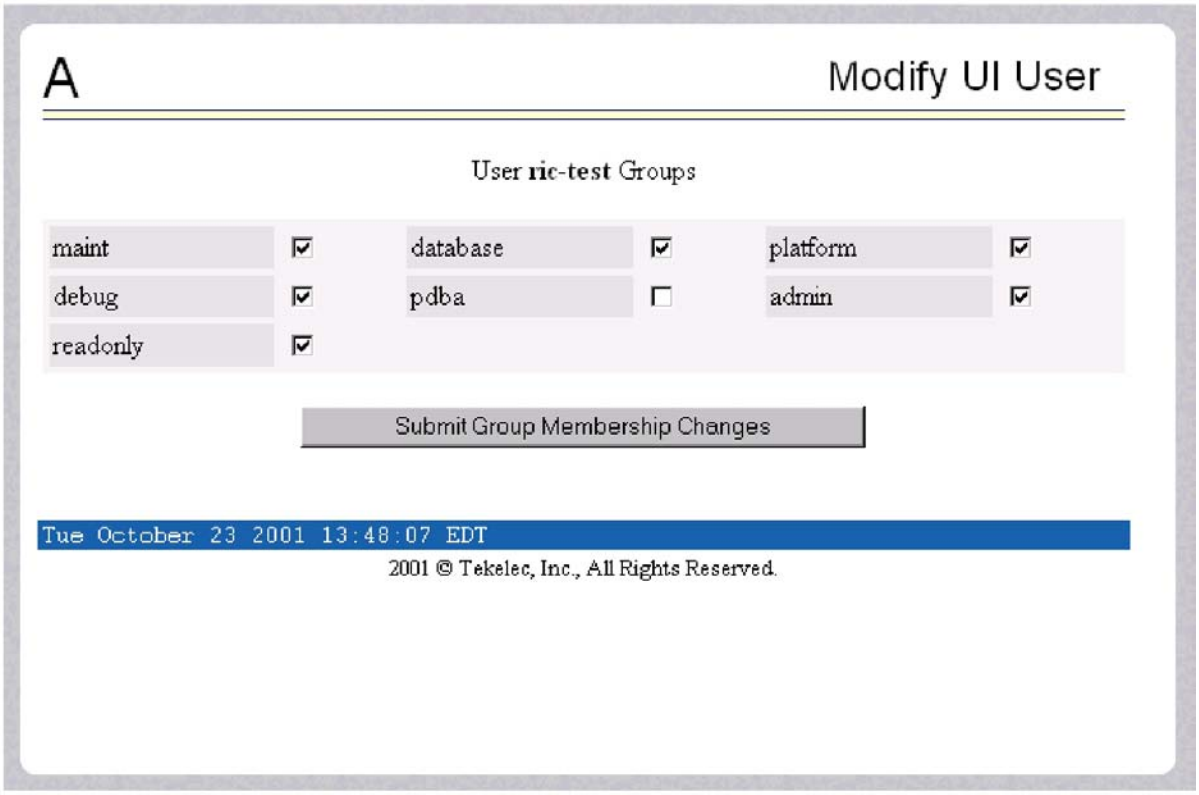
When you modify any of the direct entries, such as concurrent logins or inactivity, and click the Submit Profile Changes, you see the screen confirming the changes, as in **Figure 3-137** .

Figure 3-137. Confirming Modify UI User Profile Changes



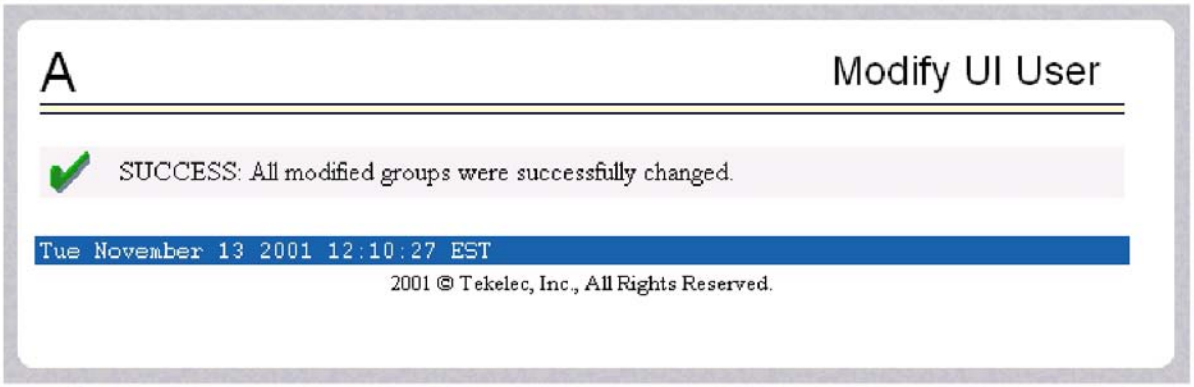
When you click Modify Group Membership in **Figure 3-136** , the screen displays the group membership choices available for the user. See **Figure 3-138** .

Figure 3-138. Modify UI User's Group Membership



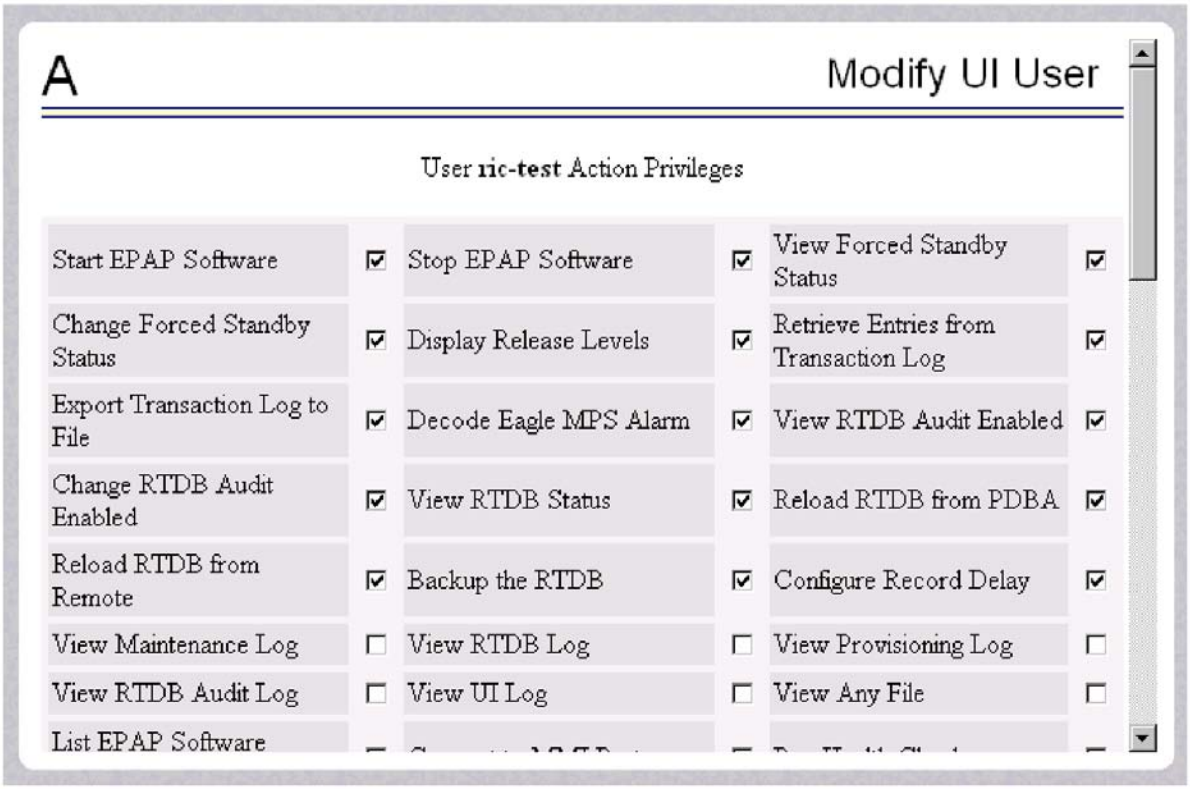
When you submit the changes for group membership, **Figure 3-139** illustrates the confirmation screen.

Figure 3-139. Confirming Modify UI User Group Membership Changes



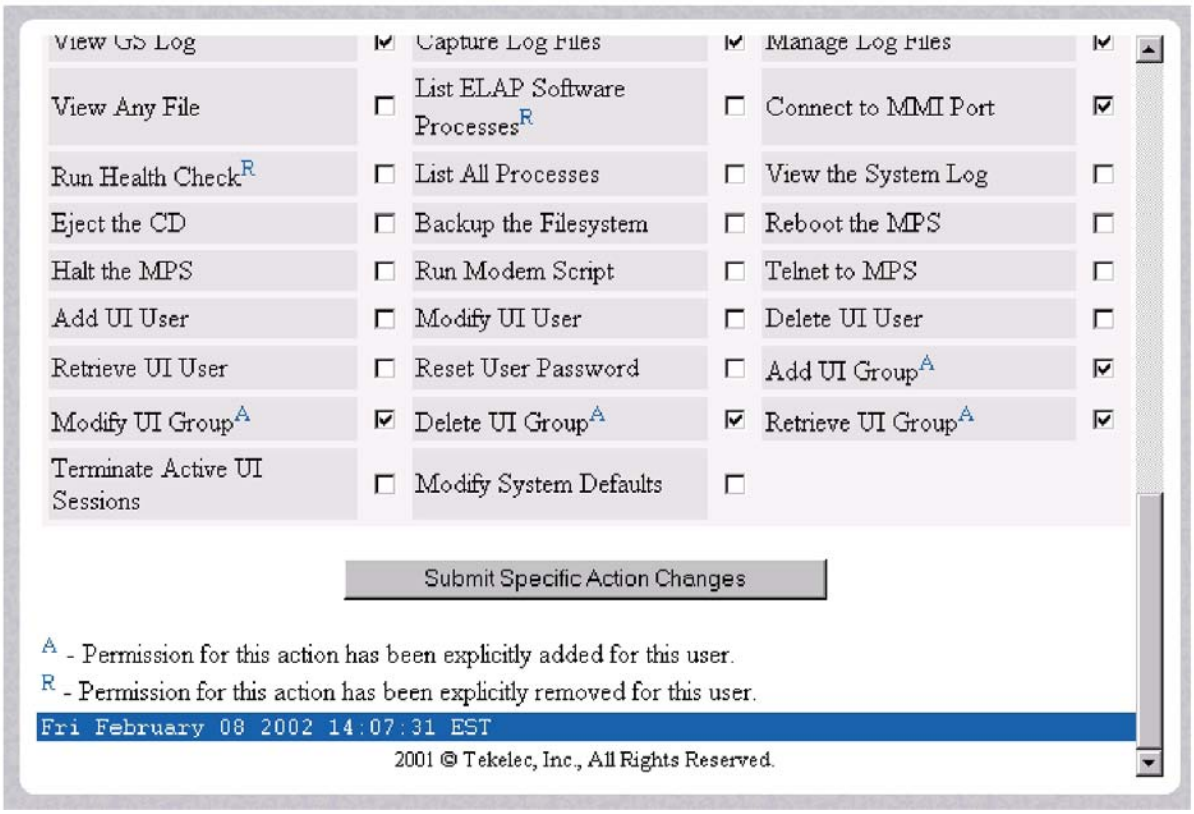
When you click Modify Specific Actions in **Figure 3-136**, the screen displays Action Privileges you can specify for the user you are modifying. See **Figure 3-140**.

Figure 3-140. Modify UI User's Specific Actions



This screen contains many selections from which to choose. **Figure 3-141** shows the continuation of the screen and the Submit button to press when you are done.

Figure 3-141. Continuing Modify UI User's Specific Actions



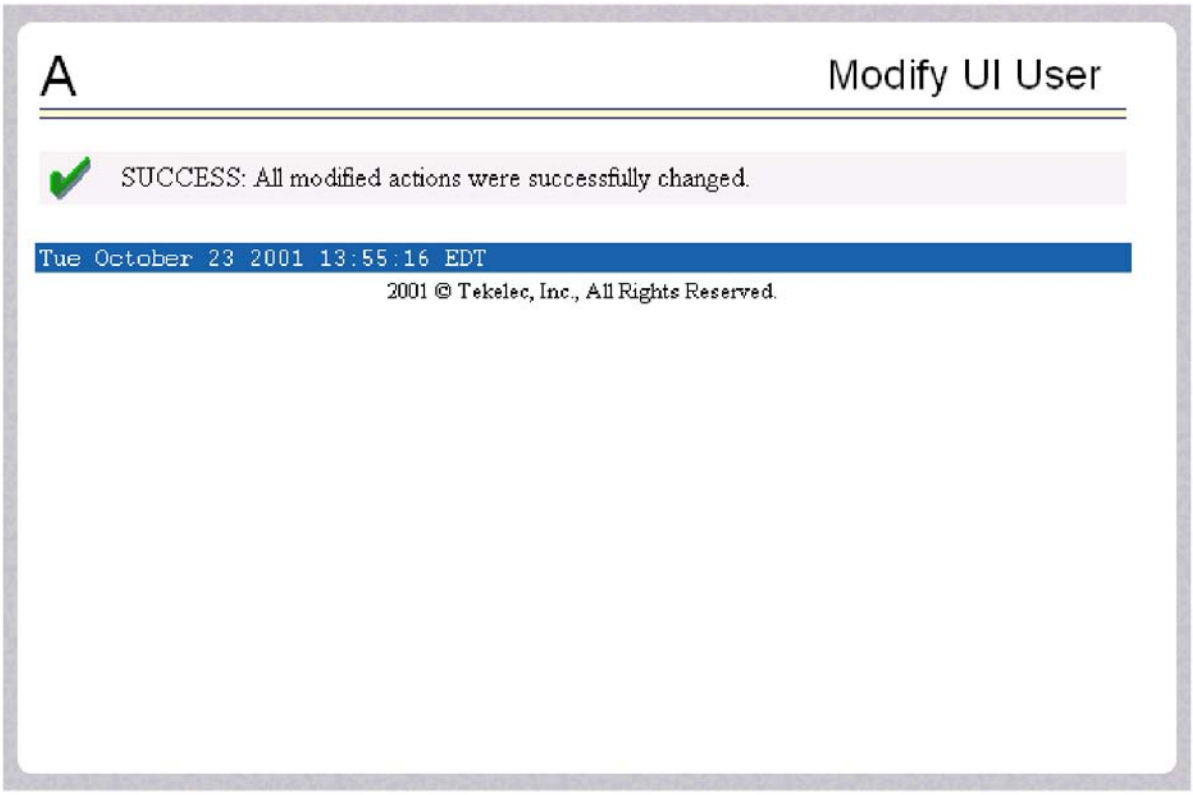
The bottom of the Modify UI User's Special Actions screen contains these explanatory notes:

- A - Permission for this action has been explicitly added for this user.
- R - Permission for this action has been explicitly removed for this user.

These notes indicate the privileges specifically added or removed for an individual user from the groups to which he/she is a member. This allows discrete refinement of user privileges even though he/she may be a member of groups.

When you submit the changes for specific actions, **Figure 3-142** shows the system accepting your change in action privileges for the specified user.

Figure 3-142. Confirming Modify UI User Specific Actions Changes



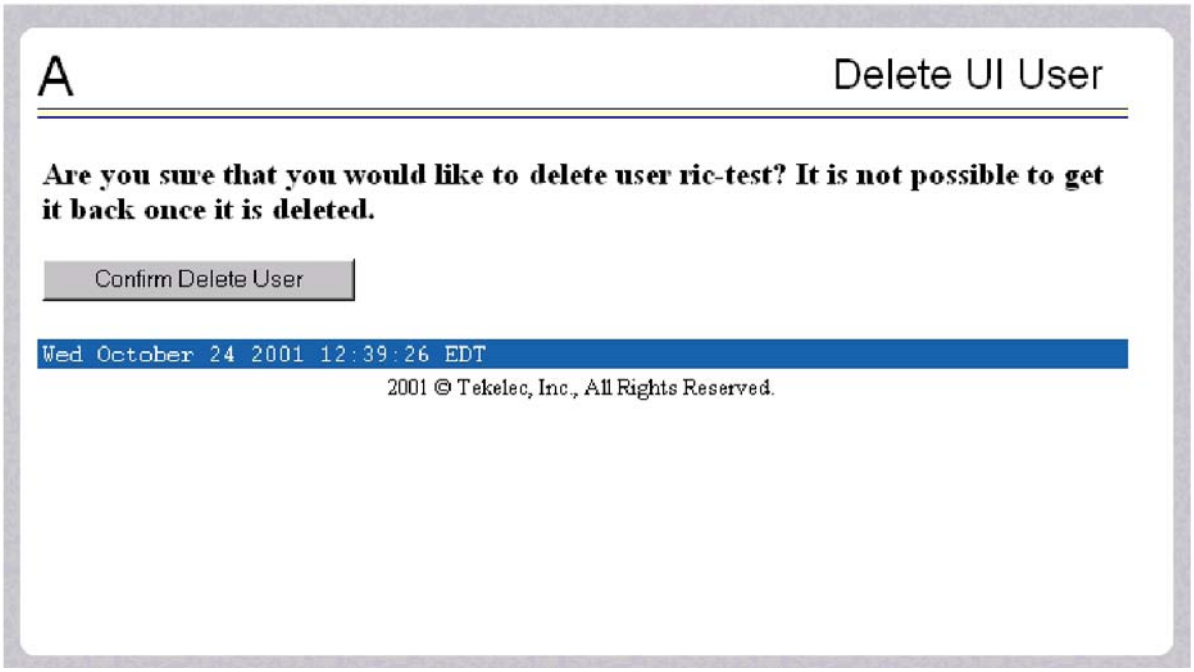
Delete User

The User Administration / Users / Delete User screen lets an administrator remove a user name from the list of user interface names. First you select the user name to be deleted and click the Delete User button, shown in **Figure 3-143** .

Figure 3-143. Delete UI User Screen

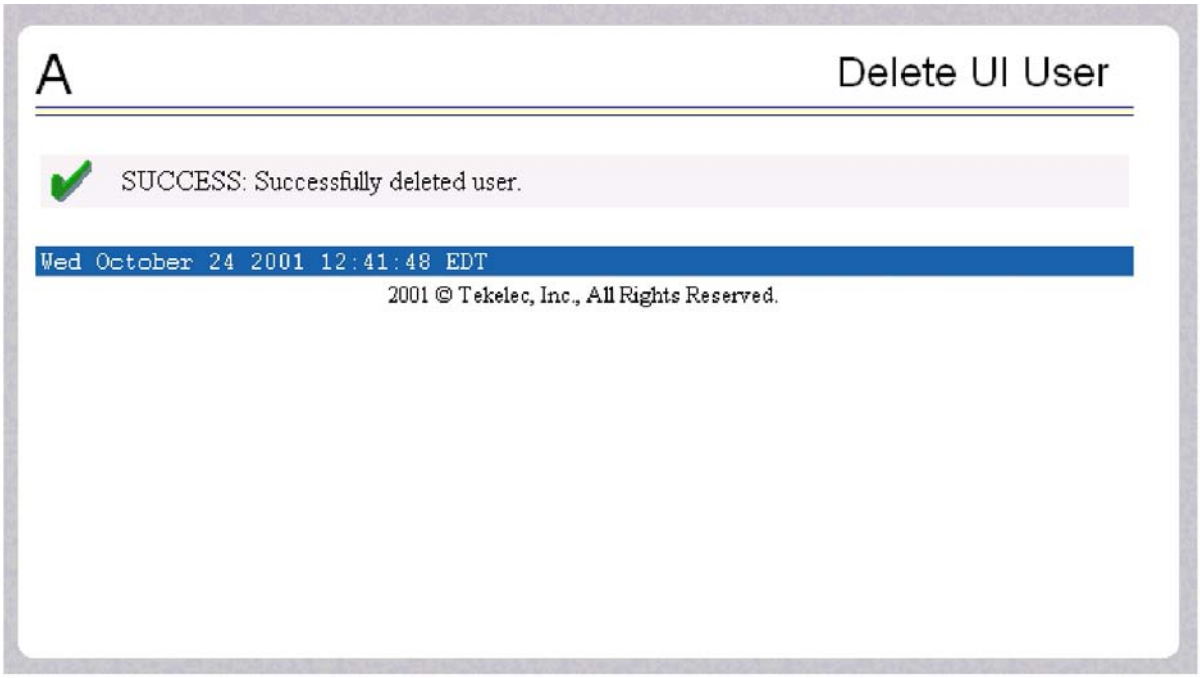
Next a confirmation screen appears, as shown in **Figure 3-144** .

Figure 3-144. Requesting Confirmation of User Deletion



Finally, the screen shows the user has been successfully removed, as shown in **Figure 3-145** .

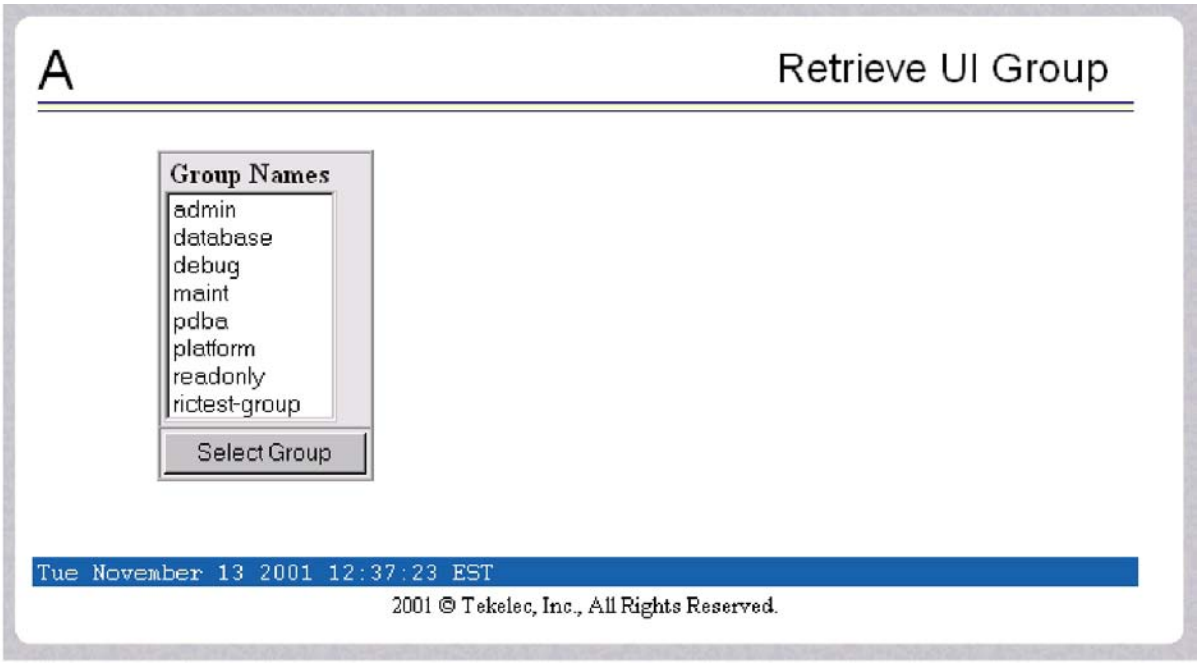
Figure 3-145. Confirming Deletion of the User



Retrieve User

The User Administration / Users / Retrieve User screen lets you display the user name permission profiles from the user interface information. First select a user name to be retrieved, and click the Select User button, as shown in **Figure 3-146** .

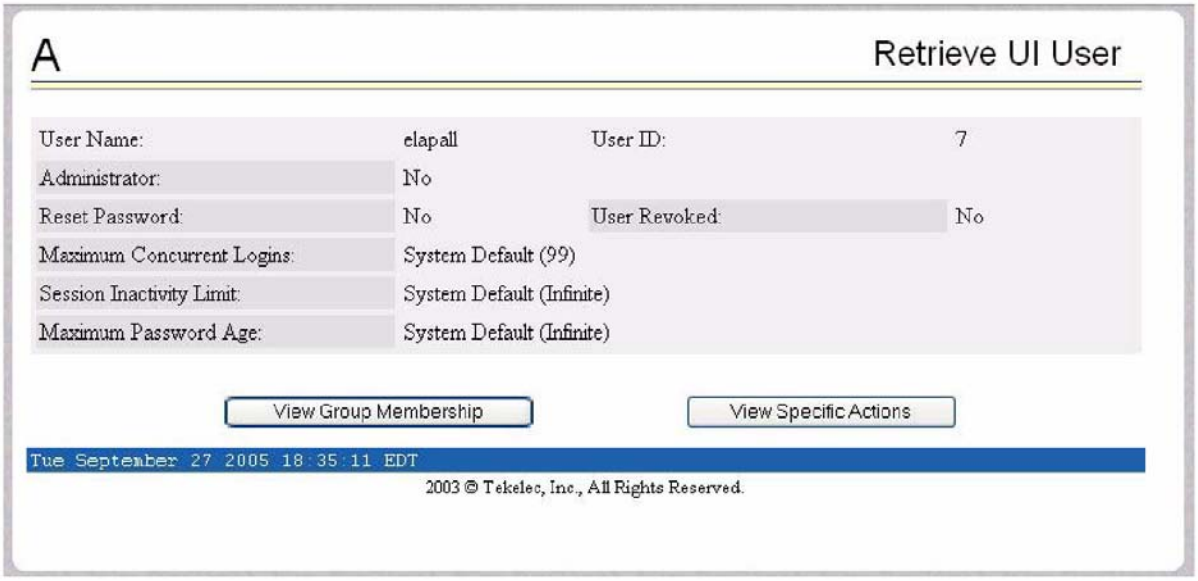
Figure 3-146. Select a User to Retrieve Screen



After you select a User Name in the screen above, the screen to view the user permissions appears, as shown in **Figure 3-147** . There you can view the permissions allowed to this user.

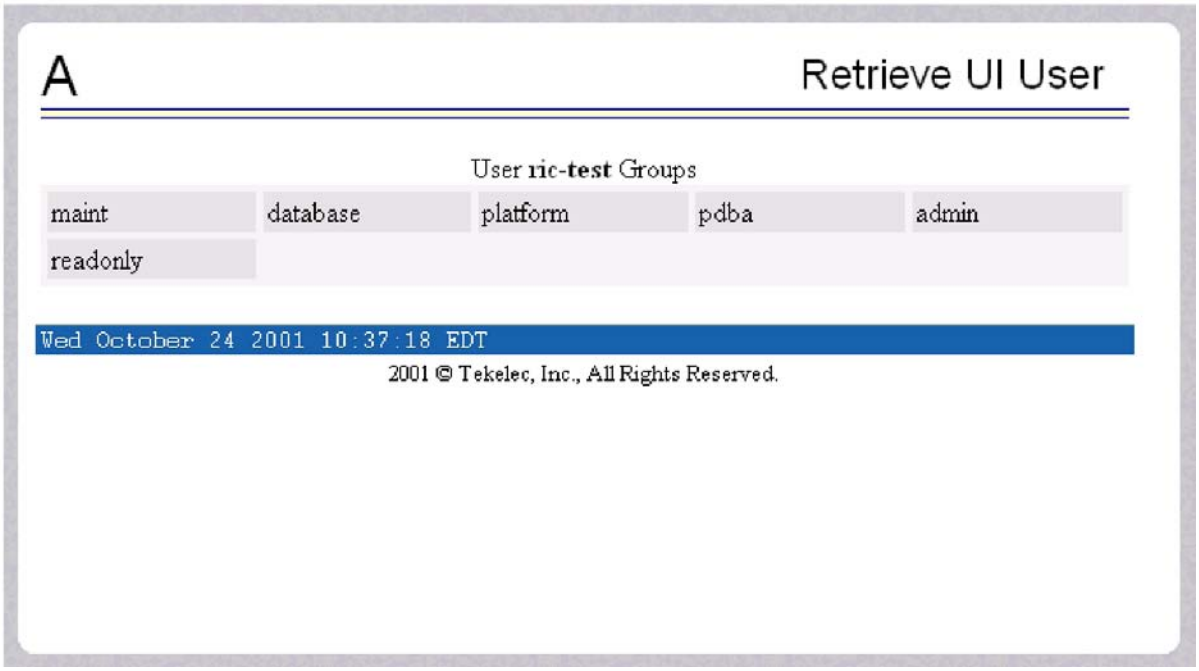
You can directly see certain information such as the maximum allowed number of concurrent log-ins and the inactivity time limit. In addition, you can go on to view the user's group membership data and specific actions (privileges). **Figure 3-147** shows the user's permissions and privileges.

Figure 3-147. Retrieval of UI User Information Screen



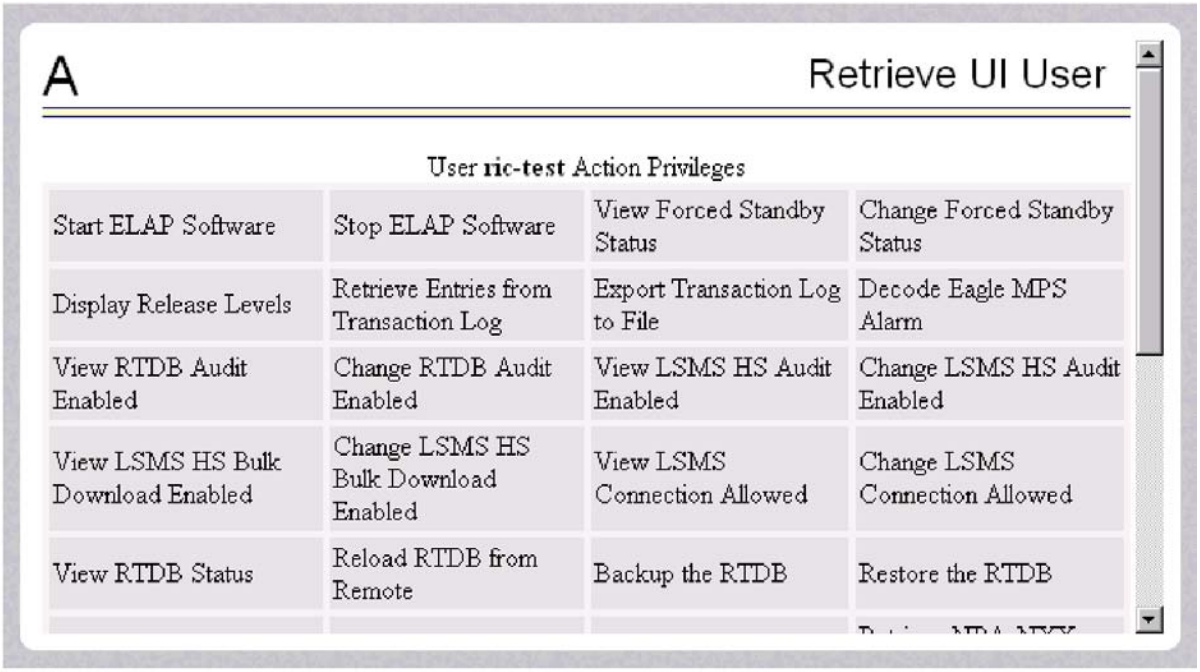
After you examine this screen, you can also continue to the view the group membership by clicking the View Group Membership button. You see the user's memberships in **Figure 3-148** .

Figure 3-148. Viewing the User's Group Membership Screen



When you click the View Specific Actions in the Retrieve UI User screen in **Figure 3-147** , you see the user privileges shown in **Figure 3-149** . This screen contains many privileges to display. **Figure 3-150** shows the continuation of the screen.

Figure 3-149. Viewing User Privileges

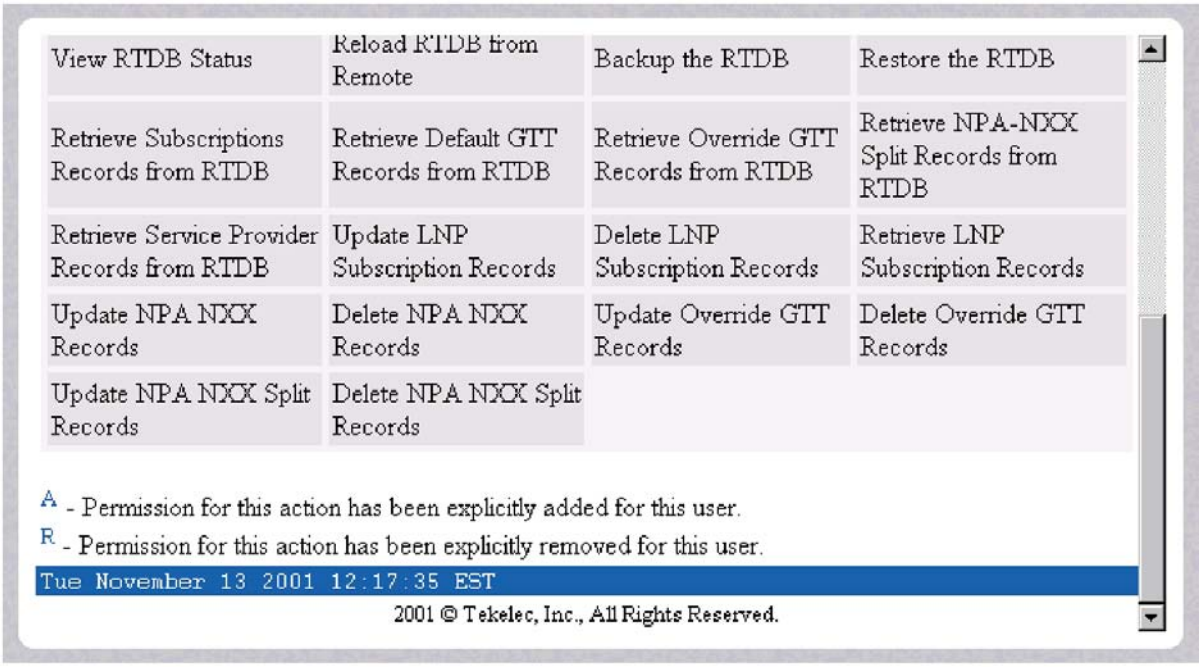


The bottom of **Figure 3-150** also can also have explanatory notes:

- A - Permission for this action has been explicitly added for this user.
- R - Permission for this action has been explicitly removed for this user.

These notes indicate the privileges specifically added or removed for an individual user from the group to which he/she is a member. These permissions allow individual variations to user privileges even though the user is a member of a group. See **Figure 3-150** .

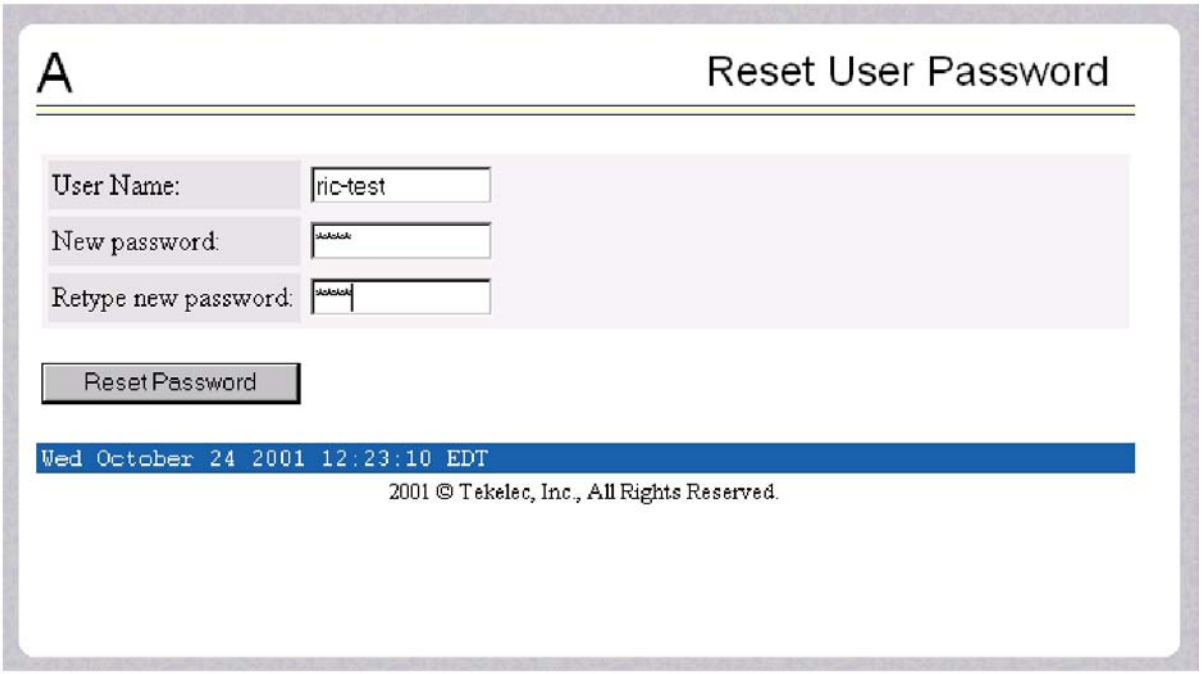
Figure 3-150. Continue Viewing User Privileges



Reset User Password

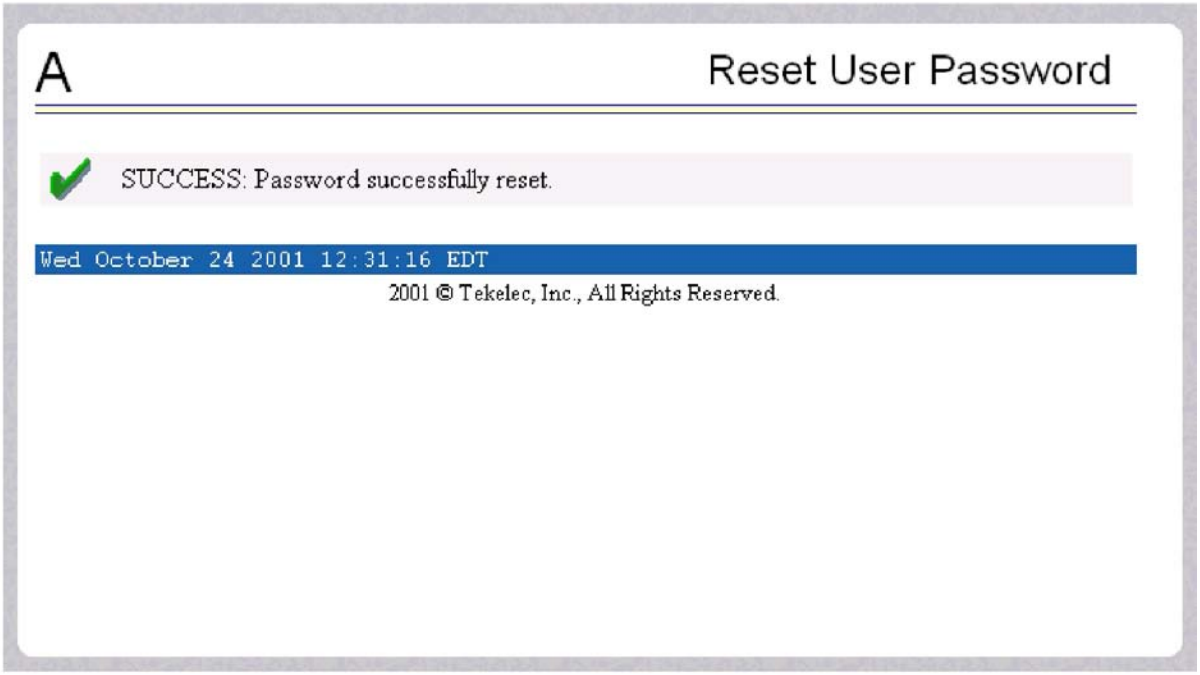
The User Administration / Users / Reset User Password screen lets you select a user name and change the password. See **Figure 3-151** .

Figure 3-151. Reset User Password Screen



Next, a confirmation screen appears when you correctly update the user's password, shown in **Figure 3-152** .

Figure 3-152. Confirming the Reset User Password



Groups Menu

The User Administration / Groups menu allows the user to administer action groups functions such as add, modify, delete, and retrieve. See the Groups menu in **Figure 3-153** .

Figure 3-153. User Administration / Groups Menu

For your convenience, actions can be grouped together. These groups can be used when assigning permissions to users. The groups can consist of whatever combinations of actions that system administrators deem reasonable. Group permissions allow any given action to be employed by more than one group.

Groups can be added, modified, deleted, and viewed through the menu items in the User Administration / Groups menu.

NOTE: The ELAP User Interface concept of groups should not be confused with the Unix concept of groups. The two are not related.

The ELAP user interface comes with pre-defined groups with the same names and action permissions used in the text-based (ELAP version 1.0) user interface:

- **`maint`**
- **`database`**
- **`platform`**
- **`debug`**
- **`admin`**

One additional pre-defined group used is new to ELAP version 3.0. This group is called **`readonly`**. The readonly group contains only actions that view status and information. The readonly group is the default group for new users.

The Groups menu performs the following actions:

- Add Group
- Modify Group
- Delete Group
- Retireve Group

Add Group

The User Administration / Groups / Add Group screen lets you enter a new user interface group and assign action privileges with the new group. See **Figure 3-154** for the Add UI Group screen.

Figure 3-154. Add UI Group Screen

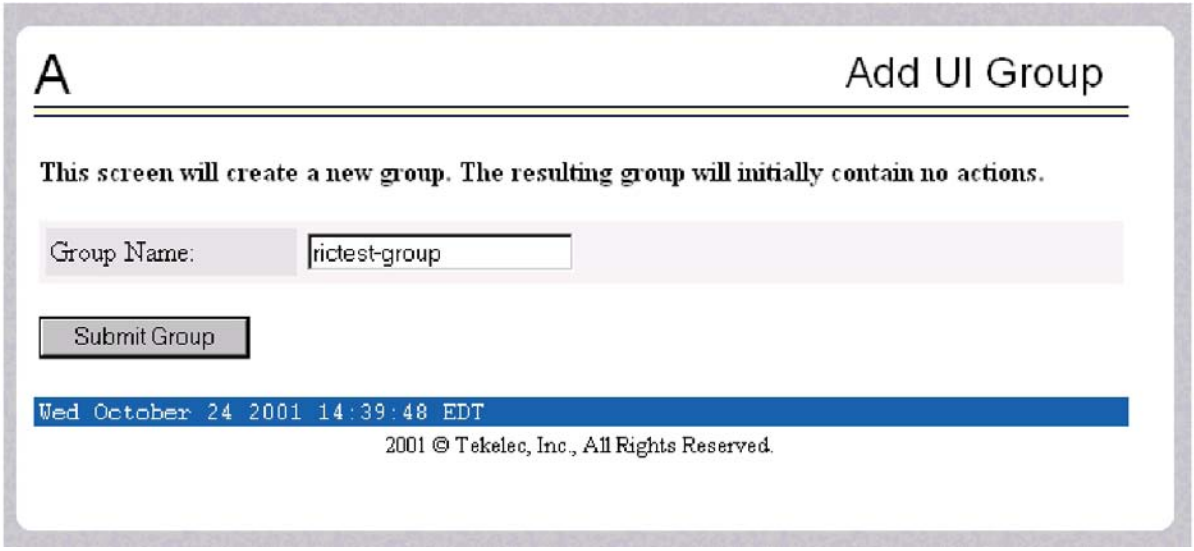
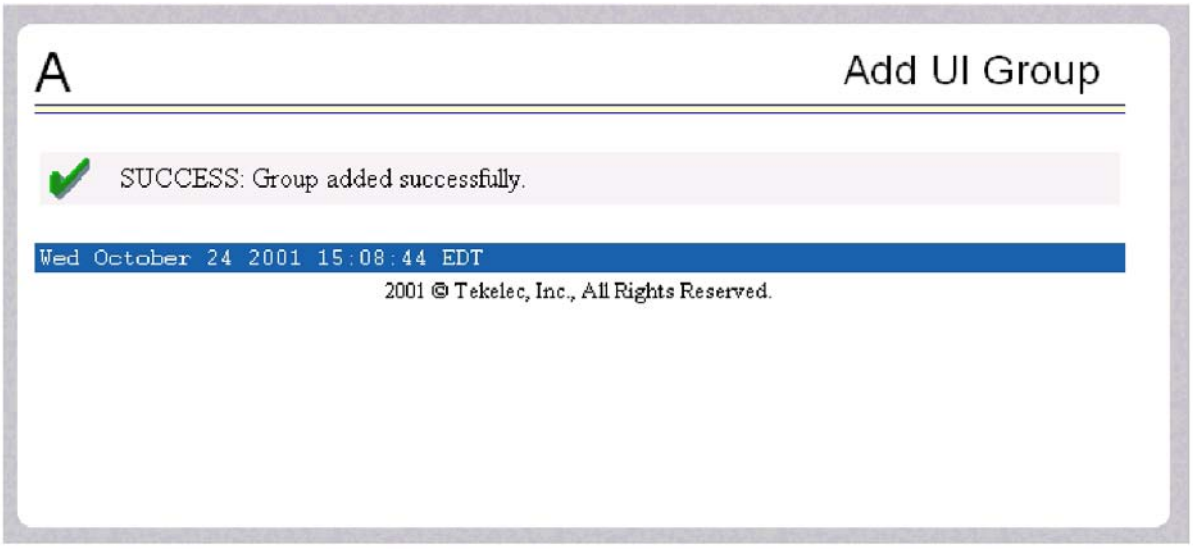


Figure 3-155 shows the screen confirmation of the newly added user interface group.

Figure 3-155. Confirming a New Group

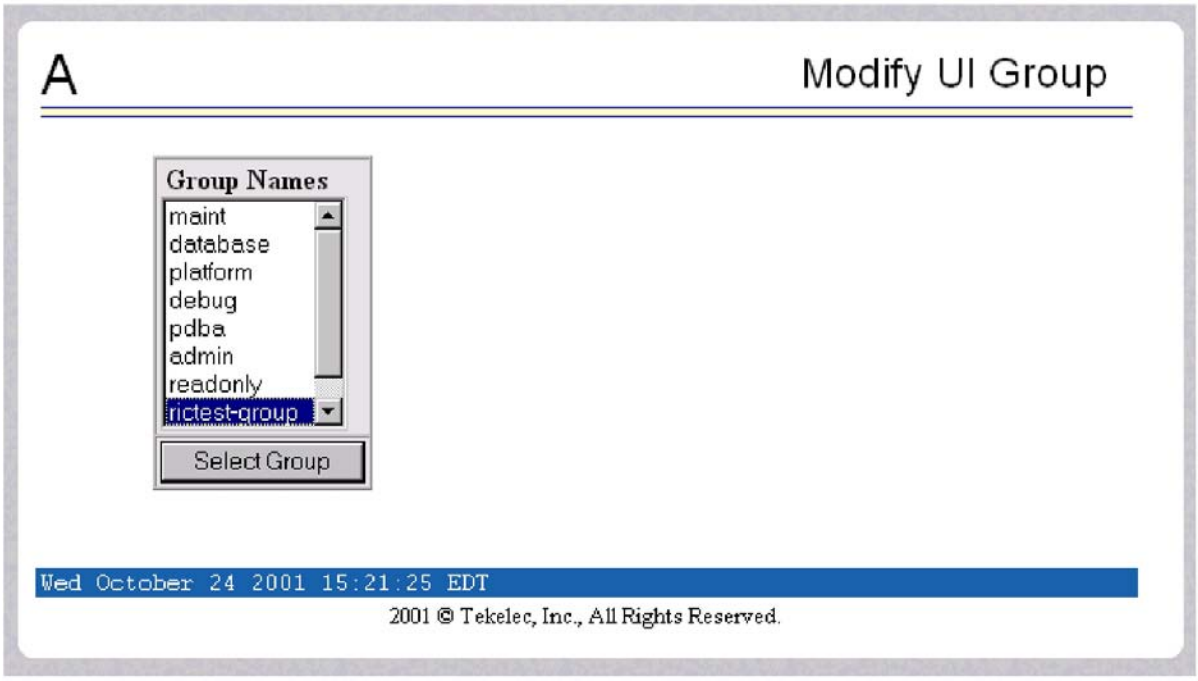


When you receive the successful group added message, you should proceed to the Modify Group and assign the Action Privileges for the new group.

Modify Group

The User Administration / Group / Modify Group screen lets you administer user interface group permission profiles. Select the Group Name, and click the Select Group button. **Figure 3-156** shows a sample Modify UI Group screen.

Figure 3-156. Modify UI Group Screen



When you have selected the group, the Modify Group Permission Profiles screen shows the current action privileges assigned to the user interface group. See **Figure 3-157** and **Figure 3-158** for the beginning and end of the Action Privileges.

Figure 3-157. Viewing a Group for Modification

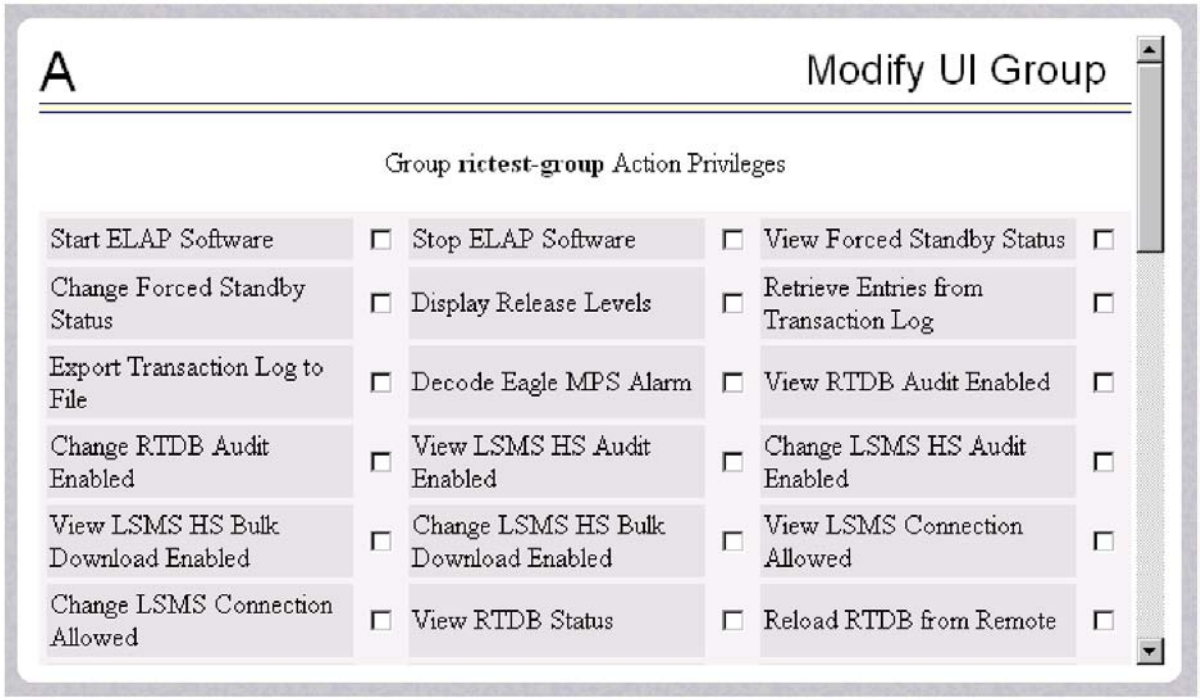
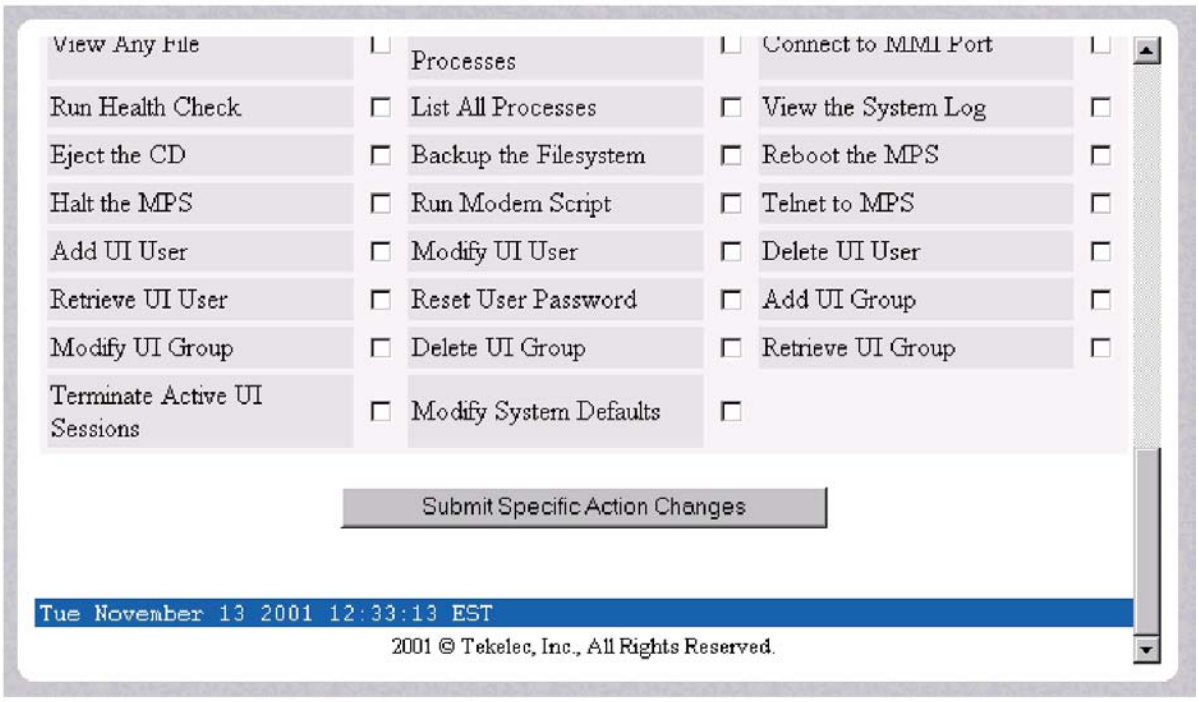
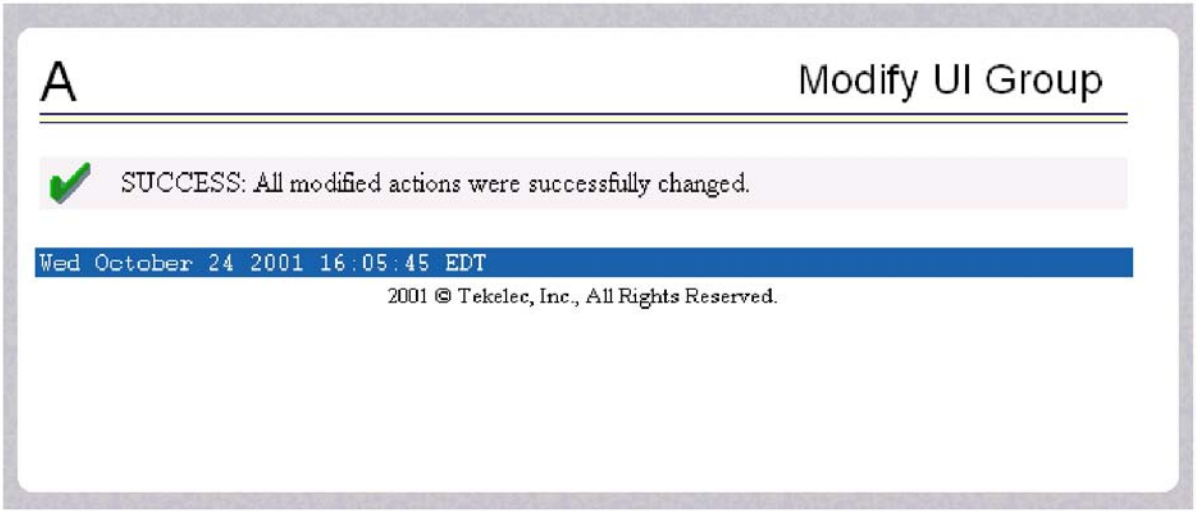


Figure 3-158. Continuing to View a Group for Modification



When you specify the Action Privileges you want to assign to this user interface group and click the Submit Specific Action Changes, you see the screen confirming the changes, as in **Figure 3-159** .

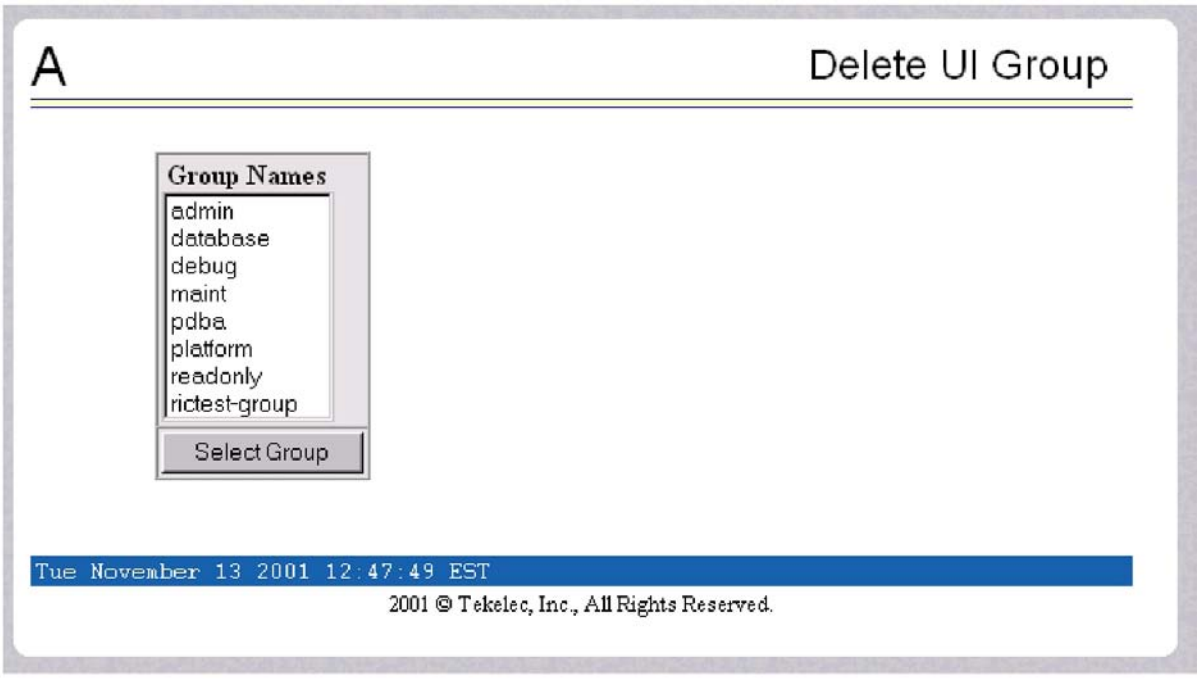
Figure 3-159. Confirming Modify UI Group Action Privileges



Delete Group

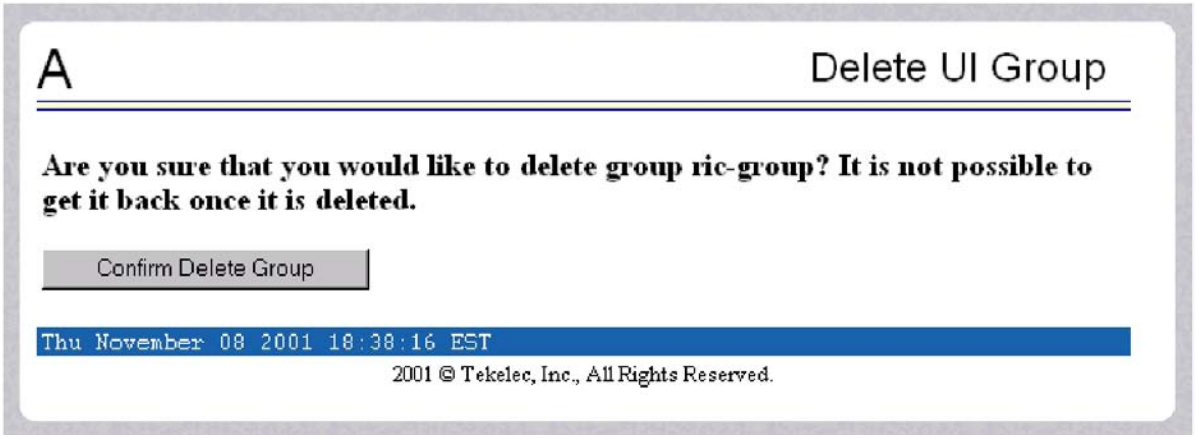
The User Administration / Group / Delete UI Group screen lets you remove a user interface group from the user interface information. The administrator must first select the user interface group name for deletion, as shown in **Figure 3-160** .

Figure 3-160. Select a Group for Deletion Screen



When you click the Select Group button, a confirmation banner and button appear, as shown in **Figure 3-161** .

Figure 3-161. Confirming the Delete Group



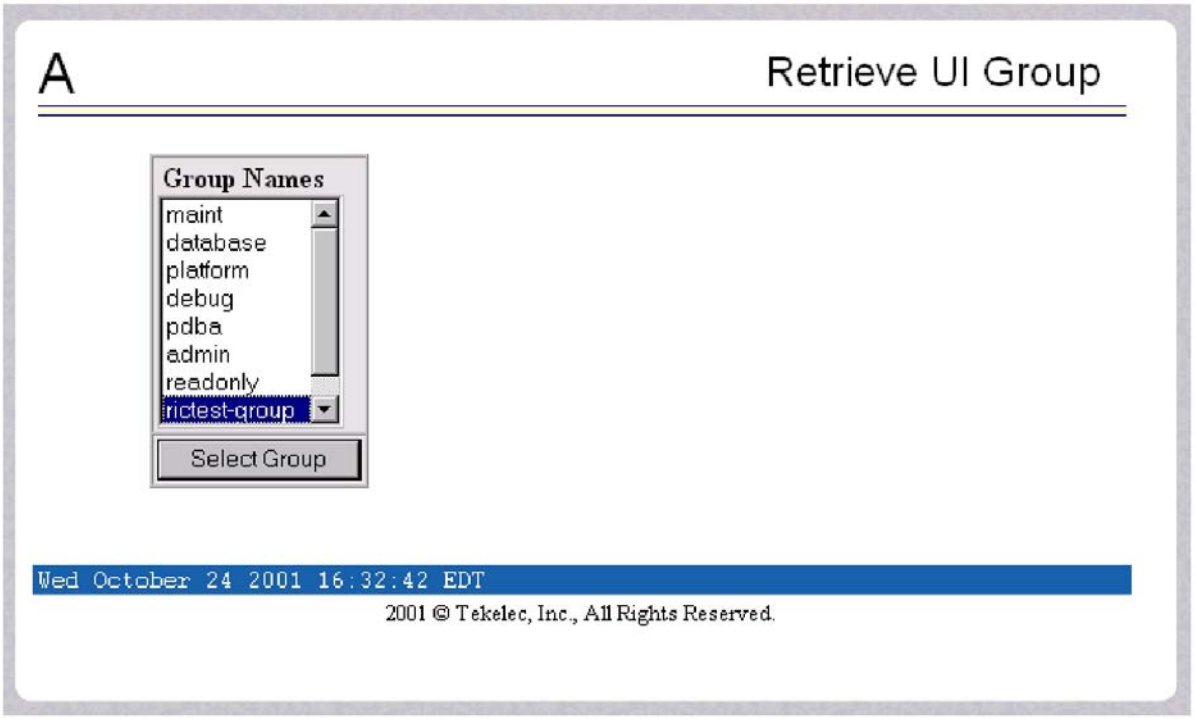
Finally, select the Confirm Delete Group button to delete the user interface group name and its permissions. See **Figure 3-162** .

Figure 3-162. Success in Delete UI Group

Retireve Group

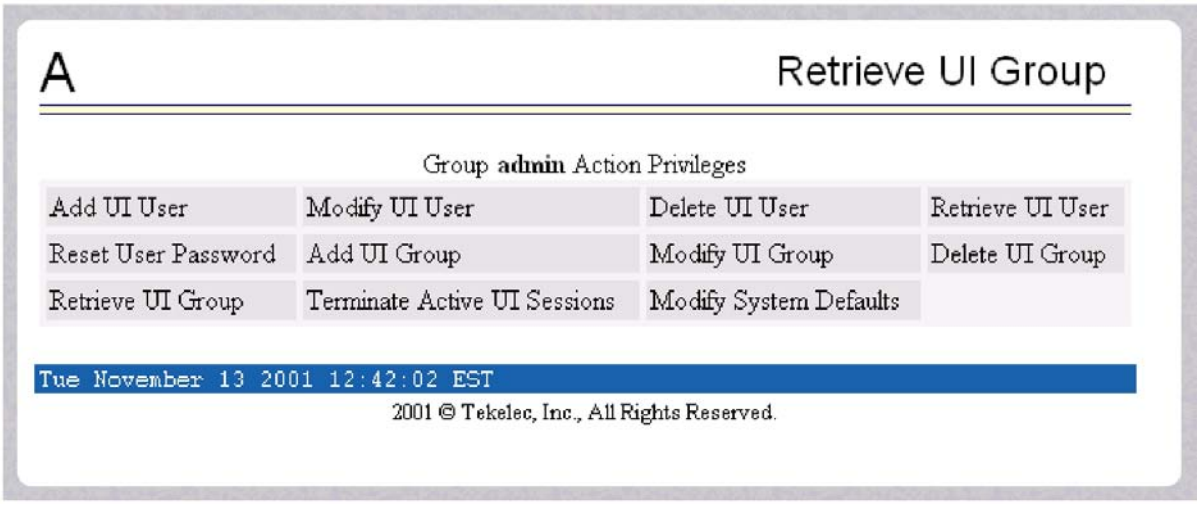
The User Administration / Users / Retrieve Group screen lets you display the permission profiles for user interface groups from the user interface information. First select a user interface group name to be retrieved, and click the Select Group button, as shown in **Figure 3-163** .

Figure 3-163. Retrieve UI Group Screen



After you select a Group Name in the screen above, the screen to view the group permissions appears, as shown in **Figure 3-164** . There you can view the permissions allowed to this user interface group. All you see is the actions supported for the group, as illustrated in **Figure 3-164** .

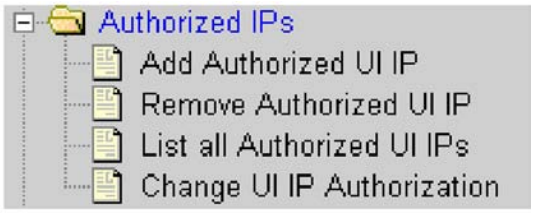
Figure 3-164. Retrieval of UI User Information Screen



Authorized IP Address Menu

The User Administration / Authorized IP menu lets you add, remove, and list all authorized UI IP addresses and also change the UI IP address authorization status. **Figure 3-165** shows the Authorized IP menu.

Figure 3-165. Authorized IP Address Menu



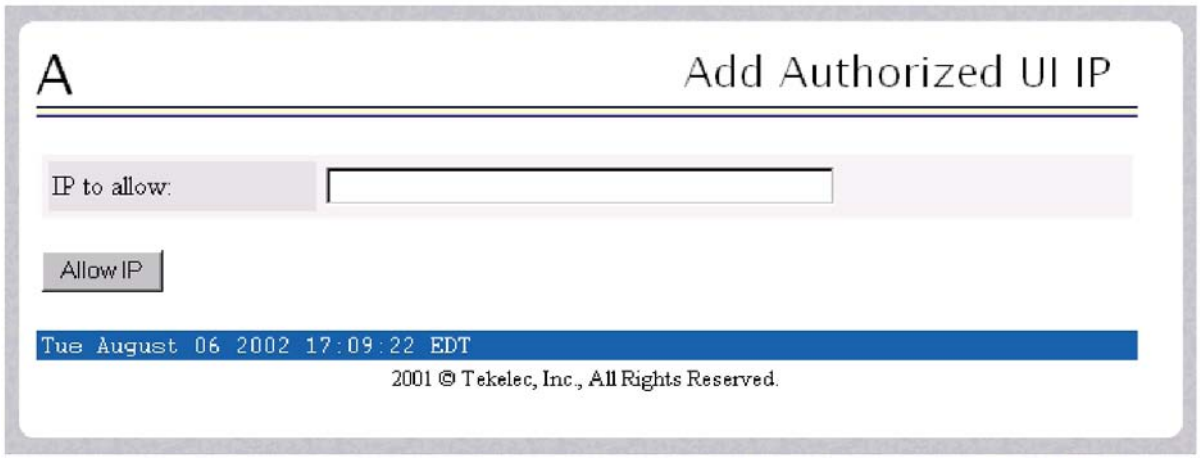
The PDBA / Authorized IP menu provides these actions:

- Add Authorized UI IP Address Screen
- Remove Authorized UI IP Address Screen
- List All Authorized UI IP Addresses
- Change UI IP Authorization Status

Add Authorized UI IP Address Screen

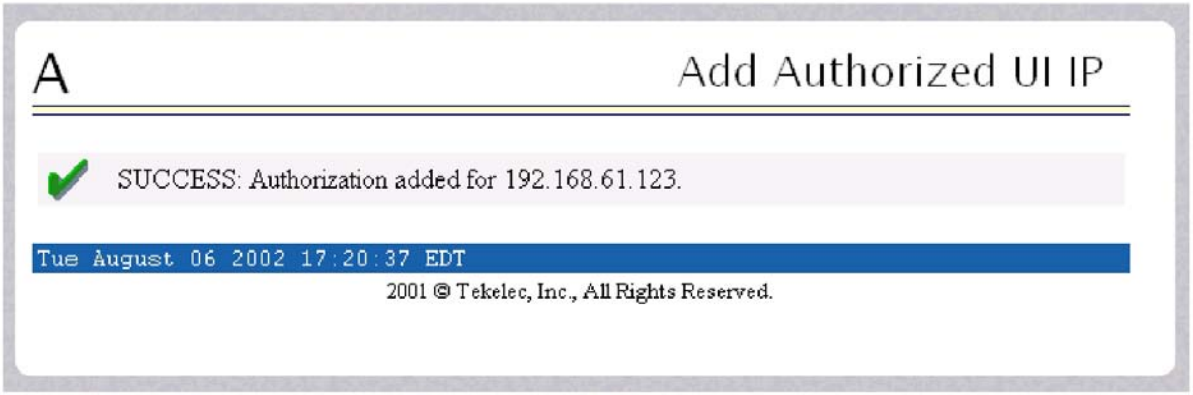
The User Administration / Authorized IP / Add Authorized UI IP screen lets you add a new IP address to the list of authorized IP addresses. Note that a pop-up syntax box appears when the cursor is positioned over the input field. See **Figure 3-166** for the Add Authorized UI IP screen.

Figure 3-166. Add Authorized UI IP Screen



Enter the IP address you want authorized and press the Allow IP button. When an authorized IP address is accepted, you see the message indicating a successful acceptance of the address in **Figure 3-167** .

Figure 3-167. Successfully Adding an Authorized UI IP Address

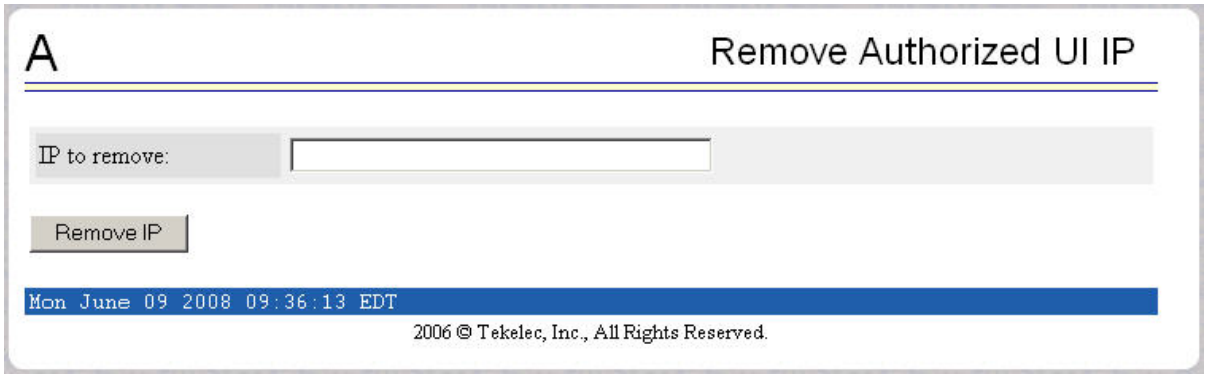


An error notification screen appears when a duplicate IP address is entered (the address already exists), when an attempt to add more than the maximum allowable number of addresses (i.e., more than 1,000), or when any internal failure is detected.

Remove Authorized UI IP Address Screen

The User Administration / Authorized IP / Remove Authorized UI IP screen lets you remove an IP address from the list of authorized IP addresses. You must enter the individual IP address or Classless Interdomain Routing Format (CIDR) IP format in the 'IP to Remove' input field. A pop-up syntax box appears when the cursor is positioned over that input field. See **Figure 3-168** for an example of the Remove Authorized UI IP screen.

Figure 3-168. Remove Authorized UI IP Screen



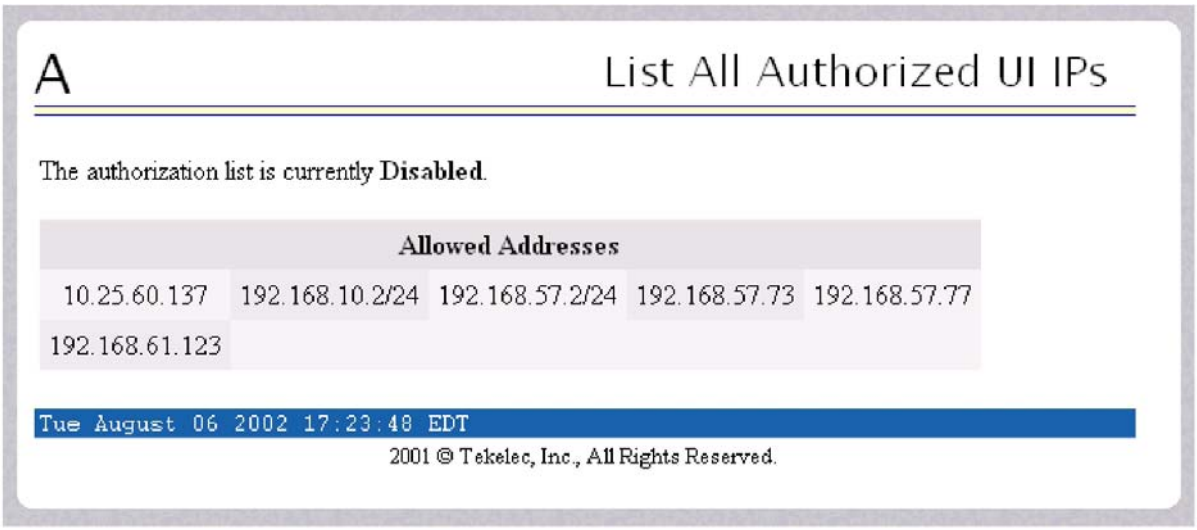
When the authorized IP address is deleted, you see the message confirming the removal of the specified address, as shown in **Figure 3-169** .

Figure 3-169. Successfully Removing an Authorized UI IP Address

List All Authorized UI IP Addresses

The User Administration / Authorized IP / List All Authorized UI IPs screen retrieves and displays all authorized IP addresses. The screen also shows whether the authorization list is Enabled or Disabled. See **Figure 3-170** for an example of the List All Authorized UI IP address screen.

Figure 3-170. List All Authorized UI IP Addresses Screen



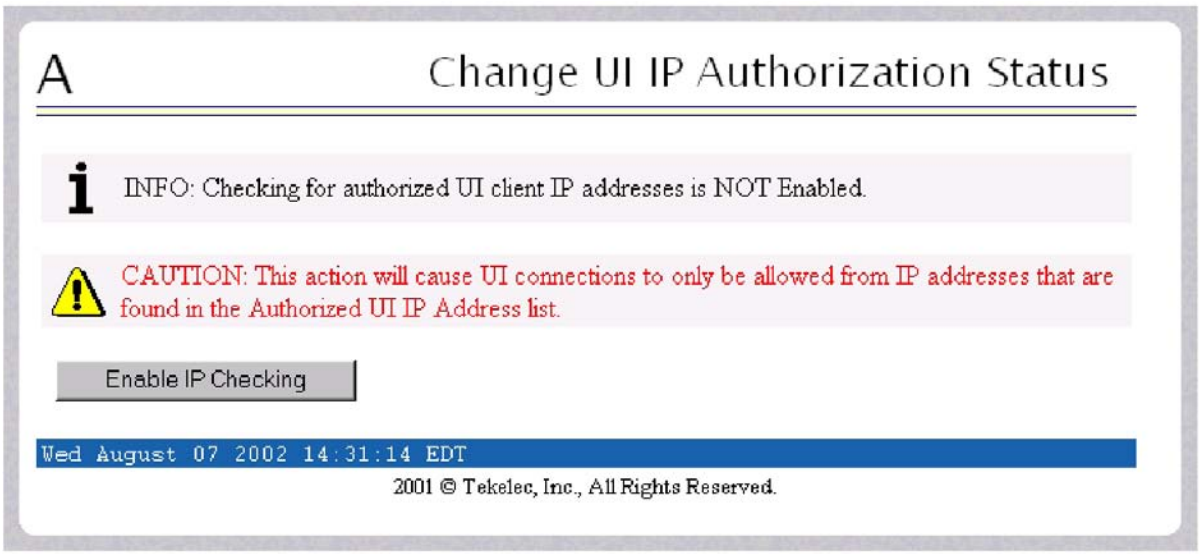
For information about enabling and disabling the authorization list, see . Change UI IP Authorization Status .

Change UI IP Authorization Status

The User Administration / Authorized IP / Change UI IP Authorization Status screen permits toggling (that is, alternating) the state of authorization list between 'enabled' and 'not enabled.'

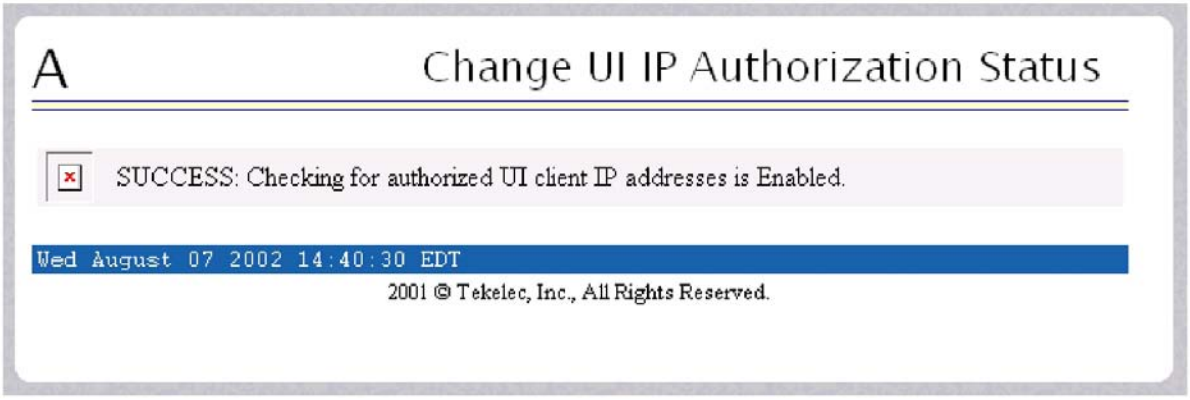
When this menu option is chosen, the current authorization state is displayed in the INFO field. See **Figure 3-171** for an example of the Change UI IP Authorization Status screen.

Figure 3-171. Change UI IP Authorization Status Screen



In the example above, the figure shows the authorization state is 'NOT Enabled.' To toggle the state to Enabled, click the Enable IP Checking button. See **Figure 3-172** for an example of the authorization status having been successfully toggled to the opposite state, now 'Enabled.'

Figure 3-172. Toggling the UI IP Authorization Status

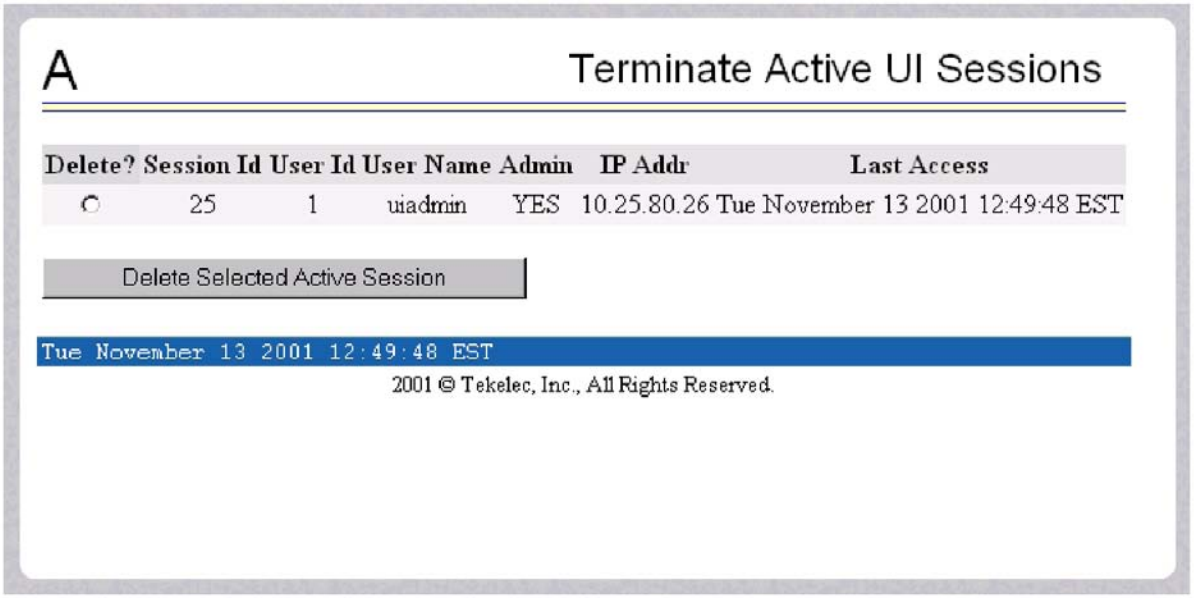


The enforcement of the checking for authorization status is immediate. The IP address of every message of every IP device using the GUI is checked as soon as the authorization status is enabled. The checking for authorized IPs does not occur only when devices log in.

Terminate Active UI Sessions

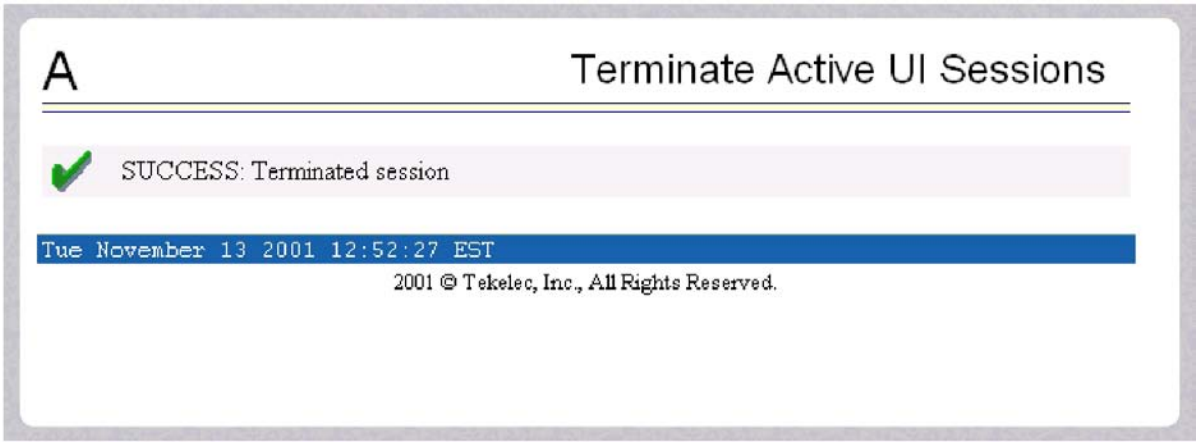
The User Administration / Terminate Active Sessions screen allows the administrator to selectively terminate individual active user interface sessions. See the Terminate Active Sessions screen in **Figure 3-173** .

Figure 3-173. Terminate Active Sessions Screen



The administrator selects a user interface session for termination, by clicking a Session in its **Delete?** column. A successful termination is shown in **Figure 3-174** .

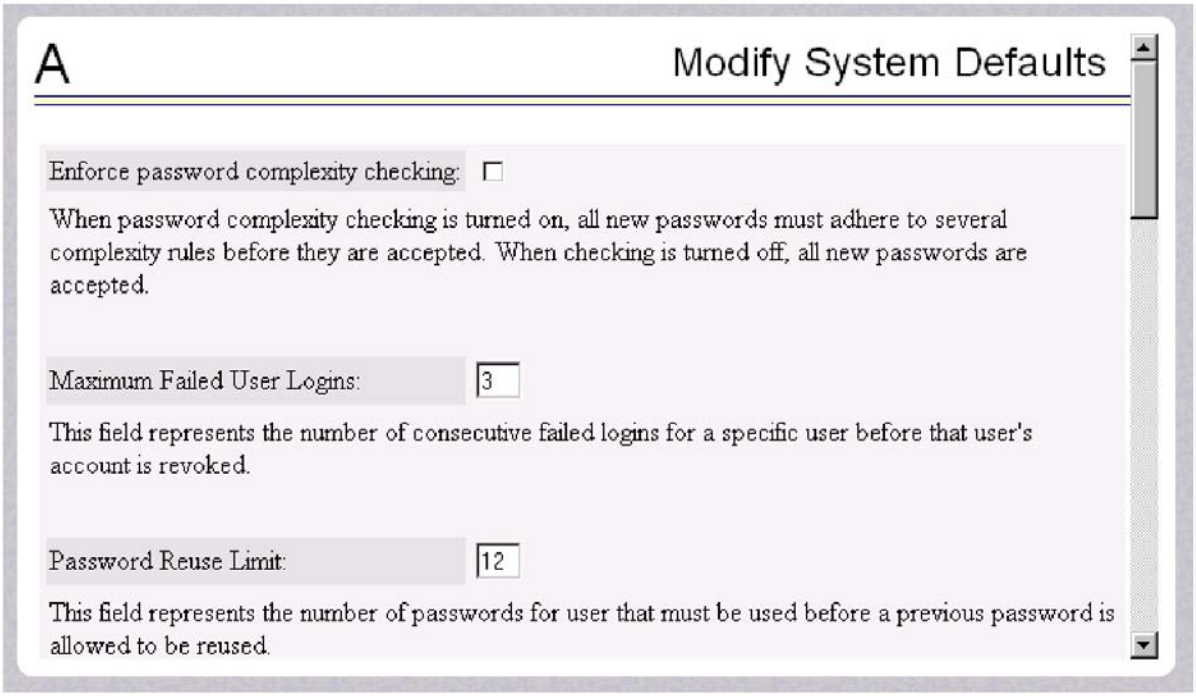
Figure 3-174. Confirmation of Session Termination



Modify System Defaults

The User Administration / Modify System Defaults screen allows the administrator to manage the systems defaults from this screen. See the start of the Modify System Defaults screen in **Figure 3-175** .

Figure 3-175. Modify System Defaults Screen



The system defaults that you can modify are the following.

- Enforce password complexity checking: When password complexity checking is enforced, all new passwords must adhere to several complexity rules before they are accepted. When checking is not enforced, all new passwords are accepted.

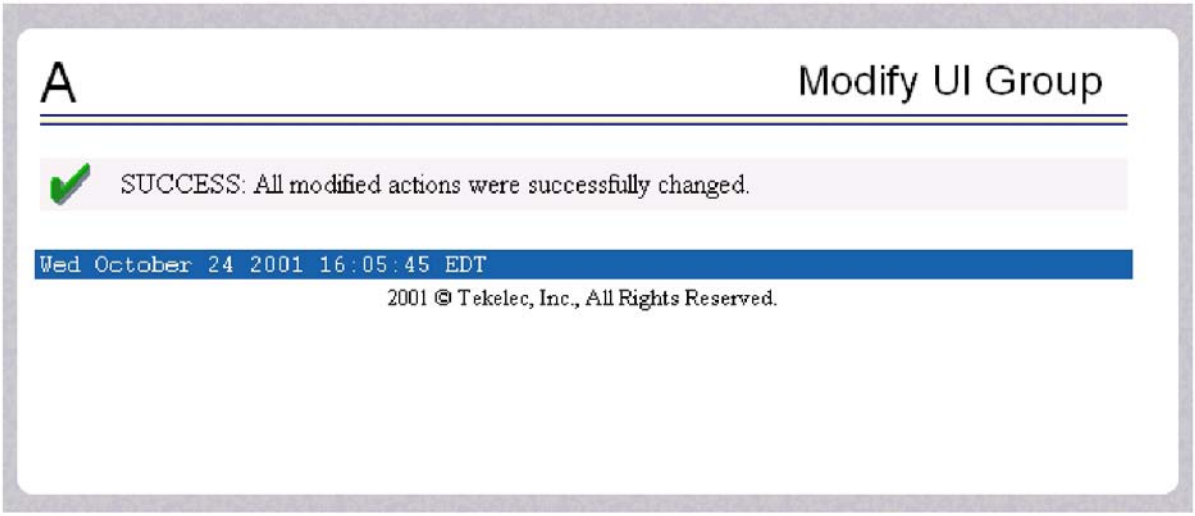
- Maximum Failed User Logins: This field specifies the number of consecutive failed logins allowed for a specific user before that user's account is revoked.
- Password Reuse Limit: This field requires a specified number of unique passwords that a user must use before accepting a previous password.
- Maximum Account Inactivity: This field specifies the maximum number of days that a user account can be idle before the account is automatically revoked.
- Session Idle Timeout: This field limits the number of minutes that an open session can remain idle before the server automatically closes the session.
- Maximum Password Age: This field limits the number of days that a user can have the same password before requiring him/her to change it.
- Maximum Concurrent User Logins: This field limits the number of concurrent login sessions that each user can have. This limitation does not apply to users with Administrative privileges.
- Maximum Concurrent Logins: This field limits the number of concurrent login sessions that can exist on the ELAP pair. Users with Administrative privileges are excluded from this total session count.
- Login Message Text: This field contains the text message displayed in the initial work area at login. The field is limited to 255 characters. The default text is:

  `NOTICE: This is a private computer system. Unauthorized access or use may lead to prosecution.`

- New User Default Groups: This field contains a list of group names (comma-delimited) with which newly created users are automatically assigned. The default group name is **`readonly`**.

When you complete the changes to the Modify System Defaults, click the Submit Defaults button. A successful change is shown in **Figure 3-176** . This screen confirms your changes.

Figure 3-176. Confirming Modify System Defaults Screen

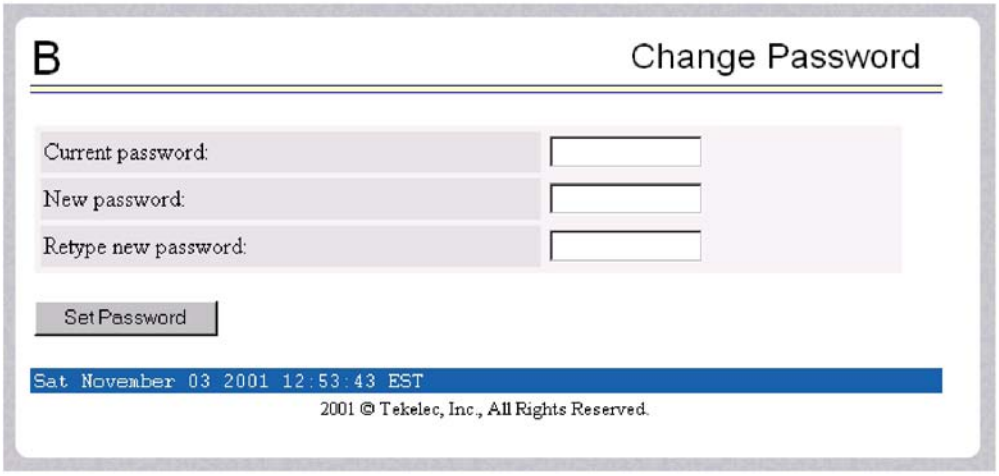


Change Password

The Change Password menu selection provides you, the ELAP user, with a screen to change your password. This basic action is available to all users and is accessible from the main menu (Figure 3-11).

To change the password, you must enter the current password, enter the new password, and retype the new password. Click the Set Password button, as shown in Figure 3-177 .

Figure 3-177. Change Password Screen



With the ability to support many users comes the need for tighter security. The user interface addresses security concerns with various restrictions and controls. In many cases, the frequency or severity of these checks is configurable by the administrator at both a user specific and system-wide level.

Users are required to use a password to log in to the UI. The following rules govern passwords.

- Complexity: Tekelec recommends that the password consist of at least five alphanumeric characters. It must include at least one alphabetic, one numeric, and one special (that is, punctuation) character. The password can contain a maximum of eight characters. It cannot include the **`userid`**.

  Note: The default value for this password complexity rule is not required.

- Aging: Users can be forced to change their passwords after a certain number of days. The administrator can set a maximum password age as a default for the system. The administrator can also specify a different maximum password age for any individual user, if that is desired.

- Force Change on Initial Login: Users can be forced to change their password the first time that they log in. The administrator can assigns a password to a user, either when the user is first created or when the password of an existing user is reset, and the user must change the password the first time that he/she logs in.

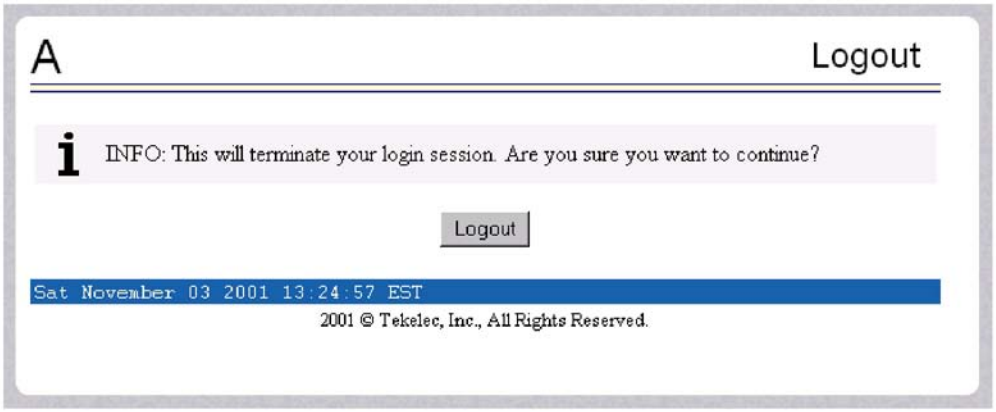
- Password Reuse: Users cannot reuse their last N passwords. N is a system-wide configurable number, with the default of **`5`** (five). The administrator can turn off this restriction by setting N to **`0`** (zero).

Logout

The Logout menu selection allows you to confirm logging out of the current session. This basic action is available to all users and is accessible from the main menu (Figure 3-11).

To logout, you are notified by the screen that this terminates your current session, and gives you the opportunity to continue or not. Click the Continue button to complete the logout, shown in **Figure 3-178** .

Figure 3-178. Logout Screen



When you have continued with the logout, the screen returns to the screen showing the Tekelec ELAP UI Login screen (see **Figure 3-2**).

ELAP Messages

ELAP Error Messages

Table 3-3 lists all of the possible error codes and associated text that the ELAP user interface can generate. The <> fields indicate values that are different for each error; they are filled in at run time.

Table 3-3. ELAP Error Messages

E1000	Unknown error <*error number*>. No error text is available.
E1001	Invalid menu selection: <*menu selection*>
E1002	Invalid syntax: <*input*>
E1003	Mate ELAPs may not have the same designation.
E1004	ELAP software is running. You must stop the ELAP software before performing this operation.
E1005	ELAP software is not running. You must start the ELAP software before performing this operation.
E1006	Mate ELAP not available
E1007	Could not eject media: <*device*>
E1008	Could not read file: <*file name*>
E1009	Active PDBA is not available.
E1010	This host is not an ELAP.
E1011	Cannot find ELAP <*A*|*B*> (host name <*host name*>)

E1012	Subscription (SP= <*subscription number*>) does not exist.
E1013	Subscription (SP= <*subscription number*>) already exists.
E1014	SP <*identifier*> does not exist.
E1015	IMSI <*identifier*> does not exist.
E1016	DN <*identifier*> does not exist.
E1017	PDBI error: <*error text*>
E1018	DN <*identifier*> already associated with IMSI <*identifier*>.
E1019	Device <*device*> unavailable.
E1020	Remote PDB unavailable.
E1021	IP address <*address*> is not authorized for PDB access.
E1022	RN <*identifier*> does not exist.
E1023	Invalid value for <*prompt >: <value*>: Valid values are <*range*>. Hit the Escape key to abort the command.
E1024	MTSU error: <*error text*>
E1025	File lock failed: <*file name*>
E1026	Environment variable <*variable name*> not defined.
E1027	ssh error: <*error text*>
E1028	IP address <*IP address*> is already authorized for PDBI access.
E1029	IP address <*IP address*> is not authorized for PDBI access.
E1030	Operation timed out waiting for a response from the PDBA.
E1031	Operation timed out waiting for a response from the RTDB.
E1032	Operation aborted by user.
E1033	Unexpected response received from the PDBA: id=<*txid*>, return code=<*return code*>
E1034	Unexpected response received from the RTDB: id=<*txid*>, return code=<*return code*>
E1035	Script <*script name*> failed: status=<*status*>
E1036	ELAP configuration failed. Please use the configuration menu to manually configure the ELAP sync and DSM networks.
E1037	One or more ELAP software processes did not start
E1038	One or more ELAP software processes did not stop
E1039	Transaction log query failed: <*error text*>
E1040	Transaction log response file was not created.
E1041	Transaction log response file could not be parsed.
E1042	Transaction log export failed: <*error text*>

E1043	The specified ELAP was not available.
E1044	Remote ELAP software is running. You must stop the remote ELAP software before performing this operation.
E1045	RTDB copy operation failed.
E1046	Improperly encoded alarm string. Re-check source.
E1047	RTDB did not respond to query.
E1048	Invalid response received from RTDB.
E1049	Could not connect to <*device or process*>: <*error text*>
E1050	Secure shell daemon is not running on mate ELAP. Config files could not be synchronized !!!
E1051	No feature(s) specified.
E1052	Both ELAP and EPAP features specified.
E1053	This action may only be performed on the local ELAP.
E1054	Another user is currently performing this same action.
E1055	Missing mandatory parameter: <*parameter*>
E1056	Unexpected parameter was provided:<*parameter*>
E1057	The ELAP must be in Forced Standby mode for this operation.
E1058	An internal error in the <*parameter*> occurred: <*error text*>
E1059	The passwords did not match.
E1060	The provisioning addresses for MPS A and B must be different.
E1061	The provisioning addresses for MPS A and B must be on the same network.
E1062	The default router must be on the same network as MPS A and MPS B.
E1063	The local and remote PDB addresses must be different.
E1064	This action may only be performed on ELAP A.
E1065	<*device or process*> must be configured.
E1066	The requested user <*user*> was not found.
E1067	The requested group <*group*> was not found.
E1068	The password entered was not correct.
E1069	The new password has been used too recently.
E1070	The provided password does not meet the security requirements. Reason: <*reason text*>
E1071	The specified group already exists.
E1072	This action may only be performed on ELAP B.
E1073	The file you have attempted to upload is larger than the <number> bytes of allocated storage space.

E1074	LPU batch failure: <error text>
E1075	This action must be done on the Active PDBA.
E1076	This action may only be performed while the LSMS connection is disabled.
E1077	File system violation: <error text>
E1078	File '<file name>' was empty
E1079	There are no PDBI connections available. Try again later.
E1080	The provisioning addresses for the main and backup networks must be different.
E1081	The specified IP already exists.
E1082	The specified IP does not exist.
E1083	The maximum number of authorized UI IPs has been reached.
E1084	This action may only performed on a provisionable MPS.
E1085	The specified address is local to this MPS.

ELAP Banner Information Messages

Table 3-4 lists the banner information messages that appear on the UI browser screen in the banner message box. These messages, sometimes referred to as ‘scroll by” messages, indicate the status of the ELAP machines.

Table 3-4. ELAP Informational Banner Messages

Attempt to correct MySQL replication failed
Backup Filesystem Failed
Backup filesystem in progress
Backup filesystem successful
Backup filesystem was aborted manually
Backup RTDB completed successfully
Backup RTDB failed
Backup RTDB in progress
Failure within filesystem backup utility. View backup_fs.fail log.
JRS Simplex Mode Enabled
MPS Reboot in Progress
MPS Resynchronization in Progress
MySQL Data replication error detected; Attempting to restore
MySQL Data replication restored: <reason>
MySQL Data Replication from <source> is Failing

Reload RTDB from <source> completed successfully
Reload RTDB from <source> failed
Reload RTDB from <source> in progress
Restore RTDB completed successfully
Restore RTDB failed
Restore RTDB in progress
Transaction log export failed: <reason>
Transaction log export in progress
Transaction log successfully exported to file: <file>

Table 3-5 lists the alarm related banner information messages that appear on the UI browser screen in the Message Box described on page 3-8. If any of the following alarm related messages appear, refer to the *Tekelec 1100 AS MPS Platform Software and Maintenance Manual* for the related corrective procedure.

Table 3-5. ELAP Alarm Related Banner Messages

LVM Snapshot Detected that is Too Old
LVM Snapshot Detected that is Too Full
LVM Snapshot Detected with Invalid Attributes
DRBD Split Brain
Uncorrectable ECC Memory Error
LSMS DB Maintenance Required
Server Fan Failure
Server Internal Disk Error
Server RAID Disk Error
Server Platform Error
Server File System Error
Server Platform Process Error
Server RAM Shortage Failure
Server Swap Space Shortage Failure
Server Provisioning Network Error
Server Eagle Network A Error
Server Eagle Network B Error
Server Sync Network Error
Server Disk Space Shortage Error
Server Default Route Network Error

Server Temperature Error
Server Mainboard Voltage Error
Server Power Feed Unavailable
Server Disk Health Test Error
Server Disk Unavailable Error
Correctable ECC Memory Error
Server Power Supply 1 Error
Server Power Supply 2 Error
Breaker Panel Feed Error
Breaker Panel Breaker Error
Breaker Panel Monitoring Error
Mate ELAP Unavailable
RTDB Mate Unavailable
Congestion
File System Full
Log Failure
RMTP Channels Down
Fatal Software Error
RTDB Corrupt
RTDB Inconsistent
RTDB Incoherent
JRS to RTDB Connection Down
Transaction Log Full
RTDB 100% Full
RTDB Resynchronization in Progress
RTDB Reload Is Required
Mate PDBA Unreachable
PDBA Connection Failure
PDBA Replication Failure
RTDB DMS Over-Allocation
RTDB Maximum Depth Reached

Server Disk Space Shortage Warning
Server Application Process Error
Server Hardware Configuration Error
Server RAM Shortage Warning
Server Software Configuration Error
Server Swap Space Shortage Warning
Server Default Router Not Defined
Server Temperature Warning
Server Core File Detected
Server NTP Daemon Not Synchronized
Server CMOS Battery Voltage Low
Server Disk Self Test Warning
Server Reboot Watchdog Initiated
RMTP Channel A Down
RMTP Channel B Down
RTDB 80% Full
Standby PDBA Falling Behind
RTDB Tree Error

4

Messages, Alarms, and Status Reporting

MPS and ELAP Status and Alarm Reporting

The System Health Check (syscheck) utility runs automatically at least every five minutes, and can be run manually, to test for error conditions in each MPS Server and in each ELAP. See Run Health Check Screen and refer to the *Tekelec 1100 AS MPS Platform Software and Maintenance Manual* for more information about executing and viewing results from the System Health Check.

Alarms of minor, major, and critical levels of severity are reported for error conditions detected for the MPS hardware platform and for the ELAP application.

On the MPS, a critical alarm lights the Fault LED, a major alarm lights the Alarm 1 LED, and a minor alarm lights the Alarm 2 LED. If more than one alarm level is active, all applicable LED lights are illuminated (not just the most severe) until all alarms in that level are cleared.

Maintenance Blocks

MPS and ELAP have no direct means of accepting user input from or displaying output messages on EAGLE 5 ISS terminals. Maintenance, measurements, error, and status information are routed to the EAGLE 5 ISS through the primary Service Module card.

The Active ELAP generates and sends Maintenance Blocks to the primary Service Module card. One Maintenance Block is sent as soon as the IP link is established between the Active ELAP and the primary Service Module card. Additional Maintenance Blocks are sent whenever the ELAP needs to report any change in status or error conditions. The information returned in Maintenance Blocks is also included in the output of the **rept-stat-mps** command.

It is possible for the ELAP to be at a provisioning congestion threshold, and to be entering and exiting congested mode at a very high rate of speed. To minimize this “thrashing” effect, the ELAP is restricted to sending no more than one ELAP Maintenance Block per second.

ELAP Maintenance Block Contents

The ELAP sends Maintenance Blocks that contain (at a minimum) the following information. The actual states are defined in the description of the **rept-stat-mps** command in the *Commands Manual*.

- MPS major, minor, and dot software versions
- MPS Status (down/up)
- MPS Status (Active/Standby)

If the ELAP needs to report one or more alarm conditions, it inserts the appropriate alarm data string for the indicated alarm category into the Maintenance Block.

EAGLE 5 ISS Alarm Reporting

A 16-character hexadecimal alarm data string reports any errors found during the last System Health Check and the level of severity for each error. The first character (four bits) uniquely identifies the alarm severity for the alarm data. The remaining 15 characters (60 bits) uniquely identify up to 60 individual failure cases for the alarm category.

The System Health Check (syscheck) is responsible for forwarding platform errors to the application. The application combines the platform alarms with the application alarms and forwards all of this information to EAGLE 5 ISS. The information that is transferred is described in the *Tekelec 1100 ASMPS Platform Software and Maintenance Manual*.

Table 4-1 defines the application and platform alarms that are forwarded to the EAGLE 5 ISS. The EAGLE 5 ISS receives the alarm number, alarm text, and alarm data string recovered from the MPS/ELAP.

Table 4-1. EAGLE 5 ISS MPS Application and Platforms UAM Alarms

Alarm Number	Level	Device	Error Description
370	Critical	MPS A or B	Critical Platform Failure
371	Critical	MPS A or B	Critical Application Failure
372	Major	MPS A or B	Major Platform Failure
373	Major	MPS A or B	Major Application Failure
374	Minor	MPS A or B	Minor Platform Failure
375	Minor	MPS A or B	Minor Application Failure
250	Clearing	MPS A or B	MPS Available

Alarm Priorities

The ELAP sends the maintenance information, including the alarm data strings, to the EAGLE 5 ISS for interpretation. Alarm priorities determine which alarm category is displayed at the EAGLE 5 ISS terminal when multiple alarm levels exist simultaneously. EAGLE 5 ISS prioritizes the data and displays only the alarm category with the highest severity level and priority for each MPS.

If an alarm category of lower priority is sent from the MPS, the lower priority alarm category is not displayed on the EAGLE 5 ISS terminal until any higher priority alarms are cleared.

Multiple Alarm Conditions

Critical, major and minor alarms appear repeatedly in each alarm delivery to the EAGLE 5 ISS until the alarm condition clears.

If multiple alarms exist, the highest priority alarm category is the Active Alarm. The Active Alarm is shown in the output from the **`rept-stat-trbl`** command and the **`rept-stat-mps`**command, and the alarm count associated with this alarm is included in the **`rept-stat-alm`** command output.

Though only the highest priority alarm is displayed at the EAGLE 5 ISS terminal when multiple alarms are reported, you can use the EAGLE 5 ISS **`rept-stat-mps`** command to list the alarm data strings for all of the alarm categories with existing alarms. Then you can use the ELAP user interface maintenance menu item Decode EAGLE 5 ISS Output of MPS Alarms to convert the hexadecimal alarm data string to text. The output text shows the alarm category represented by the string and the alarm text for each alarm encoded in the string.

Service Module Card Status Requests

When the ELAP needs to know the status of a Service Module card, it can send a Service Module card Status Request to that Service Module card. Because status messages are sent over UDP, the ELAP broadcasts the Service Module card Status Request and all Service Module cards return their status.

Service Module Card Status Reporting to the ELAP

The ELAP needs to know the current status of various aspects of the Service Module cards. Accordingly, the Service Module card sends a Service Module card status message to the ELAP when the following events occur:

- When the Service Module card is booted
- When the Service Module card receives a Service Module card Status Request message from the ELAP
- When the Service Module card determines that it needs to download the entire database

  For example, the database could become totally corrupted, or a user could initialize the card.
- When the Service Module card starts receiving DB downloads or DB updates.

  When a Service Module card starts downloading the RTDB, or if the Service Module card starts accepting database updates, it needs to send a status message informing the ELAP of the first record received. This helps the ELAP keep track of downloads in progress.

Service Module Card Status Message Fields

The Service Module card status message provides the following information to the ELAP:

- Service Module card Memory Size

  When the Service Module card is initialized, it determines the amount of applique memory present. The ELAP uses this value to determine if the Service Module card has enough memory to hold the RTDB.
- Load Mode Status

  This flag indicates whether or not 80% of the IS-NR LIMs have access to SCCP services.
- Database Level Number

  The ELAP maintains a level number for the RTDB. Each time the database is updated, the level number will be incremented. When the database is sent to the Service Module card, the Service Module card keeps track of the database level number. The database level number is included in all Status messages sent from the Service Module card. A level number of 0 signifies that no database has been loaded into the Service Module card (this can be done any time the Service Module card wants to request a full database download).
- Database Download Starting Record Number

  When the Service Module card starts downloading either the entire RTDB or updates to the database, it will identify the starting record number. This allows the ELAP to know when to wrap around the end of the file, and when the Service Module card has finished receiving the file or updates.

System Hardware Verification

Service Module card loading verifies the validity of the hardware configuration for the Service Module cards. The verification of the hardware includes:

- Validity of the Service Module card motherboard
- Verification of daughterboard memory size

System hardware verification includes checks for the appropriate LNP capable hardware when the feature bit is on. If the hardware is not capable, the feature bit cannot be turned on and the provisioning mode is set to LNP

Degraded. If capacity on the ELAP has exceeded the supplied feature keys, the Major MPS alarm is set and the Service Module cards will not load.

DSM Motherboard Verification

An AMD-K6 (or better) motherboard is required to support the LNP ELAP feature VSCCP application on the Service Module card. EAGLE 5 ISS maintenance stores the validity status of the Service Module card's motherboard configuration. The system does not allow the LNP ELAP feature to be enabled if the hardware configuration is invalid.

When the VSCCP application is initializing, it determines the motherboard type. If the motherboard is determined to be invalid for the LNP ELAP application, loading of the Service Module card is automatically inhibited and the card is booted through PMTC. Booting the card in this manner suppresses any obituary.

Service Module Card Daughterboard Memory Validation

The VSCCP application performs two types of memory validation to determine whether or not a Service Module card has sufficient memory to run the LNP ELAP VSCCP application: Local Memory validation and Continual Memory validation.

The report from the **rept-stat-sccp** command includes the daughterboard memory both allocated and physically present on each Service Module card. (See the *Commands Manual* for a description of the **rept-stat-sccp** command output.)

Local Memory Validation

Any time the LNP ELAP feature is enabled and a Service Module card is initializing, VSCCP checks to see if the Service Module card has at least one D1G daughterboard. After this is successful, VSCCP application requests the RTDB size from the MPS and determine if the Service Module card contains sufficient daughterboards to download the RTDB. These two checks occur before starting the data loading operation from the MPS.

Real-Time Memory Validation

Once communications between the Service Module card and ELAP have been established, and the Service Module card has joined the RMTP Tree, the ELAP starts downloading the RTDB to the Service Module card. After the Service Module card has downloaded the RTDB, it continues to receive database updates as necessary. The ELAP includes the size of the current RTDB in all records sent to the Service Module card. The Service Module card compares the size required to the amount of memory installed, and issues a minor alarm whenever the database exceeds 80% of the Service Module card memory. If the database completely fills the Service Module card memory, a major alarm is issued and the Service Module card status changes to IS-ANR/Restricted.

Actions Taken for Invalid Hardware

When the hardware configuration for a Service Module card is determined to be invalid for the LNP ELAP application, SCM automatically inhibits loading for that specific card. A major alarm is generated indicating that loading for that Service Module card has failed and that the card has been automatically inhibited (prevented from reloading again). When card loading is inhibited, the primary state of the card is set to OOS-MT-DSBLD and the secondary state of the card is set to MEA (Mismatch of Equipment and Attributes).

The following actions apply to a Service Module card determined to be invalid:

- The Service Module card will not download the EAGLE 5 ISS databases.
- The Service Module card will not download the RTDB from the ELAP.
- The Service Module card will not accept RTDB updates (additions, changes, and deletes) from the ELAP.

Refer to the *Tekelec 1100 AS MPS Platform Software and Maintenance Manual* to determine the appropriate corrective actions.

Service Module Card Memory Capacity Status Reporting

The Service Module card sends a message to the ELAP containing the amount of memory on the Service Module card board. The ELAP determines whether the Service Module card has enough memory to store the RTDB and sends an ACK or NAK back to the Service Module card indicating whether or not the Service Module card has an adequate amount of memory.

When the ELAP sends database updates to the Service Module cards, the update messages includes a field that contains the new database memory requirements. Each Service Module card monitors the DB size requirements and issues a minor alarm if the size of the DB exceeds 80% of its memory. If a database increases to the point that it occupies 100% of the Service Module card memory, a major alarm is issued.

The **`rept-stat-mps:loc=xxxx`** command shows the amount of memory used by the RTDB as a percent of available Service Module card memory (see rept-stat-mps).

Unstable Loading Mode

At some point, having a number of invalid Service Module cards will result in some of the LIMs being denied SCCP services. There is a threshold that needs to be monitored: if the number of valid Service Module cards is insufficient to provide service to at least 80% of the IS-NR LIMs, the system is said to be in an unstable Loading Mode.

The system interrupts and aborts card loading upon execution of an STP database change command. Loading Mode support denies the execution of STP database change commands when the system is in an unstable loading mode.

An unstable loading mode exists when any of the following conditions are true:

- The system’s maintenance baseline has not been established.
- Less than 80% of the number of LIMs provisioned are IS-NR or OOS-MT-DSBLD.

  The conditions that an insufficient number of Service Module cards are IS-NR or OOS-MT-DSBLD relative to 80% of the number of provisioned LIMs is called a failure to provide adequate SCCP capacity.
- The number of IS-NR and OOS-MT-DSBLD SCCP cards is insufficient to service at least 80% of all provisioned LIMs.

  Loading Mode is based on the ability of the system to provide SCCP service to at least 80% of the LIMs. No more than 16 LIMs can be serviced by each SCCP (or Service Module card.
- There is insufficient SCCP service, which occurs if an insufficient number of IS-NR Service Module cards are available to service at least 80% of the number of IS-NR LIMs.

  It is possible for LIMs or Service Module cards to be inhibited or to have problems that prevent them from operating normally. If enough Service Module cards are out of service, it may not be possible for the remaining IS-NR Service Module cards to service at least 80% of the number of IS-NR LIMs. This is called

"insufficient SCCP service." When this occurs, some of the LIMs will be denied SCCP service. It is possible to use the **inh-card** command to inhibit LIMs to bring the ratio back to 16:1 or better (see Actions Taken During System Unstable Loading Mode).

- If LIM cards are being denied SCCP service and any Service Module cards are in an abnormal state (OOS-MT, IS-ANR)

Actions Taken During System Unstable Loading Mode

- Unstable loading mode has no impact on RTDB downloads or the stream of RTDB updates.
- When the loading mode is unstable, the **rept-stat-sys** command will report the existence of the unstable loading mode and the specific trigger that caused it.
- When in an unstable Loading Mode, the EAGLE 5 ISS will not accept STP database updates. When updates are rejected, the reason will be given as "E3112 Cmd Rej: Loading Mode unstable due to SCCP service is deficient."

  The **inh-card** and **alw-card** commands can be used to alter SCCP service levels to achieve the 80% threshold. This can be repeated for each card until the system is able to supply SCCP services to at least 80% of the IS-NR LIMs. The remaining 20% LIM or supporting Service Module cards may remain out of service until the stream of STP database updates ceases. This stream of updates can be temporarily interrupted to allow the remaining 20% of the system to come in service.

  Once an STP database has been loaded, that database can be updated (as long as the system is not in an unstable Loading Mode). However, if an STP update comes in during STP database loading, the Service Module card will abort the current loading, issue a class 01D7 obit message (**Figure 4-1**), and reboot.

Figure 4-1. Obit Message for Abort of Card Loading

```
tekelecstp 97-04-08 12:29:04 EST EAGLE 35.0-31.8.0
   ------------------------------------------------------------------------
    STH: Received a BOOT Appl-obituary reply for restart
        Card 1317   Module RADB_MGR.C  Line  337  Class 01d7
        Register Dump :
            EFL=00000246    CS =0058        EIP=0000808d    SS =0060
            EAX=000a6ff3    ECX=000a0005    EDX=00000000    EBX=000a6fa0
            ESP=00108828    EBP=0010882c    ESI=001f1e10    EDI=00000000
            DS =0060        ES =0060        FS =0060        GS =0060

        Stack Dump :
        [SP+1E]=001f    [SP+16]=0000    [SP+0E]=000a    [SP+06]=0010
        [SP+1C]=1e10    [SP+14]=0004    [SP+0C]=6fa0    [SP+04]=8850
        [SP+1A]=0010    [SP+12]=001f    [SP+0A]=0004    [SP+02]=0001
        [SP+18]=886c    [SP+10]=4928    [SP+08]=7ec3    [SP+00]=504b

        User Data Dump :
        14 02 fa ed 01 01 1d 01 5a 01 00                    ........Z..

    Report Date:02-08-08  Time:12:29:04
```

- If executing the **ent-card** or **inh-card** command would cause the system to enter an unstable Loading Mode, it will be necessary to use the "Force" parameter on the command.

Commands

The commands described in this section report status information for the provisioning system.

rept-stat-db

The **rept-stat-db** command report includes the RTDB birthdate, level, and status. This information is used to help determine the need for and method to use for an RTDB resynchronization, audit and reconcile, reload from another RTDB, or bulk load from LSMS.

Figure 4-2. rept-stat-db Command Report Example

```
rept-stat-db:display=all:db=mps

                ELAP A  ( ACTV )
                 C  BIRTHDATE          LEVEL       EXCEPTION
                 -  -----------------  ----------  --------------
RTDB             Y  02-01-29 08:20:04       12345        -
RTDB-EAGLE          02-01-29 08:20:04       12345        -

                ELAP B ( STDBY )
                 C  BIRTHDATE          LEVEL       EXCEPTION
                 -  -----------------  ----------  --------------
RTDB             Y  02-01-29 08:20:04       12345        -
RTDB-EAGLE          02-01-29 08:20:04       12345        -

                EAGLE RTDB REPORT
CARD/APPL  LOC   C  BIRTHDATE          LEVEL       EXCEPTION
---------  ----  -  -----------------  ----------  --------------
VSCCP      1201  Y  02-01-29 08:20:04       12345        -
VSCCP      1203  Y  02-01-29 08:20:04       12345        -
VSCCP      1105  Y  02-01-29 08:20:04       12345        -
;
```

rept-stat-mps

The **rept-stat-mps** command reports the status of the provisioning system, including MPS platform status and ELAP status.

There are two possible variants of this command:

- **rept-stat-mps** - This produces a summary report showing the overall status of the provisioning system and a moderate level of information for each Service Module card.

- **rept-stat-mps:loc=xxxx** – This produces a more detailed report showing the status of a specific Service Module card.

  When the ELAP sends database updates to the Service Module cards, the update messages include a field that contains the new database memory requirements. This version of the **rept-stat-mps** command displays the amount of memory used by the RTDB as a percent of available Service Module card memory.

  Each Service Module card monitors the database size requirements, and issue a minor alarm if the size of the database exceeds 80% of its memory. If a database increases to the point that it occupies 100% of the Service Module card memory, a major alarm is issued.

Samples of the reports produced by these commands are shown in **Figure 4-3** :

Figure 4-3. `rept-stat-mps` Command Report Examples

```
0         1         2         3         4         5         6         7
01234567890123456789012345678901234567890123456789012345678901234567890123456789

rept-stat-mps
    Command entered at terminal #4.
;

    Integrat40 00-06-24 10:37:22 EST EAGLE 35.0.0-35.10.0

                       VERSION       PST            SST        AST
    ELAP A              027-015-000   OOS-MT         Fault      -----
        CRITICAL PLATFORM    ALARM DATA = No Alarms
        MAJOR    PLATFORM    ALARM DATA = h'0123456789ABCDEF
        MINOR    PLATFORM    ALARM DATA = h'0123456789ABCDEF
        CRITICAL APPLICATION ALARM DATA = No Alarms
        MAJOR    APPLICATION ALARM DATA = h'0123456789ABCDEF
        MINOR    APPLICATION ALARM DATA = No Alarms
              ALARM STATUS = ** 0371  Major Platform Failure(s)

                       VERSION       PST            SST        AST
     ELAP B             027-015-000   OOS-MT         Fault      -----
        CRITICAL PLATFORM    ALARM DATA = No Alarms
        MAJOR    PLATFORM    ALARM DATA = No Alarms
        MINOR    PLATFORM    ALARM DATA = No Alarms
        CRITICAL APPLICATION ALARM DATA = h'0123456789ABCDEF
        MAJOR    APPLICATION ALARM DATA = h'0123456789ABCDEF
        MINOR    APPLICATION ALARM DATA = No Alarms
              ALARM STATUS = *C 0373  Critical Application Failure(s)

    CARD   PST          SST       LNP STAT
    1106 P IS-NR        Active    ACT
    1201   IS-ANR       Active    SWDL
    1205   OOS-MT-DSBLD Manual    -------
    1302   OOS-MT       Fault     -------
    1310   IS-ANR       Standby   SWDL

    CARD 1106 ALARM STATUS = No Alarms
    CARD 1201 ALARM STATUS = No Alarms
    CARD 1205 ALARM STATUS = No Alarms
    CARD 1302 ALARM STATUS = ** 0013 Card is isolated from the system
    CARD 1310 ALARM STATUS = No Alarms

    Command Completed.
```

rept-stat-trbl

This command includes the Service Module card/ELAP IP link alarms.

Figure 4-4. `rept-stat-trbl`Command Output Example

```
> rept-stat-trbl
Command Accepted - Processing
    eagle10605 99-06-24 14:34:08 EST EAGLE 35.0.0
    rept-stat-trbl
    Command entered at terminal #10.
;
    eagle10605 99-06-24 14:34:08 EST EAGLE 35.0.0
    Searching devices for alarms...
;
    eagle10605 99-06-24 14:34:09 EST EAGLE 35.0.0
    SEQN UAM  AL DEVICE   ELEMENT      TROUBLE TEXT
    0002.0143  * CARD 1113 OAM         System release GPL(s) not approved
    0011.0176  * SECULOG 1116          Stdby security log -- upload required
    3540.0203 ** SLK 1201,A lsn1       REPT-LKF: lost data
    3541.0203 ** SLK 1201,B lsn4       REPT-LKF: lost data
    3542.0203 ** SLK 1202,A lsn2       REPT-LKF: lost data
    3544.0202 ** SLK 1203,A lsn3       REPT-LKF: HWP - too many link interrupts
    0021.0318 ** LSN lsn1              REPT-LKSTO: link set prohibited
    0022.0318 ** LSN lsn2              REPT-LKSTO: link set prohibited
    0023.0318 ** LSN lsn3              REPT-LKSTO: link set prohibited
    0010.0318 ** LSN lsn4              REPT-LKSTO: link set prohibited
    3537.0084 ** DSM A   1215          IP Connection Unavailable
    3536,0372 ** MPS A                 Major Platform Failure(s)
    0003.0313 *C DPC 010-010-003       DPC is prohibited
    0004.0313 *C DPC 010-010-004       DPC is prohibited
    0005.0313 *C DPC 010-010-005       DPC is prohibited
    0028.0313 *C DPC 252-010-001       DPC is prohibited
    0006.0313 *C DPC 252-010-003       DPC is prohibited
    0008.0313 *C DPC 252-010-004       DPC is prohibited
    0009.0313 *C DPC 252-011-*         DPC is prohibited
    0029.0308 *C SYSTEM                Node isolated due to SLK failures
Command Completed.
```

rept-stat-alm

This command includes the alarm totals for the Service Module card/ELAP IP links.

Figure 4-5. `repr-stat-alm` Command Report Example

```
> rept-stat-alm

Command Accepted - Processing

    eagle10605 99-06-24 23:59:39 EST EAGLE 35.0.0
    rept-stat-alm
    Command entered at terminal #10.
;

    eagle10605 99-06-24 23:59:39 EST EAGLE 35.0.0
    ALARM  TRANSFER= RMC
    ALARM  MODE      CRIT= AUDIBLE     MAJR= AUDIBLE     MINR= AUDIBLE
    ALARM  FRAME 1     CRIT=   9         MAJR=  12         MINR=   2
    ALARM  FRAME 2     CRIT=   0         MAJR=   0         MINR=   0
    ALARM  FRAME 3     CRIT=   0         MAJR=   0         MINR=   0
    ALARM  FRAME 4     CRIT=   0         MAJR=   0         MINR=   0
    ALARM  FRAME 5     CRIT=   0         MAJR=   0         MINR=   0
    ALARM  FRAME 6     CRIT=   0         MAJR=   0         MINR=   0
    ALARM  FRAME GPF   CRIT=   1         MAJR=   2         MINR=   1
    PERM. INH. ALARMS  CRIT=   0         MAJR=   0         MINR=   0
    TEMP. INH. ALARMS  CRIT=   0         MAJR=   0         MINR=   0
    ACTIVE ALARMS      CRIT=  10         MAJR=  14         MINR=   3
    TOTAL ALARMS       CRIT=  10         MAJR=  14         MINR=   3
    Command Completed.
;
```

Unsolicited Alarm Messages and Unsolicited Information Messages

The following sections describe MPS and ELAP Unsolicited Alarm Messages (UAMs) and Unsolicited Information Messages (UIMs), as well as those related to the LNP ELAP.

The EAGLE 5 ISS outputs two types of unsolicited messages:

- Unsolicited Alarm Messages (UAMs) - Denotes persistent problems with a device or object that needs the attention of a craftsperson.
- Unsolicited Informational Messages (UIMs) - Indicates transient events that have occurred.

Unsolicited Alarm Messages are generated by the maintenance system as trouble notification for the OS. The maintenance system is able to determine the status of the system through polling and periodic audits. Troubles are detected through analysis of system status and notifications from various subsystems in the EAGLE 5 ISS. The EAGLE 5 ISS controls and generates the alarm number, associated text, and formatting for alarms sent to EAGLE 5 ISS through the Maintenance Block mechanism for the LNP ELAP.

The *Maintenance Manual* describes all EAGLE 5 ISS UAMs and the appropriate recovery actions.

MPS Platform and ELAP Application Alarms

MPS platform and ELAP application alarms are reported in six categories of alarms. The categories are:

- **Critical Platform Alarm—**This is a 16-character hexadecimal string in which each bit represents a unique critical platform failure and alarm. An alarm in this category results in the associated MPS state being set to OOS-MT// Fault.

- **Major Platform Alarm—**This is a 16-character hexadecimal string in which each bit represents a unique major platform failure and alarm. An alarm in this category results in the associated MPS state being set to OOS-MT// Fault.

- **Minor Platform Alarm—**This is a 16-character hexadecimal string in which each bit represents a unique minor platform failure and alarm. An alarm in this category results in the associated MPS state being set to IS-ANR// Restricted.

- **Critical Application Alarm—**This is a 16-character hexadecimal string in which each bit represents a unique critical application failure/alarm. An alarm in this category results in the associated MPS state being set to OOS-MT//Fault.

- **Major Application Alarm—**This is a 16-character hexadecimal string in which each bit represents a unique major application failure/alarm. An alarm in this category results in the associated MPS state being set to OOS-MT// Fault.

- **Minor Application Alarm—**This is a 16-character hexadecimal string in which each bit represents a unique minor application failure and alarm. An alarm in this category results in the associated MPS state being set to IS-ANR/Restricted.

The alarm categories, shown in **Table 4-2** , are forwarded to the EAGLE 5 ISS when MPS and ELAP failures or errors are detected. Each alarm category is sent with a hexadecimal alarm data string that encodes all alarms detected in that category (see MPS and ELAP Status and Alarm Reporting). The clearing alarm for all of the MPS Platform and Application alarms is UAM 0250, MPS Available

NOTE: The recovery actions for the platform and application alarms are defined in *Tekelec 1100 ASMPS Platform Software and Maintenance Manual.*

Table 4-2. MPS Platform and ELAP Alarm Category UAMs

UAM #	Severity	Message Text
370	Critical	Critical Platform Failure(s)
371	Critical	Critical Application Failure(s)
372	Major	Major Platform Failure(s)
373	Major	Major Application Failure(s)
374	Minor	Minor Platform Failure(s)
375	Minor	Minor Application Failure(s)

Figure 4-6. Alarm Output Example

```
          1         2         3         4         5         6         7         8
12345678901234567890123456789012345678901234567890123456789012345678901234567890
    station1234 00-09-30 16:28:08 EST EAGLE 35.0.0-35.10.0
*C  0259.0370 *C MPS   B             Critical Platform Failure(s)
                ALARM DATA = h'0123456789ABCDEF
```

Figure 4-7. MPS Available Alarm

```
          1         2         3         4         5         6         7         8
 12345678901234567890123456789012345678901234567890123456789012345678901234567890
     station1234 00-09-30 16:28:08 EST EAGLE 35.0.0-35.10.0
     0259.0250    MPS   B              MPS Available
```

The clearing alarm is generated after existing alarms have been cleared. The clearing alarm sets the MPS primary status to IS-NR.

ELAP-to-Service Module Card Connection Status

The ELAP and the Service Module card are connected over one 100BASE-T Ethernet network that runs at 100 Mbps and one 10BASE-T Ethernet network that runs at 10 Mbps, and use TCP/IP. In the event connection is inoperative, the Service Module card is responsible for generating an appropriate UAM. Loss of connectivity or inability of the ELAP to communicate (from hardware or software failure, for example) is detected and reported within 30 seconds.

ELAP-Service Module Card UAMs

Maintenance Blocks sent from the ELAP have a field to identify error message requests. (See Maintenance Blocks). The Service Module card processes incoming Maintenance Blocks and generates the requested UAM. The Service Module card acts only as a delivery agent. The recovery actions for the ELAP-Service Module card UAMs are defined in "Corrective Maintenance" Chapter in the *Maintenance Manual*.

Service Module Card-ELAP Link Status Alarms

Two alarms indicate the Service Module card-to-MPS link status:

- 0084 “IP Connection Unavailable” (Major)
- 0085 “IP Connection Available” (Normal/Clearing)

  Example:

```
          1         2         3         4         5         6         7         8
 12345678901234567890123456789012345678901234567890123456789012345678901234567890
     station1234 00-09-30 16:28:08 EST EAGLE 35.0.0-35.10.0
 **  3582.0084 ** DSM B   1217          IP Connection Unavailable
```

RTDB Audit Alarms

During an audit of the Service Module cards and the ELAPs, the status of each real-time database (RTDB) is examined and the following alarms can be raised. The recovery actions for the RTDB Audit Alarms are defined in "Corrective Maintenance" Chapter in the *Maintenance Manual*.

1. When an RTDB has become corrupted, the following minor alarm is raised.

   Example:

```
          1         2         3         4         5         6         7         8
 12345678901234567890123456789012345678901234567890123456789012345678901234567890
```

```
    station1234 00-04-30 16:28:08 EST EAGLE 35.0.0-31.7.0
*   0012.0443 * CARD 1108 VSCCP        RTDB Database is corrupted
```

2. When a card's RTDB is inconsistent (its contents are not identical to the current RTDB on the Active ELAP fixed disks), the following minor alarm is raised.

   Example:

```
         1         2         3         4         5         6         7         8
12345678901234567890123456789012345678901234567890123456789012345678901234567890
    station1234 00-04-30 16:28:08 EST EAGLE 35.0.0-31.7.0
*   0012.0444 * CARD 1108 VSCCP        RTDB Database is inconsistent
```

3. When an inconsistent, incoherent, or corrupted RTDB has been fixed and the card or ELAP is in an IS-NR condition, the following alarm is raised.

   Example:

```
         1         2         3         4         5         6         7         8
12345678901234567890123456789012345678901234567890123456789012345678901234567890
    station1234 00-04-30 16:28:08 EST EAGLE 35.0.0-31.7.0
    0012.0445 CARD 1108 VSCCP          RTDB Database has been corrected
```

4. While the RTDB is being downloaded or an update has failed, it is in an incoherent state. The following minor alarm is raised.

   Example:

```
         1         2         3         4         5         6         7         8
12345678901234567890123456789012345678901234567890123456789012345678901234567890
    station1234 99-09-30 16:28:08 EST EAGLE 35.0.0-31.7.0
*   0012.0448 * CARD 1108 VSCCP        RTDB Database is incoherent
```

5. When a Service Module card detects that its RTDB needs to be resynchronized and has started the resync operation, the following major alarm is raised.

   Example:

```
         1         2         3         4         5         6         7         8
12345678901234567890123456789012345678901234567890123456789012345678901234567890
    station1234 99-09-30 16:28:08 EST EAGLE 35.0.0-31.7.0
**  0012.0449** CARD 1108 VSCCP        RTDB resynchronization in progress
```

6. After a Service Module card completes its RTDB resync operation, the following clearing alarm is raised.

   Example:

```
         1         2         3         4         5         6         7         8
12345678901234567890123456789012345678901234567890123456789012345678901234567890
    station1234 99-09-30 16:28:08 EST EAGLE 35.0.0-31.7.0
    0012.0450   CARD 1108 VSCCP        RTDB resynchronization complete
```

7. When a Service Module card detects that its RTDB needs to be reloaded because the resync log does not contain all of the required updates, the following major alarm is raised.

   Example:

```
         1         2         3         4         5         6         7         8
12345678901234567890123456789012345678901234567890123456789012345678901234567890
```

```
    station1234 99-09-30 16:28:08 EST EAGLE 35.0.0-31.7.0
**  0012.0451 ** CARD 1108 VSCCP         RTDB reload required
```

8. After a Service Module card completes its RTDB reload operation, the following clearing alarm is raised.

   Example:

```
        1         2         3         4         5         6         7         8
12345678901234567890123456789012345678901234567890123456789012345678901234567890
    station1234 99-09-30 16:28:08 EST EAGLE 35.0.0-31.7.0
    0012.0452    CARD 1108 VSCCP         RTDB reload complete
```

Feature Key Capacity UAMs

The following alarms are issued when the Service Module card detects the capacity has been exceeded. The recovery actions for the Feature Key Capacity Alarms are defined in "Corrective Maintenance" Chapter in the *Maintenance Manual*.

1. This UAM appears when the NPANXX totals on the Service Module cards has reached 90% of the total NPANXX capacity that is currently configured for the EAGLE 5 ISS.

   Example:

```
        1         2         3         4         5         6         7         8
12345678901234567890123456789012345678901234567890123456789012345678901234567890
    station1234 99-09-30 16:28:08 EST EAGLE 35.0.0-31.7.0
**  0012.0283 ** LNP SYSTEM              LNP Ported NPAs exceeds Feat. Capacity
```

2. The following example is a clearing message that appears when a previous fault with the number of LNP ported NPAs is greater than the capacity this feature supports has been corrected.

   Example:

```
        1         2         3         4         5         6         7         8
12345678901234567890123456789012345678901234567890123456789012345678901234567890
    station1234 99-09-30 16:28:08 EST EAGLE 35.0.0-31.7.0
    0012.0284    LNP SYSTEM              LNP Ported NPAs Capacity Normal
```

3. This UAM appears when the LRN totals on the Service Module cards has reached 90% of the total LRN capacity that is currently configured for the EAGLE 5 ISS.

   Example:

```
        1         2         3         4         5         6         7         8
12345678901234567890123456789012345678901234567890123456789012345678901234567890
    station1234 99-09-30 16:28:08 EST EAGLE 35.0.0-31.7.0
**  0012.0285 ** LNP SYSTEM              LNP Ported LRNs exceeds Feat. Capacity
```

4. The following example is a clearing message that appears when a previous fault with the number of LNP ported LRNs is greater than the capacity this feature supports has been corrected.

   Example:

```
        1         2         3         4         5         6         7         8
12345678901234567890123456789012345678901234567890123456789012345678901234567890
```

```
    station1234 99-09-30 16:28:08 EST EAGLE 35.0.0-31.7.0
    0012.0286    LNP SYSTEM              LNP Ported LRNs Capacity Normal
```

5. This critical UAM is output to warn that the total TN's in the LNP database has reached the configurable percentage (default value is 95%) of the allowed Feature Access Key (FAK) capacity currently configured for the EAGLE 5 ISS.

   Example:

```
         1         2         3         4         5         6         7         8
12345678901234567890123456789012345678901234567890123456789012345678901234567890
    station1234 99-09-30 16:28:08 EST EAGLE 35.0.0-31.7.0
*C  0056.0287 *C LNP SYSTEM              RTDB Table Level 2 FAK Cap exceeded
                 TABLE:  TN            Threshold Value:   95%
                                       Exceeds  91200000  of 96000000
```

6. This major UAM is output to warn that the total TNs in the LNP database has reached the configurable percentage (default value is 80%) of the allowed Feature key capacity currently configured for the EAGLE 5 ISS. The configured threshold value for UAM 0288 must be less than the configured threshold value for UAM 0287.

   Example:

```
         1         2         3         4         5         6         7         8
12345678901234567890123456789012345678901234567890123456789012345678901234567890
    station1234 99-09-30 16:28:08 EST EAGLE 35.0.0-31.7.0
**  0056.0288 ** LNP SYSTEM              RTDB Table Level 1 FAK Cap exceeded
                 TABLE:  TN            Threshold Value:   80%
                                       Exceeds  76800000  of 96000000
```

7. The following example is a clearing message that appears when a previous LNPFAK alarm condition no longer exists.

   Example:

```
         1         2         3         4         5         6         7         8
12345678901234567890123456789012345678901234567890123456789012345678901234567890
    station1234 99-09-30 16:28:08 EST EAGLE 35.0.0-31.7.0
    0058.0289    LNP SYSTEM              RTDB Table FAK Capacity Normal
```

Physical Memory Usage UAMs

The following alarms are issued when the Service Module card detects the RTDB memory capacity is not adequate for the ELAP feature. The recovery actions for the Physical Memory Usage Alarms are defined in "Corrective Maintenance" Chapter in the *Maintenance Manual*.

1. This critical UAM is displayed when the RTDB physical memory usage threshold exceeds 95% for the specified number of TNs, LRNs, or NPAs.

   Example:

```
1         2         3         4         5         6         7         8
12345678901234567890123456789012345678901234567890123456789012345678901234567890
    station1234 99-09-30 16:28:08 EST EAGLE 35.0.0-31.7.0
*C  0012.0442 *C CARD 1108 VSCCP         RTDB database capacity is 95% full
```

2. This major UAM is displayed when the RTDB physical memory usage threshold exceeds 80% for the specified number of TNs, LRNs, or NPAs.

   Example

```
         1         2         3         4         5         6         7         8
12345678901234567890123456789012345678901234567890123456789012345678901234567890
    station1234 99-09-30 16:28:08 EST EAGLE 35.0.0-31.7.0
**  0012.0446 ** CARD 1108 VSCCP         RTDB database capacity is 80% full
```

3. The following example is a clearing message that appears when a previous RTDB physical memory usage alarm condition no longer exists.

   Example:

```
         1         2         3         4         5         6         7         8
12345678901234567890123456789012345678901234567890123456789012345678901234567890
    station1234 99-09-30 16:28:08 EST EAGLE 35.0.0-31.7.0
    0012.0447    CARD 1108 VSCCP         RTDB database capacity alarm cleared
```

EAGLE Service Module Card Audit UIMs

The Service Module card performs data validation checks prior to applying updates and changes to the RTDB. This consist of comparing the checksum in the data about to be overwritten with the old checksum (new data element) in the update about to be applied.

A UIM is created when validation failure occurs because the target-cell checksums do not match the source-cell checksums. The updates are not applied and the database is marked incoherent.

Measurement Capacity UIMs

When the Measurements Platform is not installed, the OAM-based Measurements Subsystem will collect up to 100,000 LRNs and 150,000 NPANXXs from the SCCP cards. If the number of provisioned LRNs exceeds 100,000 or the number of provisioned NPANXXs exceeds 150,000, the Measurements Subsystem will generate a UIM at each hourly collection interval. The UIM is a warning that measurements data have been discarded. The UIM output may be suppressed by setting the UIM threshold limit to zero. More information on the Measurement Capacity UIMs are defined in "Corrective Maintenance" Chapter in the *Maintenance Manual*.

1. The following UIM is issued if the Measurements Platform is not enabled and the number of provisioned LRNs exceeds 100,000. This UIM is notification that the LNP LRN measurements report will be truncated, and additional LRN measurements will not be collected or reported.

   Example:

```
         1         2         3         4         5         6         7         8

12345678901234567890123456789012345678901234567890123456789012345678901234567890
    station1234 99-09-30 16:28:08 EST EAGLE 35.0.0-31.7.0
    0002.1310    CARD 1201     INFO      Sytem Meas. Limit exceeded for LRN
```

2. The following UIM is issued if the Measurements Platform is not enabled and the number of provisioned NPANXXs exceeds 150,000. This UIM is notification that the LNP NPANXXs measurements report will be truncated, and additional NPANXX measurements will not be collected or reported.

   Example:

```
         1         2         3         4         5         6         7         8
```

```
1234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890
    station1234 99-09-30 16:28:08 EST EAGLE 35.0.0-31.7.0
    0002.1311    CARD 1201     INFO      Sytem Meas. Limit exceeded for NPANXX
```

5

ELAP Software Configuration

Overview of the ELAP User Interfaces

The EAGLE LNP Application Processor (ELAP) User Interface provides two user interfaces:

- The Graphical User Interface provides GUI menus that maintain, debug, and operate the platform; it and its associated error messages are described in ELAP Graphical User Interface .

- The text-based User Interface has a Configuration menu that performs the ELAP configuration and initialization; it is described in this chapter.

The GUI provides the user with menus and screens to perform routine operations. The text-based user interface provides the ELAP Configuration menu to perform the initial configuration.

To communicate with the ELAP graphical user interface, you use a PC with a network connection and a network browser. For information about using the ELAP GUI, see ELAP Graphical User Interface .

To configure ELAP, you use the ELAP text-based user interface. For information about configuring the ELAP and how to set up its PC workstation, continue with this chapter.

Setting Up an ELAP Workstation

The customer workstation serving as a client PC (shown in Figure 3-1) must meet certain criteria, which are described next.

Screen Resolution

For optimum usability, the workstation must have a minimum resolution of 800x600 pixels and a minimum color depth of 16 thousand colors per pixel.

Compatible Browsers

The ELAP user interface was designed and written to perform with Microsoft Internet Explorer 5.0 or later. The ELAP user interface is also compatible with Mozilla Firefox 1.0.2 or later. Do not use other browsers with the ELAP user interface. When using Firefox, you will encounter the following message when logging into the ELAP GUI:

Java

The ELAP GUI uses a Java banner applet to display real-time updates and status for both A and B sides of the MPS.

The Java installation must be performed in the sequence shown:

1. Install Java Plug-In
2. Install Java Policy File
3. Add Security Parameters to an Existing Java Policy File or Create a New Java Policy File

Install Java Plug-In

Because the Java applet is required for the ELAP GUI to operate, perform the following procedure to install the Java plug-in after you complete the ELAP configuration.

NOTE: The selected browser must be the only browser open on your PC when you modify or create the Java policy file, or else the change will not take effect.

1. Using the selected browser (Internet Explorer 5.0 or later or Mozilla Firefox 1.0.2 or later), enter the IP address for your ELAP A machine. You will see the login screen.

2. Attempt to log in to the ELAP User Interface screen. If using Firefox, you will encounter the following message when logging into the ELAP GUI:

   ```
   The User Interface may not function correctly with the browser you are using. Microsoft Internet
   Explorer, version 5 and later, has been certified for this application
   ```

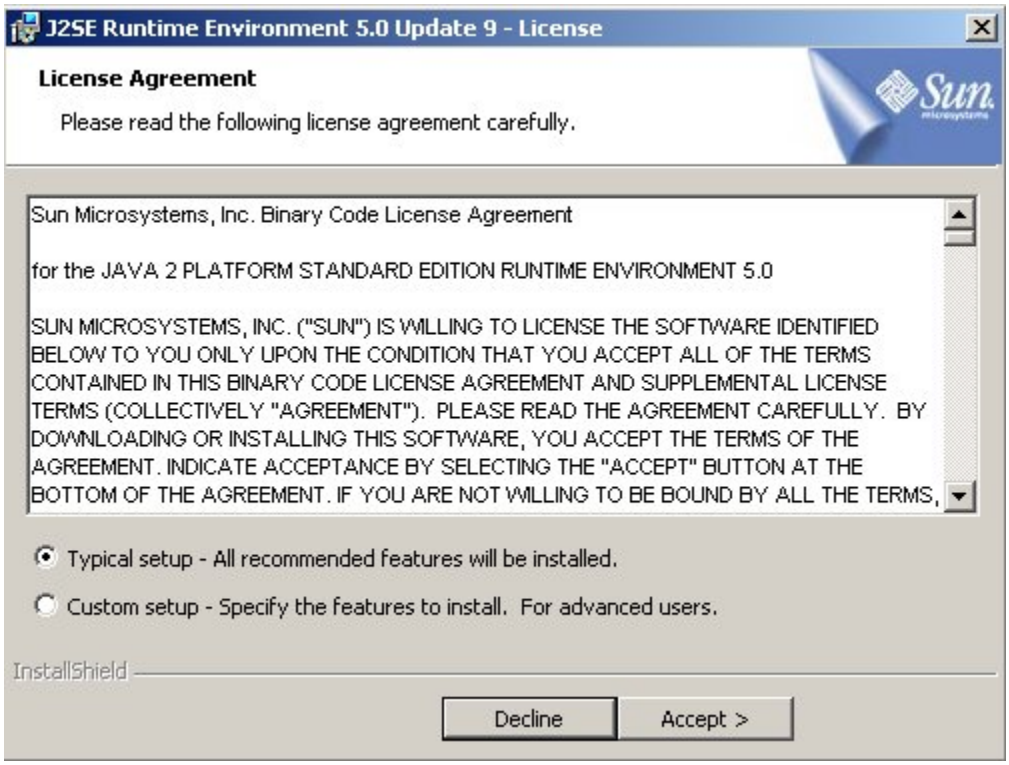
   When you have successfully entered the Username and Password, the login process checks for the required Java plug-in. When it finds the Java 1.5 plug-in not present (but you had a previous version of Java installed), the system displays a Security Warning window as shown in **Figure 5-1** .

Figure 5-1. Security Warning Window

3. Click the **Install** button to begin the process of loading the Java plug-in.

4. Next, the Java installation presents a License Agreement screen as shown in **Figure 5-2** .

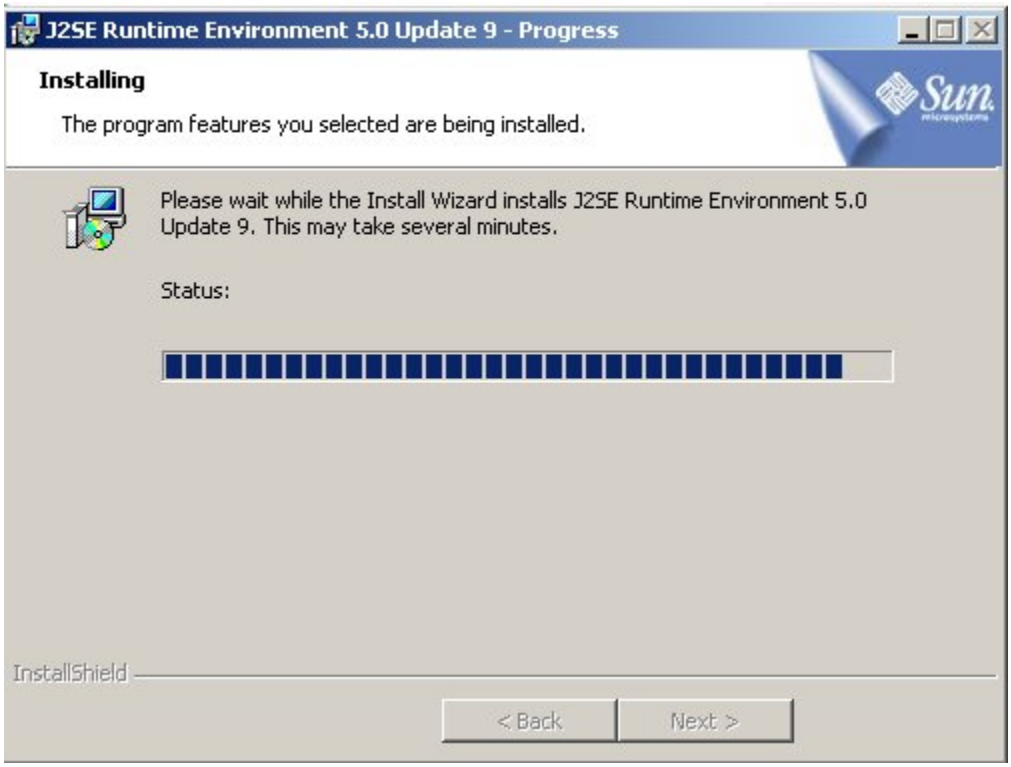
Figure 5-2. License Agreement



5. Ensure that the **Typical Setup** radio button is selected, and click the **Accept** button to accept the Sun Microsystems agreement.

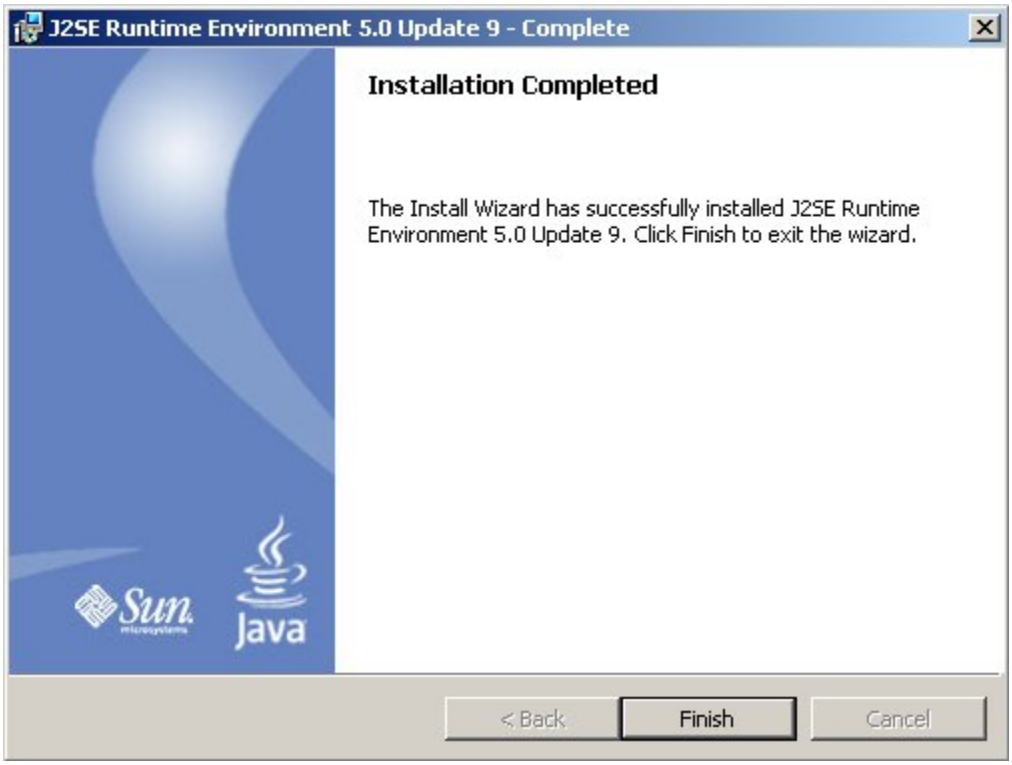
6. The installation process starts, and a progress window appears as shown in **Figure 5-3** .

Figure 5-3. Java Installation Progress Window



7. When the installation is complete, the Installation Complete window appears as shown in **Figure 5-4** .

Figure 5-4. Java Installation Complete Window



8. The installation is complete. Click the **Finish** button. You return to the browser screen containing the ELAP login screen.

Install Java Policy File

The banner applet makes a network connection to each MPS side. A Java policy file must exist for the banner applet to connect properly. If the Java policy file is not present, you will receive a Violation status (VIOL) for the machine.

NOTE: The selected browser must be the only browser open on your PC when you modify or create the Java policy file, or else the change does not take effect.

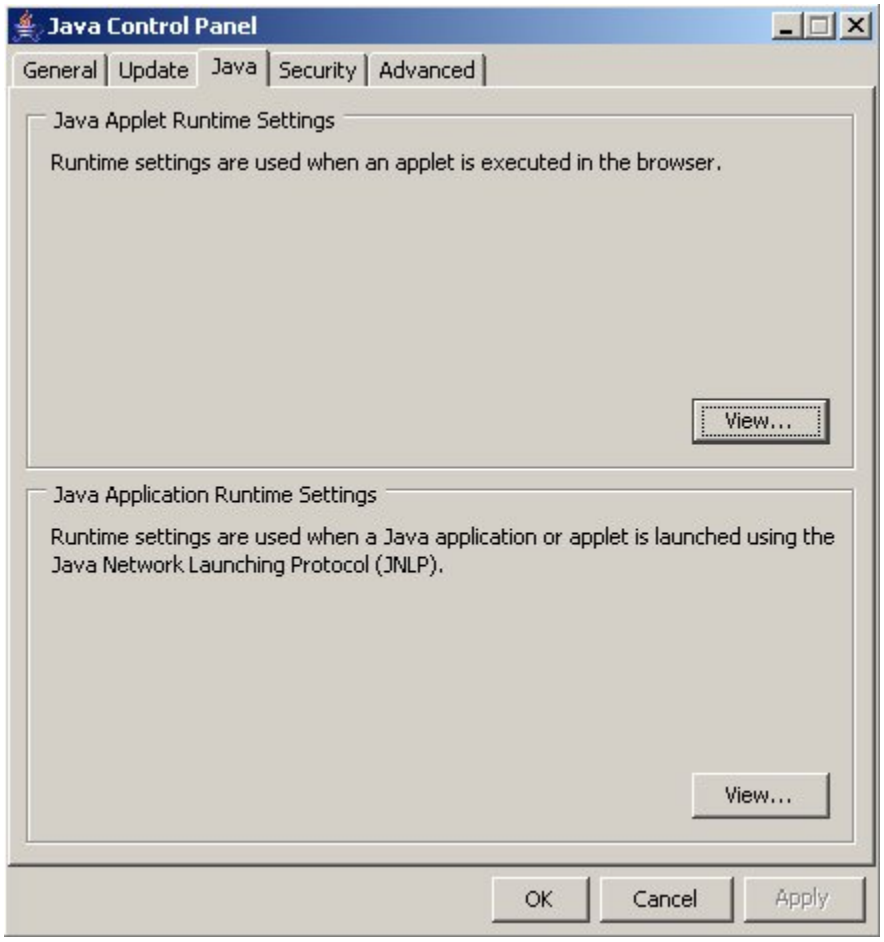
Add Security Parameters to an Existing Java Policy File

To check to see if a Java policy file is already in place, perform the following actions:

1. From the Windows **Start** menu, select **Control Panel**.

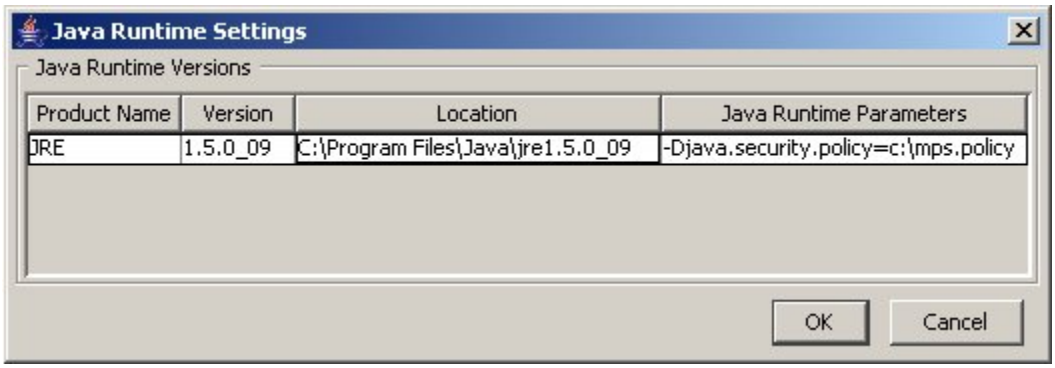
2. Select the **Java Control Panel**. When the **Java Control Panel** appears, click the **Java** tab as shown in **Figure 5-5** .

Figure 5-5. Java Control Panel, Java Tab



3. Click **View** in the **Java Applet Runtime Settings** pane. The Java Runtime Settings dialog box appears as shown in **Figure 5-6** .

Figure 5-6. Java Runtime Settings Dialog Box



4. Adjust the width of the columns until you can read the contents of the Java Runtime Parameters column (at the far right).

5. Open the policy file indicated in the Java Runtime Parameters column, and insert the following text.

```
grant {
{permission java.net.SocketPermission "*:8473", "connect";
};
```

Create a New Java Policy File

To create a Java policy file:

1. Insert the following text into a file accessible by the workstation:

```
grant {
  permission java.net.SocketPermission "*:8473", "connect";
};
```

2. Follow steps 2 through 4 in the procedure described in Add Security Parameters to an Existing Java Policy File .

3. In the Java Runtime Parameters column for Java version 1.5, type the path to the file you created in step 1 of this procedure. An example path is shown below.

```
-Djava.security.policy={full_path_to_file}
```

ELAP Configuration and Initialization

Before you can use the ELAPGUI, you must initialize and configure the ELAP software. The ELAP configuration and initialization is performed through the ELAP text-based user interface.

You will connect a local (optional) terminal connected to port 0 of the 8 -port connector box on the MPS frame at each EAGLE 5 ISS. (Refer to the *Installation Manual - EAGLE 5 ISS*.) To begin the initialization, you will log into ELAP A thefirst time as the "**elapconfig**" user. An automatic configuration is performed on both mated ELAPs.

> **NOTE: All network connections and the mate ELAP must be present and verified to allow the initial configuration to complete successfully.**

No other user is able to log in to an ELAP until the configuration step is completed for that system.

Errors and Other Messages

The following rules are applicable to configuring the ELAP:

- Mate MPS servers (MPS A and MPS B) must be powered on.
- "Initial Platform Manufacture" for the mate MPS servers must be complete.
- The Sync Network between the mate MPS servers must be operational.
- You must have the correct password for the **elapdev** user on the mate MPS server.

Required Network Address Information

The following information is needed to configure the MPSs at EAGLE 5 ISS A (**Table 5-1** and EAGLE 5 ISS B **Table 5-2**). Fill in the following tables for reference during the installation procedure.

Table 5-1. Information for MPS at EAGLE 5 ISS A

Common Information	
MPS A Provisioning Network Address	. . .
MPS B Provisioning Network Address	. . .
Netmask	. . .
Default Router	. . .
Provisioning VIP Address	
Port Forwarding and Static NAT Information (optional)	
MPS A Forwarded HTTP Port	
MPS B Forwarded HTTP Port	
MPS A Forwarded SuExec Port	
MPS B Forwarded SuExec Port	
MPS A Forwarded LSMS Port	**7483***
MPS A Forwarded LSMS Port	**7483***
MPS A Forwarded Banner Port	
MPS B Forwarded Banner Port	
MPS A Forwarded EBDA Port	**1030***
MPS B Forwarded EBDA Port	**1030***
MPS A Provisioning Static NAT Addr.	. . .
MPS B Provisioning Static NAT Addr.	. . .
* Do not change the default values for these ports	

..

Table 5-2. Information for MPS at EAGLE 5 ISS B

Common Information	
MPS A Provisioning Network Address	. . .
MPS B Provisioning Network Address	. . .
Netmask	. . .
Default Router	. . .

Common Information	
Port Forwarding and Static NAT Information (optional)	
MPS A Forwarded HTTP Port	
MPS B Forwarded HTTP Port	
MPS A Forwarded SuExec Port	
MPS B Forwarded SuExec Port	
MPS A Forwarded LSMS Port	**7483***
MPS A Forwarded LSMS Port	**7483***
MPS A Forwarded Banner Port	
MPS B Forwarded Banner Port	
MPS A Forwarded EBDA Port	**1030***
MPS B Forwarded EBDA Port	**1030***
MPS A Provisioning Static NAT Addr.	. . .
MPS B Provisioning Static NAT Addr.	. . .
* Do not change the default values for these ports	

Configuration Menu Conventions

After you have logged into the ELAP user interface with the **`elapconfig`** user name, the menu appears that corresponds to that user login name. Before going into the details about the Configuration Menu, you need to know a few things about the Menu Format, Prompts and Default Values, and Error Message Format, which are covered next.

Menu Format

The configuration menu has a header format displaying specific information. On the first line, it indicates the MPS Side A or B, with which you are active. On the same line, you are shown the **`hostname`** and **`hostid`**. The second and third lines show the **`Platform Version`**, followed by the **`Software Version`**. The last line displays the date and time. See a sample configuration headier format in **Figure 5-7** .

Figure 5-7. Configuration Menu Header Format

```
MPS Side A:  hostname: mps-t1100-a  hostid: fd0a4767
             Platform Version: 2.0.2-4.0.0_50.26.0
             Software Version: ELAP 1.0.1-4.0.0_50.37.0
             Mon Sep 26 10:57:57 EDT 2005
```

When you are shown a menu, you choose a menu item by entering the number of the item (or “e” for Exit) in response to the **`Enter Choice`** prompt that follows the menu, and press Return.

When you choose a menu item, the user interface performs the requested operation. The operation and any associated output for each menu item are described in detail later in this section.

If you enter an invalid choice (such as a letter or a number that is not available for that menu), an error appears. Perform the corrective action described for that error.

Prompts and Default Values

Depending on the menu item that you choose, you might be prompted for data (such as IP addresses) that is required to complete the selected operation. Optional fields are indicated by the text "(optional)" at the end of the prompt. To bypass an optional field without entering a value, press Return.

Default values are indicated by a value enclosed in square brackets at the end of the prompt text: [*default value*]. Example default values are shown in this chapter; they might not be the same as the default values that appear for your system. To accept the default value for a prompt instead of entering a response, press Return.

You can press the Escape key to exit any operation without entering a value for the prompt. The operation is aborted, and you are returned to the menu.

Error Message Format

Invalid menu selections, invalid user input, and failed user interface operations generate error messages on the screen. The error message remains on the screen until you press Return.

All error messages have a unique four-digit error number and associated text. The numbers and text for all error messages generated by the ELAP user interface are listed in the *ELAP Administration Manual* LINK . The possible error messages that can occur for each ELAP user interface menu item are listed in the description of the menu item in this chapter.

Error messages have the following format, where ***XXXX*** is the unique four-digit error number for the error and ***Error text*** is the corresponding error text:

```
E
 XXXX

:
 Error text

Press return to continue
```

Whenever the software must be stopped to perform an operation, you are prompted to stop the software:

```
ELAP software is running.  Stop it? [N]: Y
```

However, you must remember that while the ELAP software is stopped, no provisioning updates can be processed by the ELAP.

Overview of ELAP Configuration

When you log into an ELAP with user name "elapconfig" after the first initialization of the ELAP, the configuration process begins. (See the details in LINK .) The configuration process lets you change IP addresses, time zone, and the password for "elapconfig". You can display the host ID and exchange secure shell keys. This section describes each of these items in configuration menu. log into an

Initial “elapconfig” User Login

The first time the **elapconfig** user logs in to the system, the text screen is displayed as shown in Figure 5-8 .

Figure 5-8. Initial Configuration Text Screen

```
Caution: This is the first login of the text user interface.  Please
         review the following checklist before continuing.  Failure
         to enter complete and accurate information at this time will
         have unpredictable results.

             1. The mate MPS servers (MPS A and MPS B) must be powered on.
             2. "Initial Platform Manufacture" for the mate MPS servers
                must be complete.
             3. The sync network between the mate MPS servers must be
                operational.
             4. You must have the correct password for the ELAPdev user on
                the mate MPS server.

Press return to continue...
```

If all four criteria above are not met, the configuration cannot proceed. Ensuring that the MPS servers are powered on requires a visual check. If the “Initial Platform Manufacture” is not complete, the configuration cannot proceed; furthermore, if the sync network is not operational, the user is notified.

When the four criteria are met, press Return and the process resumes. Figure 5-9 shows the continuation of the screen information. The installer enters **y** if the installation is to continue.

Figure 5-9. Initial Configuration Continues

```
Are you sure you wish to continue? [N]: y
```

> **NOTE: Review the information required for the following section in “ Required Network Address Information ”. Make certain all required information is obtained and recorded in the tables provided.**

Next, the installer is prompted for the **elapdev** user password on the mate MPS server. Figure 5-10 shows sample output that is generated after the correct password is entered.

Figure 5-10. Entering the elapdev Password

```
Password for ELAPdev@mate:

Keys exchanged.
Verifying that ssh works correctly.
ssh is working correctly.
Building the initial database on slave.
Building the initial database on master.
There was no elap.cfg file.  Using default configuration.
Allowing access from slave.
Stopping mysql on master.
Stopping mysql on slave.
Setting up master config file.
Setting up slave config file.
Copying database to slave.
Starting MySQL on master.
Starting MySQL on slave.
```

At this point, the first appearance of the Configuration Menu occurs, and is discussed next.

Text-based Configuration Menu

Following the report appearing in **Figure 5-10** , the ELAP Configuration Menu is displayed as shown in **Figure 5-11** . The **`elapconfig`** user can now begin configuring the MPS local and remote servers.

Figure 5-11. ELAP Configuration Menu

```
MPS Side A:  hostname: mps-t1100-a  hostid: 0
             Platform Version: 3.0.2-8.0.0_80.4.0
             Software Version: ELAP 3.0.2-8.0.0_80.4.0
             Wed Apr 16 13:32:15 EDT 2008

 /-----ELAP Configuration Menu----------\
/----------------------------------------\
|  1 | Display Configuration             |
|----|-----------------------------------|
|  2 | Configure Network Interfaces Menu |
|----|-----------------------------------|
|  3 | Set Time Zone                     |
|----|-----------------------------------|
|  4 | Exchange Secure Shell Keys        |
|----|-----------------------------------|
|  5 | Change Password                   |
|----|-----------------------------------|
|  6 | Platform Menu                     |
|----|-----------------------------------|
|  7 | Configure NTP Server              |
|----|-----------------------------------|
|  8 | Mate Disaster Recovery            |
|----|-----------------------------------|
|  e | Exit                              |
\----------------------------------------/

Enter Choice: 2
```

```
MPS Side A:  hostname: mps-t1100-a  hostid: fd0a4767
             Platform Version: 2.0.2-4.0.0_50.26.0
             Software Version: ELAP 1.0.1-4.0.0_50.37.0
             Mon Sep 26 10:57:57 EDT 2005

 /-----ELAP Configuration Menu----------\
/----------------------------------------\
|  1 | Display Configuration             |
|----|-----------------------------------|
|  2 | Configure Network Interfaces Menu |
|----|-----------------------------------|
|  3 | Set Time Zone                     |
|----|-----------------------------------|
|  4 | Exchange Secure Shell Keys        |
|----|-----------------------------------|
|  5 | Change Password                   |
|----|-----------------------------------|
|  6 | Platform Menu                     |
|----|-----------------------------------|
|  7 | Configure NTP Server              |
|----|-----------------------------------|
|  e | Exit                              |
\----------------------------------------/

Enter Choice:
```

To choose a menu item, enter the number or letter of the menu item in response to the **Enter Choice** prompt that follows the menu item list, and press Return.

Display Configuration

The Display Configuration menu option 1 displays network address information and the time zone. See an example in **Figure 5-12** .

Figure 5-12. Example of Display Configuration Output

```
MPS Side A:  hostname: mps-t1100-a  hostid: 0
             Platform Version: 3.0.2-8.0.0_80.4.0
             Software Version: ELAP 3.0.2-8.0.0_80.4.0
             Wed Apr 16 13:40:38 EDT 2008

ELAP A Provisioning Network IP Address = 192.168.61.136
ELAP B Provisioning Network IP Address = 192.168.61.137
Provisioning Network Netmask           = 255.255.255.0
Provisioning Network Default Router    = 192.168.61.250
Provisioning VIP                       = 192.168.61.166
ELAP A Sync Network Address            = 169.254.1.100
ELAP B Sync Network Address            = 169.254.1.200
ELAP A Main DSM Network Address        = 192.168.120.100
ELAP B Main DSM Network Address        = 192.168.120.200
ELAP A Backup DSM Network Address      = 192.168.121.100
ELAP B Backup DSM Network Address      = 192.168.121.200
ELAP A HTTP Port                       = 80
ELAP B HTTP Port                       = 80
ELAP A HTTP SuExec Port                = 8001
ELAP B HTTP SuExec Port                = 8001
ELAP A Banner Connection Port          = 8473
ELAP B Banner Connection Port          = 8473
ELAP A Static NAT Address              = Not configured
ELAP B Static NAT Address              = Not configured
ELAP A LSMS Connection Port            = Not configured
ELAP B LSMS Connection Port            = Not configured
ELAP A EBDA Connection Port            = Not configured
```

```
ELAP B EBDA Connection Port            = Not configured
Time Zone                              = America/New_York

Press return to continue...
```

Addresses that you choose should not conflict with your internal network addresses. The class C networks you choose should not conflict with the class C network used in your network scheme. Table 5-3 shows an example of IP addresses used in the configuration process.

Table 5-3. Sample IP Addresses Used in Configuration

Provisioning Network Information	MPS A (Local) IP Addresses	MPS B (Local) IP Addresses
ELAP A Provisioning Network IP Address (MPS A)	192.168.61.90	192.168.61.119
ELAP B Provisioning Network IP Address (MPS B)	192.168.61.91	192.168.61.120
Network Net Mask	255.255.255.0	255.255.255.0
Default Router	192.168.61.250	192.168.61.250
Provisioning VIP Address	192.168.61.166	192.168.61.166

Configure Provisioning Network

The Configure Network Interfaces Menu option **2** of the Configuration Menu displays the submenu shown in Figure 5-13 . It supports the configuration of all the network interfaces for the ELAP.

Figure 5-13. Configure Network Interfaces Menu

```
/-----Configure Network Interfaces Menu----\
/-------------------------------------------\
|   1 | Configure Provisioning Network       |
|-----|--------------------------------------|
|   2 | Configure Sync Network               |
|-----|--------------------------------------|
|   3 | Configure DSM Network                |
|-----|--------------------------------------|
|   4 | Configure Backup Provisioning Network |
|-----|--------------------------------------|
|   5 | Configure Forwarded Ports            |
|-----|--------------------------------------|
|   6 | Configure Static NAT Addresses       |
|-----|--------------------------------------|
|   e | Exit                                 |
\-------------------------------------------/

Enter choice:
```

Configure Provisioning Network

The Configure Provisioning Network option **1** of the Configure Network Interfaces Menu configures the ELAP provisioning network. These include the provisioning network's IP address, netmask, and IP address. This information allows the ELAP to communicate with an existing customer network.
default router

In response to each prompt, you can enter a dotted decimal IP address or press Return to leave the current value unchanged (the current value is shown in brackets after the prompt text). See **Figure 5-14** for the option **1** output.

Figure 5-14. Configure Provisioning Network Output

```
Verifying connectivity with mate ...
Enter the ELAP A provisioning network IP Address [192.168.61.90]:
Enter the ELAP B provisioning network IP Address [192.168.61.91]:
Enter the ELAP provisioning network netmask [255.255.255.0]:
Enter the ELAP provisioning network default router IP Address: 192.168.54.250

Press return to continue ...
```

Configure Sync Network

The Configure Sync Network option **2** of the Configure Network Interfaces Menu allows you specify the Sync network IP address of the selected ELAP. Sync network IP addresses are configured to default values during ELAP initialization. The third octet of the address can be changed after ELAP initialization is complete.

See **Figure 5-15** for the option **2** output.

Figure 5-15. Configure Sync Network

```
Verifying connectivity with mate...
Enter the first 3 octets for the ELAP MPS sync Network [192.168.4]:
```

Configure DSM Network

The Configure DSM Network option **3** of the Configure Network Interfaces Menu prompts you for the ELAP DSM network IP addresses. This information allows the ELAP to communicate with the main and backup DSM networks.

In response to each prompt, you can enter a dotted decimal IP address or press Return to leave the current value unchanged (the current value is shown in brackets after the prompt text).

See **Figure 5-16** for the option **3** output.

Figure 5-16. Configure DSM Network

```
Verifying connectivity with mate ...
Enter the first 3 octets for the ELAP main DSM network [192.168.128]:
Enter the first 3 octets for the ELAP backup DSM network [192.168.129]:
```

Configure Forwarded Ports

The Configure Forwarded Ports option **5** of the Configure Network Interfaces Menu provides the functionality to configure ELAP ports for the Web UI.

Each numbered item of the Configure Forwarded Ports menu allows the user to specify a port number used for remote access to the MPS.

This information should be received from the customer for the MPS and recorded in **Table 5-2** and **Table 5-1** .

Configure Static NAT Addresses

The Configure Static NAT Addresses option 6 from the Configure Network Interfaces Menu provides the functionality to configure the static NAT addresses of the ELAP.

Each numbered item of the Configure Static NAT Addresses menu allows the user to specify an IP Address used outside of the firewall for remote access to the MPS. The following **Figure 5-17** shows an example of a resulting prompt.

Figure 5-17. Configuring NAT Addresses Prompt

```
ELAP A Static NAT Address:
```

Select Time Zone

NOTE: Do not perform the Select the Time Zone function on a running system. Contact Tekelec Technical Services for assistance.

The Select Time Zone option **3** prompts you for the time zone to be used by the ELAP. The time zone can be the zone where the ELAP is located, Greenwich Mean Time, or another zone that is selected by the customer to meet the needs of the system.

NOTE: The value for the time zone should be obtained from the customer's Information Services department. The default value for the time zone is "US/Eastern".

To select a file in one of the subdirectories, enter a relative path name (such as "US/Eastern") in response to the prompt. See Select Time Zone Menu for the option **3** output.

Figure 5-18. Select Time Zone Menu

```
Press return to continue...
Verifying connectivity with mate...
Are you sure you wish to change the timezone for MPS A and B? [N]: y
Enter a time zone:
```

You must enter a valid UNIX time zone file name. Alternatively, to display a complete list of the valid time zones, simply press Return in response to the prompt, and all valid time zone names are displayed. See the *ELAP Administration Manual - 8.0* Time Zone File Names for the list that appears when you press the Return key or enter invalid time zone file name.

The time zone change does not take effect until the next time the MPS is rebooted. The Reboot MPS screen is described in the *ELAP Administration Manual - 8.0* Reboot the MPS .

Exchange Secure Shell Keys

The Exchange Secure Shell Keys option **4** from the ELAP Configuration Menu, enables connections between local and remote ELAPs. The ELAPs exchange encryption keys, which are required to run the secure shell.

The exchange normally occurs automatically during ELAP initialization. Use this menu item only if the exchange must be performed manually.

The **elapconfig** user must know the password for the **ELAPdev@mate**.

The exchange normally occurs automatically during ELAP initialization. Use this menu item only if the exchange must be performed manually.

See **Figure 5-19** for the option **4** output.

Figure 5-19. Exchange Secure Shell Keys Output

```
Are you sure you wish to exchange keys? [N]: y
```

Change Password

The Change Password option **5** from the ELAP Configuration Menu, changes the text-based user interface password for the **elapconfig** login name for both MPS A and B.

See **Figure 5-20** for the option **5** output.

Figure 5-20. Change Password

```
Verifying connectivity with mate...
Are you sure you wish to change the text UI password on MPS A and B? [N]: y
Enter new password for text UI user:
Re-enter new password:

Press return to continue...
```

Platform Menu and Options

The ELAP Platform Menu option **6**, from the ELAP Configuration Menu, accesses the Platform menu so that the **elapconfig** user can access and manage platform functions shown next. See **Figure 5-21** for the option 8 output.

Figure 5-21. Platform Menu Output

```
MPS Side A:  hostname: mps-t1100-a  hostid: fd0a4767
             Platform Version: 2.0.2-4.0.0_50.26.0
             Software Version: ELAP 1.0.1-4.0.0_50.37.0
             Mon Sep 26 10:57:57 EDT 2005

/-----ELAP Platform Menu-\
/-------------------------\
|  1 | Initiate Upgrade    |
|----|---------------------|
|  2 | Eject CD            |
|----|---------------------|
|  3 | Reboot MPS          |
|----|---------------------|
|  4 | Halt MPS            |
|----|---------------------|
|  5 | MySQL Backup        |
|----|---------------------|
|  6 | RTDB Backup         |
|----|---------------------|
|  e | Exit                |
\-------------------------/

Enter choice:
```

Initiate Upgrade

The Initiate Upgrade menu option 1 initiates an upgrade on the selected ELAP. For upgrade procedures, contact Customer Care Center .

Eject CD

The Eject CD menu option 2 initiates an ejection of the CD media on the selected ELAP. The default, as shown next, is 'BOTH'.

```
Eject CD tray of MPS A, MPS B or BOTH? [BOTH]:
```

Reboot MPS

The Reboot MPS menu option 3 initiates a reboot of either MPS or both. The default, as shown below, is BOTH.

NOTE: The `elapconfig` user can abort rebooting the MPS by pressing the Escape key at the displayed prompt.

```
Reboot MPS A, MPS B or [BOTH]:
```

CAUTION: Rebooting the MPS stops all ELAP processes. Databases cannot be updated until MPS is fully booted.

Halt MPS

The Halt MPS menu option 4 initiates a halt of one MPS or both. The default, as shown below, is BOTH.

CAUTION: Halting an MPS stops all ELAP processes. Selecting the default (halt both MPS A and MPS B) requires a person to be physically present in order to reboot MPS and allow for further access!

NOTE: The `elapconfig` user can abort the MPS Halt by pressing the Escape key at the displayed prompt.

MySQL Backup

The MySQL Backup menu option 5 backs up the MySQL database. The output is shown below.

NOTE: ELAP software must be stopped or MySQL backup will abort and return to the ELAP Platform Menu.

```
Are you sure you want to back up the MySQL database on MPS A? [N]: y
Connecting to local MySQL server...
Getting read lock...
Tarring the NPDB...
Disconnecting from local MySQL server...
```

RTDB Backup

The RTDB Backup menu option 6 backs up the RTDB database. The output is shown below.

NOTE: ELAP software must be stopped or RTDB backup will abort and return to the ELAP Platform Menu.

```
Are you sure you want to back up the RTDB database on MPS A to
"/var/TKLC/appl/free/rtdbBackup_mps-t1100-a_20050926110224.tar"? [N]: y
```

ELAP Platform Menu Exit

The Exit menu option e exits from the ELAP Platform Menu and returns to the ELAP Configuration Menu.

Configure NTP Server and Options

The Configure NTP Server option 7 allows for the display, addition, and removal of an external NTP server. See **Figure 5-22** for the option 7 output.

Figure 5-22. Configure NTP Server Output

```
 /----ELAP Configure NTP Server Menu-\
/-------------------------------------\
|  1 | Display External NTP Server     |
|----|---------------------------------|
|  2 | Add External NTP Server         |
|----|---------------------------------|
|  3 | Remove External NTP Server      |
|----|---------------------------------|
|  e | Exit                            |
\-------------------------------------/

Enter Choice:
```

Display External NTP Server

The Display External NTP Server menu option 1 displays External NTP Server information. If a server is present, the server name and IP address are displayed. If an NTP Server is not present, the following is displayed.

```
There are no External NTP Servers. Press return to continue...
```

Add External NTP Server

The Add External NTP Server menu option 2 adds an External NTP Server. The output below is an example of the addition of an External NTP Server.

NOTE: The IP address must be a valid address for an External NTP Server.

```
Are you sure you wish to add new NTP Server? [N]: yEnter the ELAP NTP Server IP Address:
192.168.61.69Verifying NTP Server. It might take up to 1 minute. External NTP Server [server
192.168.61.69 prefer] has been added. Press return to continue...Verifying NTP Server. It might take
up to 1 minute. External NTP Server [server 192.102.61.91  prefer] has been added.
```

Remove External NTP Server

The Remove External NTP Server menu option 3 removes an External NTP Server. If a server is present, selecting the Remove External NTP Server removes the server. If an NTP Server is not present, the following appears.

```
There are no External NTP Servers. Press return to continue...
```

ELAP Configure NTP Server Menu Exit

The ELAP Configure NTP Server Menu Exit menu option e exits the ELAP Configure NTP Server Menu, and returns to the ELAP Configuration Menu.

Exit

The Exit menu option e exits the ELAP Configuration menu.

ELAP Configuration Procedure

Initialization and configuration are provided through a text-based user interface (UI) described in this chapter. The user accesses the text-based configuration procedure by means of the product UI.

The first time user **elapconfig** logs into MPS A, the system performs an auto-configuration on both MPS ELAP pairs. The sync network and main and backup DSM networks are initialized to their default values, described in the *ELAP Administration Manual - 8.0* Network Connections and defined in the *Installation Manual - EAGLE 5 ISS*. Various internal configuration parameters are also set to their default values. The installer must perform initial configuration on MPS A on EAGLE 5 ISS A and MPS A on EAGLE 5 ISS B.

Configuration Terms and Assumptions

- The initial configuration steps assume that each MPS has previously undergone successful Initial Platform Manufacture (IPM).
- The network paths must be present and verified before the MPS servers are ready for ELAP configuration.
- Initial configuration can be implemented on only the MPS A side of EAGLE 5 ISS A and MPS A side of EAGLE 5 ISS B. Attempting to perform initial configuration on MPS B of EAGLE 5 ISS A is not allowed, and the **elapconfig** user will be notified. The attempted configuration will be aborted with no impact on either MPS A or B.

  After the initial configuration of MPS A on EAGLE 5 ISS A and MPS A on EAGLE 5 ISS B, both ELAPs should be operational unless the system failed to successfully initialize during reboot or the configured values for the Sync and/or DSM networks conflict with other equipment in the network. Tekelec recommends that you do not change the default network values.
- The provisioning values displayed for the following initialization and configuration steps are example values only.
- Default values can be accepted just by pressing the Return key at the prompt; default values are shown enclosed in brackets [ ].
- It is the customer's decision about the timing and frequency of performing a back-up of his databases. Of course, databases should be backed up when they are initially populated with data; however, the priority that the customer assigns to data and time lost in restoring it will dictate the frequency of database back-up.
- Adding an NTP server is optional. Additionally, only one NTP server is needed to provide time synchronization for all the MPS servers on both EAGLE 5 ISS pairs.
- The ELAP terms ' local' and ' remote' are relative with respect to the ELAP configuration software. In other words, if the installer is running the configuration software on the physical MPS (that is, the MPS that the installer is physically on-site and has his terminal connected to), the configuration software refers to that MPS as 'local'. However if the installer connects through the network into the MPS A on EAGLE 5 ISS B, the configuration software executing at EAGLE 5 ISS B sees itself as 'local', referring to MPS that the installer is physically connected to as the 'remote'.

  Remember that the 'local' MPS is whichever MPS A that the configuration software is being executed on, regardless of where the user is physically located.

  The MPS of EAGLE 5 ISS A is the first MPS to which the installer physically connects and on which initial configuration of the ELAPs is always begun.

To avoid confusion of these relative terms, the MPS A on EAGLE 5 ISS A is considered to be the on-site MPS to which the installer has the physical connection. This document refers to the MPS to which the installer does not have the physical connection as MPS A on EAGLE 5 ISS B.

Configuration Symbols

During the Configuration Procedure, the installer will initialize and configure the MPSs to perform various functions. Special instructions are required occasionally for an MPS on EAGLE 5 ISS A, an MPS on EAGLE 5 ISS B. To assist the installer, this manual uses these symbols to indicate individual instructions to be performed for those specific MPSs.

Table 5-4. MPS Configuration Symbols

MPS Symbol	Symbol Description
	This symbol indicates installation instructions to be performed specifically for the MPSs (MPS A and MPS B) on EAGLE 5 ISS A.
	This symbol indicates installation instructions to be performed specifically for the MPSs (MPS A and MPS B) on EAGLE 5 ISS B.

Initial Setup and Connecting to MPSs

Installation personnel may choose to employ various methods for connecting to an MPS. The ELAP software requires that an MPS be configured from side A. This procedure describes a likely method for connecting to EAGLE 5 ISS A and then EAGLE 5 ISS B. Installers require that all console output be captured.

Connecting to EAGLE 5 ISS A

To prepare for the configuration of the MPS on EAGLE 5 ISS A, the installer connects directly to the MPS at EAGLE 5 ISS A. Use the following method to connect to MPS B of EAGLE 5 ISS A.

1. Use the PPP utility to connect the modem located in the OOBM card in server A.
   (For information about setting up the PPP utility, refer to the *ELAP Administration Manual - 8.0* LINK .
2. When the prompt appears, enter the following command to start a secure shell session with an ELAP server:

   ```
   ssh elapconfig@<server_IP_address>
   ```

   where **<server_IP_address>** is the IP address of the MPS B at EAGLE 5 ISS A.
3. This will access the ELAP text interface.
   The **elapconfig** username and a password provided by your system administrator are required to continue.

Connecting to EAGLE 5 ISS B

To prepare for the configuration of the MPS on EAGLE 5 ISS B, the installer must first complete the connection to and configuration of the MPS on EAGLE 5 ISS A. The installer is then able to use a secure shell session to MPS at EAGLE 5 ISS B to configure it.

1. The installer can now use a secure shell session from the system prompt to the MPS A on EAGLE 5 ISS B, using the IP address shown in **Table 5-2** .

```
 ssh 192.168.61.119 Trying 192.168.61.119... Connected to 192.168.61.119. Escape character is
'^]'. SunOS 5.7
```

Procedure for Configuring ELAPs

Perform the configuration procedure by following these steps in the text-based user interface. After you have connected to an MPS (as described in Initial Setup and Connecting to MPSs ”), you can perform this procedure to configure the ELAPs in your network.

NOTE: Initial configuration cannot be performed through the GUI. The IP addresses required for browser connectivity are not defined until the initial configuration, using the text-based UI, is completed.

Using the set up and connection described previously, the installer connects to an MPS to perform configuration. In a typical installation, the installer connects directly to the MPS at EAGLE 5 ISS A to configure it, then uses **ssh** to connect to the MPS at EAGLE 5 ISS B and configure it.

1. After connecting to the MPS on EAGLE 5 ISS A, the installer is prompted to login.

   The installer must login as **elapconfig**. A note of caution appears, and the installer must evaluate them. When all the conditions of the Caution notice are satisfied, the installer presses the Return key to continue.

```
SunOS 5.7
mpsa-f0c7c3 console login: elapconfig
Password:
Caution: This is the first login of the text user interface.  Please
         review the following checklist before continuing.  Failure
         to enter complete and accurate information at this time will
         have unpredictable results.

             1. The mate MPS servers (MPS A and MPS B) must be powered on.
             2. "Initial Platform Manufacture" for the mate MPS servers
                must be complete.
             3. The sync network between the mate MPS servers must be
                operational.
             4. You must have the correct password for the ELAPdev user on
                the mate MPS server.
Press return to continue…
```

2. Upon pressing Return key to continue, the installer can now abort or proceed with the initial configuration.

   (Note that pressing the Return key would accept the default value **n**.) To continue with the configuration, enter **y**.

```
Are you sure you wish to continue? [N]: y
```

   NOTE: The configuration software is now being executed on the MPSs on EAGLE 5 ISS B. While the MPSs on EAGLE 5 ISS B were formerly referred to as 'remote', remember that the configuration software now considers the same MPS pair now to be 'local' (for more information, refer to the “ Configuration Terms and Assumptions ” section).

3. Next, the installer is prompted for the **elapdev** user password on the mate MPS server in order to confirm the secure shell keys are successfully exchanged.

   The example shows the output generated when the correct password is entered, the secure shell keys are successfully exchanged, and the UI database is set up on MPS A and MPS B at this site.

```
Password for ELAPdev@mate:
Keys exchanged.
Verifying that ssh works correctly.
ssh is working correctly.
```

```
Building the initial database on slave.
Building the initial database on master.
There was no elap.cfg file.  Using default configuration.
Allowing access from slave.
Stopping mysql on master.
Stopping mysql on slave.
Setting up master config file.
Setting up slave config file.
Copying database to slave.
Starting MySQL on master.
Starting MySQL on slave.
```

4. A successful configuration file setup results in the display (for the first time) of the ELAP Configuration Menu and its associated header information.

The server designation of MPS A at this site is displayed as well as **`hostname`**, **`hostid`**, **`Platform Version`**, **`Software Version`**, and the date.

```
MPS Side A:  hostname: mps-t1100-a  hostid: fd0a4767
             Platform Version: 2.0.2-4.0.0_50.26.0
             Software Version: ELAP 1.0.1-4.0.0_50.37.0
             Mon Sep 26 10:57:57 EDT 2005
 /-------ELAP Configuration Menu--------\
/----------------------------------------\
|  1 | Display Configuration             |
|----|-----------------------------------|
|  2 | Configure Network Interfaces Menu |
|----|-----------------------------------|
|  3 | Set Time Zone                     |
|----|-----------------------------------|
|  4 | Exchange Secure Shell Keys        |
|----|-----------------------------------|
|  5 | Change Password                   |
|----|-----------------------------------|
|  6 | Platform Menu                     |
|----|-----------------------------------|
|  7 | Configure NTP Server Menu         |
|----|-----------------------------------|
|  e | Exit                              |
\----------------------------------------/
Enter Choice:
```

5. Choose option **1** for Display Configuration, which provides a means of verifying ELAP A and ELAP B Provisioning Network IP addresses, the Time Zone, and other provisioning values for the MPS on EAGLE 5 ISS A.

```
MPS Side A:  hostname: mps-t1100-a  hostid: fd0a4767
             Platform Version: 2.0.2-4.0.0_50.26.0
             Software Version: ELAP 1.0.1-4.0.0_50.37.0
             Mon Sep 26 10:57:57 EDT 2005
ELAP A Provisioning Network IP Address = 192.168.61.90
ELAP B Provisioning Network IP Address = 192.168.61.91
Provisioning Network Netmask           = 255.255.255.0
Provisioning Network Default Router    = 192.168.61.250
ELAP A Backup Prov Network IP Address  = Not configured
ELAP B Backup Prov Network IP Address  = Not configured
Backup Prov Network Netmask            = Not configured
Backup Prov Network Default Router     = Not configured
ELAP A Sync Network Address            = 192.168.2.100
ELAP B Sync Network Address            = 192.168.2.200
ELAP A Main DSM Network Address        = 192.168.128.100
ELAP B Main DSM Network Address        = 192.168.128.200
ELAP A Backup DSM Network Address      = 192.168.129.100
ELAP B Backup DSM Network Address      = 192.168.129.200
ELAP A HTTP Port                       = 8888
ELAP B HTTP Port                       = 80
ELAP A HTTP SuExec Port                = 8001
ELAP B HTTP SuExec Port                = 8001
ELAP A Banner Connection Port          = 8473
ELAP B Banner Connection Port          = 8473
```

```
ELAP A Static NAT Address              = 10.25.50.10
ELAP B Static NAT Address              = 10.25.50.11
ELAP A LSMS Connection Port            = 7402
ELAP B LSMS Connection Port            = 7403
ELAP A EBDA Connection Port            = 1030
ELAP B EBDA Connection Port            = 1030
Time Zone                              = US/Eastern
Press return to continue…
```

6. Press Return to return to the ELAP Configuration Menu.
7. Choose option **2**, Configure Network Interfaces Menu from the ELAP Configuration Menu.

```
 /-------ELAP Configuration Menu--------\
/---------------------------------------\
|  1 | Display Configuration             |
|----|-----------------------------------|
|  2 | Configure Network Interfaces Menu |
|----|-----------------------------------|
|  3 | Set Time Zone                     |
|----|-----------------------------------|
|  4 | Exchange Secure Shell Keys        |
|----|-----------------------------------|
|  5 | Change Password                   |
|----|-----------------------------------|
|  6 | Platform Menu                     |
|----|-----------------------------------|
|  7 | Configure NTP Server Menu         |
|----|-----------------------------------|
|  e | Exit                              |
\---------------------------------------/
Enter Choice: 2
```

8. Choose option **1**, Configure Provisioning Network form the Configure Network Interfaces Menu.

```
/-----Configure Network Interfaces Menu----\
/-----------------------------------------\
|  1 | Configure Provisioning Network       |
|----|--------------------------------------|
|  2 | Configure Sync Network               |
|----|--------------------------------------|
|  3 | Configure DSM Network                |
|----|--------------------------------------|
|  4 | Configure Backup Provisioning Network |
|----|--------------------------------------|
|  5 | Configure Forwarded Ports            |
|----|--------------------------------------|
|  6 | Configure Static NAT Addresses       |
|----|--------------------------------------|
|  e | Exit                                 |
\-----------------------------------------/
Enter choice: 1
```

9. The Configure Provisioning Network lets the installer accept the default IP address values presented by the configuration software for ELAP A and ELAP B provisioning network and network netmask, or to enter specific IP values previously received from the customer for the MPS.

   Refer to the information recorded in **Table 5-1** and **Table 5-2** for the correct addresses.

   NOTE: No default value is provided for the ELAP provisioning network default router. This value must be received from the customer.

   The display for the submenu for configuring communications networks and other information shown next.

```
Verifying connectivity with mate…
Enter the ELAP A provisioning network IP Address [192.168.61.90]:
Enter the ELAP B provisioning network IP Address [192.168.61.91]:
Enter the ELAP provisioning network netmask [255.255.255.0]:
Enter the ELAP provisioning network default router IP Address: 192.168.54.250
Press return to continue…
```

10. Press the Return key, to return to the Configure Network Interfaces Menu.
11. Enter option **2**, Configure Sync Network from the Configure Network Interfaces Menu.

    NOTE: Unless there is a known network address conflict, skip all steps related to option 2.

```
/-----Configure Network Interfaces Menu----\
/-----------------------------------------\
|  1 | Configure Provisioning Network       |
|----|--------------------------------------|
|  2 | Configure Sync Network               |
|----|--------------------------------------|
|  3 | Configure DSM Network                |
|----|--------------------------------------|
|  4 | Configure Backup Provisioning Network |
|----|--------------------------------------|
|  5 | Configure Forwarded Ports            |
|----|--------------------------------------|
|  6 | Configure Static NAT Addresses       |
|----|--------------------------------------|
|  e | Exit                                 |
\-----------------------------------------/
Enter choice: 2
```

12. A sample output follows:

```
Verifying connectivity with mate...
Enter the first 3 octets for the ELAP MPS sync Network [192.168.4]
Press return to continue...
```

13. The Installer is now able to accept or change the default values default Sync Network IP address octet values presented by the configuration software.

    The installer can press the Return key or, if there is a known conflict, can enter the customer-specified IP address octet values.

14. After accepting the default value or entering a specific ELAP Sync IP address octet value, the installer returns to the Configure Network Interfaces Menu.
15. Choose option **3**, Configure DSM Network from the Configure Network Interfaces Menu.

    NOTE: Unless there is a known network address conflict, proceed to Step 18 .

```
/-----Configure Network Interfaces Menu----\
/-----------------------------------------\
|  1 | Configure Provisioning Network       |
|----|--------------------------------------|
|  2 | Configure Sync Network               |
|----|--------------------------------------|
|  3 | Configure DSM Network                |
|----|--------------------------------------|
|  4 | Configure Backup Provisioning Network |
|----|--------------------------------------|
|  5 | Configure Forwarded Ports            |
|----|--------------------------------------|
|  6 | Configure Static NAT Addresses       |
|----|--------------------------------------|
|  e | Exit                                 |
\-----------------------------------------/
Enter choice: 3
```

16. The Configure DSM Network choice automatically adds the DSM network IP address to the list of known hosts.

    The installer should then accept default IP address octets for the ELAP main DSM network and the ELAP backup DSM network presented by the configuration software unless a known network conflict exists.

```
Verifying connectivity with mate...
```

```
Enter the first 3 octets for the ELAP main DSM network [192.168.136]:
Enter the first 3 octets for the ELAP backup DSM network [192.168.137]:
```

17. After accepting the default value or entering a specific ELAP backup DSM network octet IP address value, the installer returns to the Configure Network Interfaces Menu.

18. Choose option **5**, Configure Forwarded Ports from the Configure Network Interfaces Menu.

NOTE: Unless the MPS is separated from GUI workstations and provisioning systems by a port forwarding firewall, skip all steps related to option 5. Proceed to Step 23 .

```
/-----Configure Forwarded Ports Menu------\
/-----------------------------------------\
|  1 | Change ELAP A HTTP Port              |
|----|--------------------------------------|
|  2 | Change ELAP B HTTP Port              |
|----|--------------------------------------|
|  3 | Change ELAP A HTTP SuExec Port       |
|----|--------------------------------------|
|  4 | Change ELAP B HTTP SuExec Port       |
|----|--------------------------------------|
|  5 | Change ELAP A Banner Connection Port |
|----|--------------------------------------|
|  6 | Change ELAP B Banner Connection Port |
|----|--------------------------------------|
|  7 | Change ELAP A LSMS Connection Port   |
|----|--------------------------------------|
|  8 | Change ELAP B LSMS Connection Port   |
|----|--------------------------------------|
|  9 | Change ELAP A EBDA Connection Port   |
|----|--------------------------------------|
| 10 | Change ELAP B EBDA Connection Port   |
|----|--------------------------------------|
|  e | Exit                                 |
\-----------------------------------------/
Enter choice: 5
```

19. Enter the correct option number for the port information to be entered.

Refer to the information recorded in Table 5-1 and Table 5-2 for the correct information.

NOTE: The LSMS is not capable of changing the LSMS/EBDA ports it can connect to on the MPS. Therefore, the default values for options 7 through 10 on the Configure Forwarded Ports Menu should not be changed.

```
ELAP A HTTP Port [80]:
```

20. Enter the appropriate information.

Press return once to return to the Configure Forwarded Ports Menu.

21. Enter the option number or enter e to return to the Configure Network Interfaces Menu.

22. The installer returns to the Configure Network Interfaces Menu.

23. Choose option **6**, Configure Static NAT Addresses from the Configure Network Interfaces Menu.

```
/-----Configure Network Interfaces Menu----\
/-----------------------------------------\
|  1 | Configure Provisioning Network       |
|----|--------------------------------------|
|  2 | Configure Sync Network               |
|----|--------------------------------------|
|  3 | Configure DSM Network                |
|----|--------------------------------------|
|  4 | Configure Backup Provisioning Network |
|----|--------------------------------------|
|  5 | Configure Forwarded Ports            |
|----|--------------------------------------|
|  6 | Configure Static NAT Addresses       |
|----|--------------------------------------|
|  e | Exit                                 |
```

```
\-----------------------------------------/
Enter choice: 6
```

24. Enter option **1** or **2** Configure Static NAT Addresses Menu.

Each numbered item of the Configure Static NAT Addresses Menu allows the user to specify an IP Address used outside of the firewall for remote access to the MPS. The following table shows an example of a resulting prompt.

```
/-----Configure Static NAT Addresses Menu-\
/-----------------------------------------\
|  1 | Change ELAP A Static NAT Address     |
|----|--------------------------------------|
|  2 | Change ELAP B Static NAT Address     |
|----|--------------------------------------|
|  e | Exit                                 |
\-----------------------------------------/
```

25. Enter a valid NATIP address from **Table 5-1** and **Table 5-2** .

```
ELAP A Static NAT Address:
```

26. Choose option **e** on the Configure Static NAT Addresses Menu **to return to the** Configure Network Interfaces Menu.

27. Choose option **e**, Exit from the Configure Network Interfaces Menu to return to the ELAP Configuration Menu.

28. Choose option **3**, Set Time Zone on the ELAP Configuration Menu.

NOTE: Obtain the value for the time zone from the customer's Information Services department. The default value for the time zone is US/Eastern.

```
 /-------ELAP Configuration Menu--------\
/---------------------------------------\
|  1 | Display Configuration              |
|----|------------------------------------|
|  2 | Configure Network Interfaces Menu  |
|----|------------------------------------|
|  3 | Set Time Zone                      |
|----|------------------------------------|
|  4 | Exchange Secure Shell Keys         |
|----|------------------------------------|
|  5 | Change Password                    |
|----|------------------------------------|
|  6 | Platform Menu                      |
|----|------------------------------------|
|  7 | Configure NTP Server Menu          |
|----|------------------------------------|
|  e | Exit                               |
\---------------------------------------/
Enter Choice: 3
```

29. An important Caution statement is displayed.

After noting the caution, press the Return key to continue.

```
Caution: This action requires a reboot of the affected MPS servers to
         activate the change.  Operation of the ELAP software before
         the MPS servers are rebooted may have unpredictable consequences.
Press return to continue...
```

30. The installer is prompted for confirmation on setting the time zone for MPS A and MPS B at his site.

The installer enters **y** to confirm the change. (Pressing the Return key accepts the default of 'N' (or no) and the action is aborted. In this case, the installer returns to the ELAP Configuration Menu.)

```
Are you sure you wish to change the timezone for MPS A and B? [N]: y
```

When the affirmative response **y** is given to change the time zone, the following prompt is displayed. The time zone can be the zone where the ELAP is located, Greenwich Mean Time, or another zone that is selected by the customer to meet the needs of the system. If the time zone is known, it can be entered at the prompt. If the exact time zone value is not known, just press the Return key, and a list of the valid names is displayed.

```
Enter a time zone file (relative to /usr/share/lib/zoneinfo):
```

(This list of valid time zones is also in , Time Zone File Names)If an incorrect time zone is entered or if only the Return key is pressed, a list of all available time zone values is displayed. The installer can select a value from this table.The time zone change does not take effect until the next time the MPS is rebooted.

31. After setting the time zone successfully, the installer is returned to the ELAP Configuration Menu.

32. Enter option **4**, Exchange Secure Shell Keys, from the ELAP Configuration Menu.

NOTE: Although the exchange of ELAP Secure Shell (SSH) Keys is performed automatically by the configuration software at the start of the ELAP configuration (Step 1.d), exchange of SSH keys with the LSMS (LINK)must be performed manually in order for the ELAP to receive bulk downloads from the LSMS.

```
/-------ELAP Configuration Menu--------\
/----------------------------------------\
|  1 | Display Configuration             |
|----|-----------------------------------|
|  2 | Configure Network Interfaces Menu |
|----|-----------------------------------|
|  3 | Set Time Zone                     |
|----|-----------------------------------|
|  4 | Exchange Secure Shell Keys        |
|----|-----------------------------------|
|  5 | Change Password                   |
|----|-----------------------------------|
|  6 | Platform Menu                     |
|----|-----------------------------------|
|  7 | Configure NTP Server Menu         |
|----|-----------------------------------|
|  e | Exit                              |
\----------------------------------------/
Enter Choice: 4
```

33. The following is output.

```
Are you sure you wish to exchange keys? [N]: y
```

34. The following is output.

The installer is notified that secure shell keys have already been exchanged.

```
Verifying connectivity with mate...
Caution: Secure shell keys have already been exchanged between this MPS
         server and its mate.  Secure shell is working properly.
Press return to continue...
```

35. Pressing the Return key brings up a prompt requiring confirmation to continue with the exchange.

Pressing the Return key at this confirmation prompt defaults to 'N' or 'no', and the exchange action is aborted. Entering **y** confirms the exchange, and the installer is prompted for the password of the mate. (Contact Tekelec Technical Services for the password; refer to Customer Care Center .)After entering the appropriate password, a verification of the exchange is displayed. The installer is returned to the ELAP Configuration Menu.

```
Are you sure you wish to exchange keys with the mate? [N]: y
Password for ELAPdev@mate:
Keys exchanged.
Verifying that ssh works correctly.
ssh is working correctly.
```

36. Enter option **5**, **`Change Password, from the ELAP Configuration Menu to change`** the text-based user interface password for the **`elapconfig`** login name for both MPS A and B at this site.

NOTE: If you do not need to change the text-based UI password for the MPSs at this site, skip all steps related to option 5 and proceed to Step 39 .

```
 /-------ELAP Configuration Menu--------\
/---------------------------------------\
|  1 | Display Configuration             |
|----|-----------------------------------|
|  2 | Configure Network Interfaces Menu |
|----|-----------------------------------|
|  3 | Set Time Zone                     |
|----|-----------------------------------|
|  4 | Exchange Secure Shell Keys        |
|----|-----------------------------------|
|  5 | Change Password                   |
|----|-----------------------------------|
|  6 | Platform Menu                     |
|----|-----------------------------------|
|  7 | Configure NTP Server Menu         |
|----|-----------------------------------|
|  e | Exit                              |
\---------------------------------------/
Enter Choice: 5
```

37. The installer is prompted to confirm the action of changing the password for both the MPS A and MPS B servers at this site.

Pressing the Return key accepts the default of 'N' or 'no,' and aborts the action to the change the password.Entering **y** invokes a prompt for the new password, followed by the re-entry of the password to confirm the entry.

```
Verifying connectivity with mate...
Are you sure you wish to change the text UI password on MPS A and B? [N]: y
Enter new password for text UI user:
Re-enter new password:
Press return to continue ...
```

38. Successful entry of the new password returns the installer to the ELAP Configuration Menu.

39. Enter option **7**, Configure NTP Server Menu, from the ELAP Configuration Menu to add an NTP Server.

NOTE: If you do not need to add an NTP server skip all steps related to option 7 and proceed to Step 44 .

```
 /-------ELAP Configuration Menu--------\
/---------------------------------------\
|  1 | Display Configuration             |
|----|-----------------------------------|
|  2 | Configure Network Interfaces Menu |
|----|-----------------------------------|
|  3 | Set Time Zone                     |
|----|-----------------------------------|
|  4 | Exchange Secure Shell Keys        |
|----|-----------------------------------|
|  5 | Change Password                   |
|----|-----------------------------------|
|  6 | Platform Menu                     |
|----|-----------------------------------|
|  7 | Configure NTP Server Menu         |
|----|-----------------------------------|
|  e | Exit                              |
\---------------------------------------/
Enter Choice: 7
```

40. Enter option **2**, Add External NTP Server from the ELAP Configure NTP Server Menu.

```
 /-----ELAP Configure NTP Server Menu-\
/--------------------------------------\
|  1 | Display External NTP Server     |
|----|---------------------------------|
|  2 | Add External NTP Server         |
|----|---------------------------------|
|  3 | Remove External NTP Server      |
|----|---------------------------------|
|  e | Exit                            |
\--------------------------------------/
Enter Choice: 2
```

41. Now the installer is prompted to confirm the action of adding a new NTP Server.

(Pressing Return would accept the default of 'N' or 'no', and would abort the action to add an external NTP server.) Instead, the installer enters **y**, which invokes a prompt where the IP address of the NTP server is added, as shown below.

NOTE: The installer should now enter the same IP address for the NTP server that was previously added to the MPS A and B servers on EAGLE 5 ISS A. This action allows the one NTP server to keep all MPS servers in synchronization.

```
Are you sure you wish to add new NTP Server? [N]: y
Enter the ELAP NTP Server IP Address: 192.168.61.69
Verifying NTP Server. It might take up to 1 minute.
External NTP Server [server 192.168.61.69 prefer]
has been added.
Press return to continue...
Verifying NTP Server. It might take up to 1 minute.
External NTP Server [server 192.102.61.91  prefer] has been added.
Press return to continue...
```

NOTE: All NTP Server IP addresses shown are only examples.

The display shows the server verification occurring. The installer receives a confirmation of a successful addition of the NTP server. The installer presses the Return key and returns to the ELAP Configure NTP Server Menu.

42. Enter option **1**, Display External NTP Server from the ELAP Configure NTP Server Menu, to confirm successful addition of the NTP server.

```
 /-----ELAP Configure NTP Server Menu-\
/--------------------------------------\
|  1 | Display External NTP Server     |
|----|---------------------------------|
|  2 | Add External NTP Server         |
|----|---------------------------------|
|  3 | Remove External NTP Server      |
|----|---------------------------------|
|  e | Exit                            |
\--------------------------------------/
Enter Choice: 1
```

43. The following output is displayed.

Verify that the External NTP Server IP address is correct.

```
External NTP Server [server 192.168.61.69 prefer ]
Press return to continue...
```

44. Press the Return key to return to the ELAP Configure NTP Server Menu.

45. Enter option **e** to exit the ELAP Configure NTP Server Menu and return to the ELAP Configuration Menu.

```
 /-----ELAP Configure NTP Server Menu-\
/--------------------------------------\
|  1 | Display External NTP Server     |
|----|---------------------------------|
```

```
|  2 | Add External NTP Server         |
|----|---------------------------------|
|  3 | Remove External NTP Server      |
|----|---------------------------------|
|  e | Exit                            |
\-------------------------------------/
Enter Choice: e
```

46. The installer is returned to the ELAP Configuration Menu, as shown below.

NOTE: During configuration of MPSs on EAGLE 5 ISS B, if the time zone was changed (LINK) and if the Backup Provisioning Network (LINK) was configured on either MPS, both MPS pairs on EAGLE 5 ISS A and on EAGLE 5 ISS B must be rebooted.

47. Enter option **6**, Platform Menu from the ELAP Configuration Menu.

```
 /-------ELAP Configuration Menu--------\
/---------------------------------------\
|  1 | Display Configuration             |
|----|-----------------------------------|
|  2 | Configure Network Interfaces Menu |
|----|-----------------------------------|
|  3 | Set Time Zone                     |
|----|-----------------------------------|
|  4 | Exchange Secure Shell Keys        |
|----|-----------------------------------|
|  5 | Change Password                   |
|----|-----------------------------------|
|  6 | Platform Menu                     |
|----|-----------------------------------|
|  7 | Configure NTP Server Menu         |
|----|-----------------------------------|
|  e | Exit                              |
\---------------------------------------/
Enter Choice: 6
```

48. Enter option **3**, Reboot MPS, from the ELAP Platform Menu.

```
/-----ELAP Platform Menu-\
/------------------------\
|  1 | Initiate Upgrade    |
|----|---------------------|
|  2 | Eject CD            |
|----|---------------------|
|  3 | Reboot MPS          |
|----|---------------------|
|  4 | Halt MPS            |
|----|---------------------|
|  5 | MySQL Backup        |
|----|---------------------|
|  6 | RTDB Backup         |
|----|---------------------|
|  e | Exit                |
\------------------------/
Enter Choice: 3
```

49. The installer is prompted on whether MPS A, MPS B or BOTH sides are to be rebooted.

The correct response is to select the default value of **BOTH**. Use the Return key to select both MPS A and MPS B.

```
Reboot MPS A, MPS B or [BOTH]:
```

50. When the rebooting of the present MPS server pair on EAGLE 5 ISS B ends, the Platform Menu may re-appear; however, the connection to the MPS server will be closed, and the installer is returned to the system prompt.

51. The console logon appears at the system prompt signifying the ELAP initial configuration is complete.

NOTE: The console logon is preceded by many lines of reboot output.

The initial configuration of MPSs on EAGLE 5 ISS B is now complete. Both MPSs on EAGLE 5 ISS A and MPSs on B are now configured and rebooted.

A

Time Zone File Names

Time Zone File Names

This appendix lists the valid UNIX file names, from the /usr/share/lib/zoneinfo /directory, for setting the time zone in ELAP software configuration. The initial default value for the time zone is “US/Eastern”.

africa	EET	Etc/GMT-9
asia	Egypt	etcetera
australasia	Eire	europe
Australia/ACT	EST	factory
Australia/Broken_Hill	EST5EDT	Factory
Australia/LHI	Etc/GMT	GB
Australia/North	Etc/GMT+0	GB-Eire
Australia/NSW	Etc/GMT+1	GMT
Australia/Queensland	Etc/GMT+10	GMT+0
Australia/South	Etc/GMT+11	GMT+1
Australia/Tasmania	Etc/GMT+12	GMT+10
Australia/Victoria	Etc/GMT+2	GMT+11
Australia/West	Etc/GMT+3	GMT+12
Australia/Yancowinna	Etc/GMT+4	GMT+13
backward	Etc/GMT+5	GMT+2
Brazil/Acre	Etc/GMT+6	GMT+3
Brazil/DeNoronha	Etc/GMT+7	GMT+4

Brazil/East	Etc/GMT+8	GMT+5
Brazil/West	Etc/GMT+9	GMT+6
Canada/Atlantic	Etc/GMT-0	GMT+7
Canada/Central	Etc/GMT-1	GMT+8
Canada/Eastern	Etc/GMT-10	GMT+9
Canada/East-Saskatchewan	Etc/GMT-11	GMT-0
Canada/Mountain	Etc/GMT-12	GMT-1
Canada/Newfoundland	Etc/GMT-13	GMT-10
Canada/Pacific	Etc/GMT-2	GMT-11
Canada/Yukon	Etc/GMT-3	GMT-12
CET	Etc/GMT-4	GMT-2
Chile/Continental	Etc/GMT-5	GMT-3
Chile/EasterIsland	Etc/GMT-6	GMT-4
CST6CDT	Etc/GMT-7	GMT-5
Cuba	Etc/GMT-8	GMT-6
GMT-7	Mideast/Riyadh89	Turkey
GMT-8	MST	UCT
GMT-9	MST7MDT	Universal
Greenwich	Navajo	US/Alaska
Hongkong	northamerica	US/Aleutian
HST	NZ	US/Arizona
Iceland	NZ-CHAT	US/Central
Iran	pacificnew	US/Eastern
Israel	Poland	US/East-Indiana
Jamaica	Portugal	US/Hawaii
Japan	PRC	US/Michigan
Kwajalein	PST8PDT	US/Mountain
Libya	ROC	US/Pacific
MET	ROK	US/Pacific-New
Mexico/BajaNorte	Singapore	US/Samoa
Mexico/BajaSur	solar87	UTC

Mexico/General	solar88	WET
Mideast/Riyadh87	solar89	W-SU
Mideast/Riyadh88	southamerica	Zulu

B

ELAP Local Provisioning Utility

Introduction

This chaper provides user guide information for the ELAP Local Provisioning Utility (LPU) batch command language.

LPU Commands

For each command listed in this section, the following information is given:

- A description of the command
- The command syntax

- A description of the command parameters
- An example of the command usage
- Rules, dependencies, and notes relevant to the command
- A list of related commands

upd_lnp_sub

Update LNP 10-Digit Subscription

Use this command to enter or change LNP 10-digit telephone number (TN) subscription or pooled TN's along with related services in the database.

Related services refer to message relay global title information. If the TN already exists, then the newly input data replaces the existing data. This command automatically creates the NPANXX for a TN-LRN record if the NPANXX does not already exist. It also creates an SP for a specified SP that does not already exist. The command updates data normally administered from the NPAC. Pooled TN's are allocated on an even 1000-block boundary. Specific ported TN's may overlap a pooled block and contain different routing.

Keyword

`upd_lnp_sub`

Parameters

`TN =>` (mandatory)

The telephone number.

Range = To specify a single TN subscription: 10 decimal digits

To pool a block of 1000 TNs: 7 digits with 3 asterisks (**`***`**) appended

`SP=>` (mandatory)

Service provider ID.

Range = 1-4 alphanumeric characters

`LRN`=> (mandatory)

The new location routing number.

Range = 10 decimal digits

`CLASS_DPC=> (optional)`

ANSI destination point code in the form of *network indicator-network cluster-network cluster member* (*ni-nc-ncm*) for CLASS MR GTT.

Range = *ni* **001-255**

nc **`001–255`** (if *ni* = **`001–005`**)

`000–255` (if *ni* = **`006–255`**)

ncm **000–255**

Default = Null

CLASS_SSN=> (optional)

Subsystem number for CLASS MR GTT

Range = **0, 2–255**

Default = Null

LIDB_DPC=> (optional)

ANSI destination point code in the form of *network indicator-network cluster-network cluster member* (*ni-nc-ncm*) for LIDB MR GTT.

Range = *ni* **001-255**

nc **001–255** (if *ni* = **001–005**)

000–255 (if *ni* = **006–255**)

ncm **000–255**

Default = Null

LIDB_SSN=> (optional)

Subsystem number for LIDB MR GTT

Range = **0, 2–255**

Default = Null

ISVM_DPC=> (optional)

ANSI destination point code in the form of *network indicator-network cluster-network cluster member* (*ni-nc-ncm*) for ISVM MR GTT.

Range = *ni* **001-255**

nc **001–255** (if *ni* = **001–005**)

000–255 (if *ni* = **006–255**)

ncm **000–255**

Default = Null

ISVM_SSN=> (optional)

Subsystem number for ISVM MR GTT

Range = **0, 2–255**

Default = Null

CNAM_DPC=> (optional)

ANSI destination point code in the form of *network indicator-network cluster-network cluster member* (*ni-nc-ncm*) for CNAM MR GTT.

Range = *ni* **001-255**

nc **001–255** (if *ni* = **001–005**)

000–255 (if *ni* = **006–255**)

ncm **000–255**

Default = Null

CNAM_SSN=> (optional)

Subsystem number for CNAM MR GTT

Range = **0, 2–255**

Default = Null

Examples

Individual TN:

upd_lnp_sub (TN => '1234567890', SP => 'A123', LRN => '1234567890', CLASS_ DPC => '233-233-233', CLASS_ SSN => '0');

TN Pool

upd_lnp_sub (TN => '1234567***', SP => 'A123', LRN => '1234567890', CLASS_ DPC => '233-233-233', CLASS_ SSN => '2');

Command Rules

The **TN** parameter must be 10 decimal digits or 7 decimal digits followed by 3 *s.

SP parameter must be 1-4 numbers/letters.

LRN parameter must be 10 decimal digits.

xxxxx_DPC parameter must be a valid ANSI DPC.

A service's **DPC** and **SSN** parameters must be specified together or not at all.

If the **LRN** parameter already exists, the **SP** parameter must be the same as the existing one for the **LRN** parameter.

Related Commands

dlt_lnp_sub, rtrv_lnp_sub

upd_lnp_npanxx

Update LNP NPANXX

Use this command to enter or change an existing LNP NPANXX record, including an LNP query or message relay default global title translation in the database.

The upd_lnp_npanxx command allows the user to enter or to change an LNP NPANXX and its associated LNP default global title translations in(to) the database. If the NPANXX already exists, then the newly input data replaces the existing data.

Keyword

upd_lnp_npanxx

Parameters

NPANXX=> (mandatory)

Block of 10,000 numbers.

Range = 6 digits

AIN=> (mandatory)

Local Advanced Intelligent Network (AIN) indicator.

Range = Y, N

IN=> (mandatory)

Local Intelligent Network (IN) indicator.

Range = Y, N

CLASS_DPC=> (optional)

ANSI destination point code in the form of *network indicator-network cluster-network cluster member* (*ni-nc-ncm*) for CLASS Default GTT.

Range = *ni* **001-255**

nc **001–255** (if *ni* = **001–005**)

000–255 (if *ni* = **006–255**)

ncm **000–255**

Default = Null

CLASS_SSN=> (optional)

Subsystem number for CLASS Default GTT.

Range = 0, 2–255

Default = Null

CLASS_RI=> (optional)

Routing Indicator for CLASS Default GTT.

Range = G (the outgoing CDPA routing indicator of Route on Global Title) D (the outgoing CDPA routing indicator of Route on DPC/SSN)

Default = Null

CLASS_NEWTT=> (optional)

New Translation Type for CLASS Default GTT.

Range = 0-255

Default = Null

`LIDB_DPC=> (optional)`

ANSI destination point code in the form of *network indicator-network cluster-network cluster member* (*ni-nc-ncm*) for LIDB Default GTT.

Range = *ni* **001-255**

nc **`001–255`** (if *ni* = **`001–005`**)

`000–255` (if *ni* = **`006–255`**)

ncm **`000–255`**

Default = Null

`LIDB_SSN`=> (optional)

Subsystem number for LIDB Default GTT

Range = `0, 2–255`

Default = Null

LIDB_RI=> (optional)

Routing Indicator for LIDB Default GTT.

Range = G (the outgoing CDPA routing indicator of Route on Global Title) D (the outgoing CDPA routing indicator of Route on DPC/SSN)

Default = Null

LIDB_NEWTT=> (optional)

New Translation Type for LIDB Default GTT.

Range = 0-255

Default = Null

`ISVM_DPC=> (optional)`

ANSI destination point code in the form of *network indicator-network cluster-network cluster member* (*ni-nc-ncm*) for ISVM Default GTT.

Range = *ni* **001-255**

nc **`001–255`** (if *ni* = **`001–005`**)

`000–255` (if *ni* = **`006–255`**)

ncm **`000–255`**

Default = Null

`ISVM_SSN`=> (optional)

Subsystem number for ISVM Default GTT

Range = `0, 2–255`

Default = Null

ISVM_RI=> (optional)

Routing Indicator for ISVM Default GTT.

Range = G (the outgoing CDPA routing indicator of Route on Global Title) D (the outgoing CDPA routing indicator of Route on DPC/SSN)

Default = Null

ISVM_NEWTT=> (optional)

New Translation Type for ISVM Default GTT.

Range = 0-255

Default = Null

CNAM_DPC=> (optional)

ANSI destination point code in the form of *network indicator-network cluster-network cluster member* (*ni-nc-ncm*) for CNAM Default GTT.

Range = *ni* **001-255**

nc **001–255** (if *ni* = **001–005**)

000–255 (if *ni* = **006–255**)

ncm **000–255**

Default = Null

CNAM_SSN=> (optional)

Subsystem number for CNAM Default GTT

Range = 0, 2–255

Default = Null

CNAM_RI=> (optional)

Routing Indicator for CNAM Default GTT.

Range = G (the outgoing CDPA routing indicator of Route on Global Title) D (the outgoing CDPA routing indicator of Route on DPC/SSN)

Default = Null

CNAM_NEWTT=> (optional)

New Translation Type for CNAM Default GTT.

Range = 0-255

Default = Null

Example

upd_lnp_npanxx (NPANXX => '123456', AIN => 'Y', IN => 'Y', CLASS_ DPC => '233-233-233', CLASS_ SSN => '0', CLASS_RI => 'G', CLASS_NEWTT => '71');

upd_lnp_npanxx (NPANXX => '234567', AIN => 'N', IN => 'N', CLASS_ DPC => '33-23-33', CLASS_ SSN => '72', CLASS_RI => 'D', CLASS_NEWTT => '0');

Command Rules

NPANXX parameter must be 6 decimal digits.

AIN parameter must be **Y** (for Yes) or **N** (for No).

IN parameter must be **Y** (for Yes) or **N** (for No).

xxxxx_DPC parameter must be a valid ANSI DPC.

A service's **DPC** , **SSN** , **RI** , and **NEWTT** parameters must be specified together or not at all.

xxxxx_RI parameter must be **G** (for GT) or **D** (for DPC/SSN).

xxxxx_NEWTT parameter must be 0-255, inclusive.

A service's **NEWTT** parameter must be 0 unless its **RI** parameter is **G** and its **SSN** parameter is **0**.

Notes

XXXX_RI => **G** is for an outgoing CDPA routing indicator of Route on Global Title.

XXXX_RI => **D** is for an outgoing CDPA routing indicator of Route on DPC/SSN.

Table B-1. Mapping EAGLE 5 ISS to upd_lnp_npanxx LPU Command

EAGLE 5 ISS XLAT	EAGLE 5 ISS RI	EAGLE 5 ISS SSN	EAGLE 5 ISS NGT	LPU RI	LPU SSN	LPU NEWTT
DPC	GT	-	-	G	0	0
DPC	SSN	-	-	D	0	0
DPCSSN	GT	0-255	-	G	2-255	0
DPCSSN	SSN	0-255	-	D	2-255	0
DPCNGT	GT	-	0-255	G	0	1-255

Related Commands

`dlt_lnp_npanxx`

upd_lnp_lrn

Update LNP Location Routing Number

Use this command to enter or change existing location routing number (LRN) specific information in the database.

This command allows the user to enter or to change an LNP Location Routing Number and its associated LNP message relay override global title translations in(to) the database. If the LRN already exists, then the newly input data replaces the existing data.

Keyword

`upd_lnp_lrn`

Parameters

`LRN=>` (mandatory)

The location routing number.

Range = 10 decimal digits

`SP=>` (mandatory)

Service provider ID.

Range = 1-4 alphanumeric characters

`CLASS_DPC=> (optional)`

ANSI destination point code in the form of *network indicator-network cluster-network cluster member* (*ni-nc-ncm*) for CLASS MR Override GTT.

Range = *ni* **001-255**

nc **`001–255`** (if *ni* = **`001–005`**)

`000–255` (if *ni* = **`006–255`**)

ncm **`000–255`**

Default = Null

`CLASS_SSN`=> (optional)

Subsystem number for CLASS MR Override GTT.

Range = **`0, 2–255`**

Default = Null

CLASS_RI=> (optional)

Routing Indicator for CLASS MR Override GTT.

Range = G (the outgoing CDPA routing indicator of Route on Global Title)

D (the outgoing CDPA routing indicator of Route on DPC/SSN)

Default = Null

CLASS_NEWTT=> (optional)

New Translation Type for CLASS MR Override GTT.

Range = 0-255

Default = Null

CLASS_RGTA=> (optional)

Replace Global Title Address (TN) with LRN for CLASS MR Override GTT.

Range = Y, N

Default = Null

`LIDB_DPC=> (optional)`

ANSI destination point code in the form of *network indicator-network cluster-network cluster member* (*ni-nc-ncm*) for LIDB MR Override GTT.

Range = *ni* **001-255**

nc **001–255** (if *ni* = **001–005**)

000–255 (if *ni* = **006–255**)

ncm **000–255**

Default = Null

LIDB_SSN=> (optional)

Subsystem number for LIDB MR Override GTT

Range = **0, 2–255**

Default = Null

LIDB_RI=> (optional)

Routing Indicator for LIDB MR Override GTT.

Range = G (the outgoing CDPA routing indicator of Route on Global Title) D (the outgoing CDPA routing indicator of Route on DPC/SSN)

Default = Null

LIDB_NEWTT=> (optional)

New Translation Type for LIDB MR Override GTT.

Range = 0-255

Default = Null

LIDB_RGTA=> (optional)

Replace Global Title Address (TN) with LRN for LIDB MR Override GTT.

Range = Y, N

Default = Null

ISVM_DPC=> (optional)

ANSI destination point code in the form of *network indicator-network cluster-network cluster member* (*ni-nc-ncm*) for ISVM MR Override GTT.

Range = *ni* **001-255**

nc **001–255** (if *ni* = **001–005**)

000–255 (if *ni* = **006–255**)

ncm **000–255**

Default = Null

ISVM_SSN=> (optional)

Subsystem number for ISVM MR Override GTT

Range = **0, 2–255**

Default = Null

ISVM_RI=> (optional)

Routing Indicator for ISVM MR Override GTT.

Range = G (the outgoing CDPA routing indicator of Route on Global Title) D (the outgoing CDPA routing indicator of Route on DPC/SSN)

Default = Null

ISVM_NEWTT=> (optional)

New Translation Type for ISVM MR Override GTT.

Range = 0-255

Default = Null

ISVM_RGTA=> (optional)

Replace Global Title Address (TN) with LRN for ISVM MR Override GTT.

Range = Y, N

Default = Null

CNAM_DPC=> (optional)

ANSI destination point code in the form of *network indicator-network cluster-network cluster member* (*ni-nc-ncm*) for CNAM MR Override GTT.

Range = *ni* **001-255**

nc **001–255** (if *ni* = **001–005**)

000–255 (if *ni* = **006–255**)

ncm **000–255**

Default = Null

CNAM_SSN=> (optional)

Subsystem number for CNAM MR Override GTT

Range = **0, 2–255**

Default = Null

CNAM_RI=> (optional)

Routing Indicator for CNAM MR Override GTT.

Range = G (the outgoing CDPA routing indicator of Route on Global Title) D (the outgoing CDPA routing indicator of Route on DPC/SSN)

Default = Null

CNAM_NEWTT=> (optional)

New Translation Type for CNAM MR Override GTT.

Range = 0-255

Default = Null

CNAM_RGTA=> (optional)

Replace Global Title Address (TN) with LRN for CNAM MR Override GTT.

Range = Y, N

Default = Null

Example

```
upd_lnp_lrn (LRN => '1234567890', SP => 'A123', CLASS_DPC => '233-233-233',
CLASS_SSN => '0', CLASS_RI => 'G', CLASS_NEWTT => '71', CLASS_RGTA =>
'Y');

upd_lnp_lrn (LRN => '1234567890', SP => 'A123', CLASS_DPC => '33-23-33',
CLASS_SSN => '72', CLASS_RI => 'D', CLASS_NEWTT => '0', CLASS_RGTA =>
'Y');
```

Command Rules

The **LRN** parameter must be 10 decimal digits.

The **SP** parameter must be 1-4 numbers/letters.

The **xxxxx_DPC** parameter must be a valid ANSI DPC.

The **xxxxx_RI** parameter must be **G** (for GT) or **D** (for DPC/SSN).

The **xxxxx_NEWTT** parameter must be 0-255, inclusive.

The **xxxx_RGTA** parameter must be **Y** (for Yes) or **N** (for No).

A service's **DPC** , **SSN** , **RI** , **NEWTT** , and **RGTA** parameters must be specified together or not at all.

A service's **NEWTT** parameter must be 0 unless its **RI** parameter is **G** and its **SSN** parameter is **0**.

At least one service must be specified

If the **LRN** parameter already exists, the **SP** parameter must be the same as the existing one for the **LRN** parameter.

Notes

XXXX_RI => **G** is for an outgoing CDPA routing indicator of Route on Global Title.

XXXX_RI => **D** is for an outgoing CDPA routing indicator of Route on DPC/SSN.

Table B-2. Mapping EAGLE 5 ISS to upd_lnp_lrn LPU Command

EAGLE 5 ISS XLAT	EAGLE 5 ISS RI	EAGLE 5 ISS SSN	EAGLE 5 ISS NGT	LPU RI	LPU SSN	LPU NEWTT
DPC	GT	-	-	G	0	0
DPC	SSN	-	-	D	0	0

EAGLE 5 ISS XLAT	EAGLE 5 ISS RI	EAGLE 5 ISS SSN	EAGLE 5 ISS NGT	LPU RI	LPU SSN	LPU NEWTT
DPCSSN	GT	0-255	-	G	2-255	0
DPCSSN	SSN	0-255	-	D	2-255	0
DPCNGT	GT	-	0-255	G	0	1-255

RGTA is not in the Table because it maps directly and is independent of the other parameters.

Related Commands

`dlt_lnp_lrn`

upd_split_npa

Update Split NPANXX

Use this command to force two different NPANXXs to reference the same last 4-digit telephone number (TN) in the database. During this time, updates to either NPANXX will update the same last 4-digit entry of a 10-digit ported TN. All existing NPANXX data is copied automatically to the new NPANXX for the split. It does not matter if the old block is specified as NNPANXX and the new is specified as NPANXX (i.e. the parameters are switched); they will still point to the same set of last 4 digits.

Keyword

`upd_split_npa`

Parameters

`NPANXX=>` (mandatory)

Block of 10,000 numbers.

Range = 6 digits

`NNPANXX=>` (mandatory)

New NPANXX.

Range = 6 digits

Example

```
upd_split_npa (NPANXX => '123456', NNPANXX => '234567');
```

Command Rules

NPANXX parameter must be 6 decimal digits.

NNPANXX parameter must be 6 decimal digits.

The **NPANXX** parameter must not already be split.

The new block cannot have any existing TNs.

The new block cannot be the same as the old.

The new block cannot have non-null service data that does not match the service data for the old block.

Related Commands

`dlt_split_npa`

Delete Commands

ELAP supports the following delete commands:

- dlt_lnp_sub
- dlt_lnp_npanxx
- dlt_lnp_lrn
- dlt_split_npa

dlt_lnp_sub

Delete LNP 10-Digit Telephone Number Subscription

This command is used to remove an LNP 10-digit ported telephone number (TN) or a Pooled Block of 1000 TN's along with its related services from the database. Related services refer to message relay global title information. This command deletes data normally administered from the NPAC.

Keyword

`dlt_lnp_sub`

Parameters

`TN =>` (mandatory)

The telephone number.

Range = To specify a single TN subscription: 10 decimal digits

To pool a block of 1000 TNs: 7 digits with 3 asterisks (**`***`**) appended

Examples

Individual TN:

dlt_lnp_sub (TN => '1234567890');

TN Pool

dlt_lnp_sub (TN => '1234567***');

Command Rules

The **TN** parameter must be 10 decimal digits or 7 decimal digits followed by 3 *s.

Notes

No error message when the TN parameter does not exist.

Related Commands

upd_lnp_sub, rtrv_lnp_sub

dlt_lnp_npanxx

Delete LNP Numbering Plan and Exchange

This command is used to delete an LNP numbering plan area and exchange (NPANXX) and its associated LNP query or message relay default global title translations from the database.

Keyword

dlt_lnp_npanxx

Parameters

NPANXX=> (mandatory)

Block of 10,000 numbers.

Range = 6 digits

Example

dlt_lnp_npanxx (NPANXX => '123456');

Command Rules

The **NPANXX** parameter must be 6 decimal digits.

The **NPANXX** parameter cannot be part of a NPA split.

The **NPANXX** parameter cannot be part of a ported TN.

Notes

No error message when the NPANXX parameter does not exist.

Related Commands

upd_lnp_npanxx

dlt_lnp_lrn

Delete LNP Location Routing Number

Use this command to delete an existing location routing number (LRN) and its corresponding final overriding message relay global title translations from the database. The LRN can only be deleted if it is not referenced by a 10-digit telephone number.

Keyword

dlt_lnp_lrn

Parameters

LRN=> (mandatory)

The location routing number.

Range = 10 decimal digits

Example

```
dlt_lnp_lrn (LRN => '1234567890');
```

Command Rules

The **LRN** parameter must be 10 decimal digits.

Notes

No error message when LRN parameter does not exist.

Related Commands

upd_lnp_lrn

dlt_split_npa

Delete Split NPANXX

Use this command to remove the NPANXX from the database. This command allows the user to remove 1 of the 2 different NPANXXs referencing the same last 4 digits of TN in the database.

Keyword

dlt_split_npa

Parameters

NPANXX=> (mandatory)

Block of 10,000 numbers.

Range = 6 digits

Example

dlt_split_npa (NPANXX => '123456');

Command Rules

The **NPANXX** parameter must be 6 decimal digits.

The **NPANXX** parameter must be part of NPA split.

Notes

None

Related Commands

upd_split_npa

Retrieve Command

ELAP supports the rtrv_lnp_sub retrieve commands.

rtrv_lnp_sub

Retrieve LNP 10-digit Subscription

Use this command to retrieve LNP 10 digit ported TN or a single Pooled Block of 1000 TN's along with related services from the database. Related services refer to message relay global title information. The command retrieves data normally administered from the NPAC.

Keyword

rtrv_lnp_sub

Parameters

TN=> (mandatory)

The telephone number.

Range = To specify a single TN subscription: 10 decimal digits

To pool a block of 1000 TNs: 7 digits with 3 asterisks (*******) appended

Example

Individual TN:

```
rtrv_lnp_sub (TN => '1234567890');
```

TN Pool:

```
rtrv_lnp_sub (TN => '1234567***');
```

Command Rules

The **TN** parameter must be 10 decimal digits or 7 decimal digits followed by 3 *s.

Notes

None

Related Commands

upd_lnp_sub, dlt_lnp_sub

Output

Found:

```
TN = 2345678000
LRN = 0123456789
SP = oc1
Service TT  DPC         SSN RI NEWTT
------- --- ----------- --- -- -----
CLASS     3 001-001-001   0 G    0
ISVM      6 001-002-003   4 D  ---
TN = 2345000***
LRN = 0123456789
SP = oc1
Service TT  DPC         SSN RI NEWTT
------- --- ----------- --- -- -----
CLASS     3 001-001-001   0 G    0
ISVM      6 001-002-003   4 D  ---
```

Not Found:

```
TN 9195551234 not found.
```

Miscellenous Commands

ELAP supports the following miscellenous commands:

- set_echo
- set_cont_wo_remote

set_echo

This command is used to Turn on or off the output of calls to commands.

Example

set_echo(1);

dlt_lnp_sub(TN => '9195551234');

set_echo(0);

dlt_lnp_sub(TN => '9195554321');

Outputs

```
Processing dlt_lnp_sub (
TN => '9195551234',
)
Done.
```

set_cont_wo_remote

This command is used to turn on or off the ability to continue to execute commands in the face of no connection to the remote LSMS port.

Example

set_cont_wo_remote(1);

Common Information

The following sub-sections highlight messages, formats, templates, and errors that are not specific to particular batch commands.

Success message

The following message is output when a batch file is successfully executed:

```
SUCCESS: The LPU batch file has been successfully executed.
```

Error message format

All command errors will follow the following format:

```
E1074: LPU batch failure: Batch Error: Message text at /export/home/elapall/LPU_batch line x
```

Message text will be replaced with the message text associated with the rule as provided in the command details.

x will be replaced with the line number within the batch file where the error occurred.

Service parameters within error messages

When a service parameter is specified in the error message texts, a template is used to avoid repeating the message text for each possible service.

The templates are as follows:

- xxxx_DPC
- xxxx_SSN
- xxxx_RI

- xxxx_NEWTT
- xxxx_RGTA

xxxx will be replaced with the appropriate service's mnemonic (e.g. CLASS, LIDB, ISVM, or CNAM)

Missing mandatory parameter

For all commands, the message text for a missing mandatory parameter is the following:

Missing mandatory argument x

x will be replaced with the parameter's mnemonic (e.g. TN, SP, LRN, AIN, IN, or NPANXX).

Communication errors

The following are connection errors that may occur when processing batch commands. They are listed from most common to least common. The most likely corrective action for each are included:

1. Could not connect to local LSMS port
    - Check the LSMS Connection Allowed state. If the LSMS Connection is currently Disabled, then Enable the LSMS Connection.
    - Check the LSMS HS Bulk Download Enabled state. If the LSMS Bulk Download for this ELAP is currently Enabled, then Disable the LSMS Bulk Download for this ELAP.
    - Check the state of the software on both ELAP sides. If the software is stopped (side is down), then start the software.
    - Possibly, the LSMS was in the middle of connecting to the ELAPs. Try again.
2. No connection to remote LSMS port
    - Probably, the LSMS was in the middle of connecting to the ELAPs. Try again.
3. Could not connect to local LPU port
    - Probably, a user on the mate started a batch at the same time which grabbed the port before the local user's batch could. Try again.
4. Connection to LPU port closed by another instance
    - Probably, the local user's batch grabbed the port just before or just after the mate user's batch. Try again.

The following are send and receive errors that may occur when processing batch commands. They are listed in no particular order. They should very rarely happen:

1. Could not send message
2. Receive header timed out
3. Could not receive header
4. Receive data timed out
5. Could not receive data

Perl errors

The following are Perl-related errors that may occur along with their probable causes:

1. Unable to create sub named "*Safe::Root0::x"
    - Probably misspelled command or function name

Perl Statements and Functions

The batch language is actually a subset of the Perl language with the addition of the functions/commands specified under LPU Commands . For more information on Perl, see reference [1].

The following subsections highlight some of the more useful Perl statements and functions for batch processing.

#

If not quoted, comments out rest of line.

foreach

Iterates through a list, assigning the current element to a variable. For example, the following will retrieve TNs 919-555-0000 through 919-555-9999:

```
foreach $extension ('0000'..'9999')
{
    rtrv_lnp_sub(TN => "919555$extension");
}
```

print

Outputs string(s). For example, the following will output the TNs being deleted

```
foreach $tn ('9195550000'..'9195559999')
{
print ("Deleting TN $tn \n");
dlt_lnp_sub (TN => $tn);
}
```

scalar localtime

Returns the current time for the current locale in UNIX date command form. For example, the following:

```
print scalar localtime, "\n";
```

Output the following

```
Wed Apr 24 15:45:27 2002
```

eval

Allows user to catch an error without stopping execution of the batch. On error, the error message is put into the special variable $@ and execution continues at the next line after the eval block.

For example without an eval, the following:

```
set_echo(1);
upd_lnp_sub (TN=>'9194601234', LRN=>'3456789012', SP=>'tklc',
CLASS_SSN=>2);
upd_lnp_sub (TN=>'9194602341', LRN=>'3456789012', SP=>'tklc');
rtrv_lnp_sub(TN=>'9194601234');
```

Produces:

```
Processing upd_lnp_sub (
  CLASS_SSN => '2',
  LRN => '3456789012',
  SP => 'tklc',
  TN => '9194601234',
)
ERROR: An error occurred while attempting the requested operation.
E1074: LPU batch failure: Batch Error: CLASS_DPC and CLASS_SSN must be specified together at /export/
home/elapall/LPU_batch line 3
```

However, if one puts the updates in an eval, the error can be caught and dealt with instead of exiting the batch execution. For example:

```
set_echo(1);
eval
{
    upd_lnp_sub (TN=>'9194601234', LRN=>'3456789012', SP=>'tklc',
CLASS_SSN=>2);
    upd_lnp_sub (TN=>'9194602341', LRN=>'3456789012', SP=>'tklc');
};
print $@ if $@;
rtrv_lnp_sub(TN=>'9194601234');
rtrv_lnp_sub(TN=>'9194602341');
```

Produces:

```
Processing upd_lnp_sub (
  CLASS_SSN => '2',
  LRN => '3456789012',
  SP => 'tklc',
  TN => '9194601234',
)
CLASS_DPC and CLASS_SSN must be specified together at /export/home/elapall/LPU_batch line 5
Processing rtrv_lnp_sub (
  TN => '9194601234',
)
TN 9194601234 not found.
```

```
Processing rtrv_lnp_sub (
  TN => '9194602341',
)
TN 9194602341 not found.
Done.
SUCCESS: The LPU batch file has been successfully executed.
```

Glossary

A

ACK	Data Acknowledgement
ACT	Activate
AIN	Advanced Intelligent Network
ANSI	American National Standards Institute
AS	Application Server

C

CD	Carrier Detect Compact Disk
CET	Customer Environment Test
Channel	A single Time-Division-Multiplexed (TDM) timeslot within a channelized E1/T1 port. Generically, channels can be used for transporting signaling, digitized voice, or data information. Unused channels typically are filled with defined idle codes designed to maintain sufficient ones density to ensure frame-level synchronization.
CLASS	Custom Local Area Signaling Service Custom Local Area Subscriber Services
CLLI	Common Language Location Identifier
CNAM	Calling Name Delivery Service
CSR	Customer Service Request
CTS	Clear to Send

D

daemon	A process that runs in the background and performs a specified operation at predefined times or in response to certain events.
Database	All data that can be administered by the user, including cards, destination point codes, gateway screening tables, global title translation tables, links, LNP services, LNP service providers, location routing numbers, routes, shelves, subsystem applications, and 10 digit telephone numbers.
DB	Database Daughter Board Documentation Bulletin
DN	Directory number A DN can refer to any mobile or wireline subscriber number, and can include MSISDN, MDN, MIN, or the wireline Dialed Number.
DPC	Destination Point Code The point code of the signaling point to which the MSU is routed. This point code can be adjacent to the EAGLE 5 ISS, but does not have to be.

DSM	Database Service Module.

E

EBDA	Enhanced Bulk Download and Audit
ECC	Error Correction Coded
ELAP	EAGLE LNP Application Processor

F

FAK	Feature Access Key.
FTA	File Transfer Area.
FTP	Feature Test Plan File Transfer Protocol.

G

GB	Gigabyte — 1,073,741,824 bytes
GMT	Greenwich Mean Time
GPS	Global Positioning System
GT	Global Title Routing Indicator
GTT	Global Title Translation.
GUI	Graphical User Interface

H

HS	High Speed
HSOP	High Speed Operation Protocol

I

ID	Identity, identifier
IMSI	International Mobile Station Identity
IMT	Inter-Module-Transport The communication software that operates the inter-module-transport bus on all cards except the LIMATM, DCM, DSM, and HMUX.
IN	Intelligent Network
IP	Intelligent Peripheral Internet Protocol
IP^7	Tekelec's Internet Protocol to SS7 Interface
IP Address	The location of a device on a TCP/IP network. The IP Address is a number in dotted decimal notation which looks something like [192.168.1.1].
IPM	Implementation Project Management IMT Power and Multiplexer Card Initial Product Manufacture
IS-ANR	In Service - Abnormal

	The entity is in service but only able to perform a limited subset of its normal service functions.
IS-NR	In Service - Normal
ISS	Integrated Signaling System

K

Key	For the ICNP feature, a unique DS value used to access a table entry, consisting of a number length and number type.

L

LAN	Local Area Network See also STP LAN.
LED	Light Emitting Diode
LIDB	Line Information Database
LIM	Link Interface Module
LNP	Local Number Portability
LRN	Location Routing Number A 10 digit number identifying the new location of the ported 10 digit telephone number.
LSMS	Local Service Management System

M

MEA	Memory Extension Applique Mismatch of Equipment and Attributes
MMI	Man-Machine Interface
MPS	Multi-Purpose Server
MR	Message Relay
MSU	Message Signaling Unit
MTSU	Message Transfer System Utility

N

NAK	Negative Acknowledgment
NGT	New Global Title
NPA	Number Plan Area.
NPAC	Number Portability Administration Center
NPANXX	The area code and office prefix of a telephone number. For example, with the telephone number 919-555-1212, the digits 919 are the area code (NPA) and the digits 555 are the office prefix (NXX).
NTP	Network Time Protocol

O

OAM	Operations, Administration, and Maintenance
OOS-MT	Out of Service - Maintenance

OS	Operating System Operations Systems

P

PC	Point Code.
PDBA	Provisioning Database Application
PDBI	Provisioning Database Interface
PMTC	Peripheral Maintenance
PPP	Point-to-Point Protocol

R

RAID	Redundant Array of Independent Disks
RAM	Random Access Memory A type of computer memory that can be accessed randomly; that is, any byte of memory can be accessed without touching the preceding bytes.
Restricted	The network management state of a route, link set, or signaling link that is not operating properly and cannot carry all of its traffic. This condition only allows the highest priority messages to sent to the database entity first, and if space allows, followed by the other traffic. Traffic that cannot be sent on the restricted database entity must be rerouted or the traffic is discarded.
RFC	Request for Comment
RI	Routing Indicator
RMTP	Reliable Multicast Transport Protocol
RN	Routing Number
Route	A path to another signaling point.
RTDB	Real Time Database
RTS	Ready to Send Request to Send

S

SCCP	Signaling Connection Control Part
SCM	System Configuration Manager System Configuration Matrix.
SP	Service Provider Signaling Point
SPID	Service Provider ID
Split NPA	Split Number Planning Area A process that forces two different NPANXXs to reference the same last 4 digits of a 10 digit ported telephone number in the database. When either NPANXX is updated, the 10 digit ported telephone numbers in each NPANXX with the same last 4 digits are updated. When the NPANXX is split, all existing NPANXX data for the NPANXX being split is copied to the new NPANXX.
SSH	Secure Shell
SSN	SS7 Subsystem Number

	Subsystem Number
STP	Signal Transfer Point
Subsystem Number	The subsystem number of a given point code. The subsystem number identifies the SCP application that should receive the message or the subsystem number of the destination point code to be assigned to an X.25 address or the LNP subsystem of the EAGLE 5 ISS. A value of the routing indicator portion of the global title translation data commands indicating that no further global title translation is required for the specified entry.

T

TCP/IP	Transmission Control Protocol/Internet Protocol
TN	Telephone Number A 10 digit ported telephone number.

U

UAM	Unsolicited Alarm Message.
UDP	User Datagram Protocol
UI	User Interface
UIM	Unsolicited Information Message

V

VIOL	A value displayed on an application GUI that indicates that the client brower's Java policy file is incorrect.
VSCCP	VxWorks Signaling Connection Control Part The application used by the Service Module card to support the G-Flex, G-Port, INP, AINPQ, EIR, A-Port, IGM, V-Flex, and LNP features. If the G-Flex, G-Port, INP, AINPQ, EIR, A-Port, IGM, V-Flex, or LNP feature is not turned on, and a Service Module card is present, the VSCCP GPL processes normal GTT traffic.

W

WAN	Wide Area Network
WSMSC	Wireless Short Message Service Center

X

XLAT	Translate Indicator

Index

C

D

S