Tekelec EAGLE® 5
Integrated Signaling System

EPAP Administration Manual

910-5058-001 Revision B
November 2007

TEKELEC

Notice
Information in this documentation is subject to change without notice. Unauthorized use or copying 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 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, IP^7, IP^{7}Edge, IP^7 Secure Gateway, and TALI are registered trademarks of Tekelec. TekServer and A-Port 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

Foreign Patent Numbers:

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

Ordering Information
For additional copies of this document, contact your Tekelec sales representative.

Table of Contents

List of Figures

List of Tables

1

Introduction

Overview

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

The EPAP program runs on the Multi Purpose Server (MPS), a hardware platform that supports high speed provisioning of large databases for the Tekelec EAGLE 5 Integrated Signaling System (ISS). EPAP supports the G-Flex, G-Port, EIR, and INP features for the European market, as well as G-Flex in North America.

Change bars in this manual represent changes made since the publication of 910-4475-001 Revision A, on which this manual is based.

Scope and Audience

This manual is intended for anyone performing EPAP administration or using the EPAP 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 EPAP user interface documentation, the organization of this manual, and how to get technical assistance.
- Chapter 2, *"Functional Description,"* provides a description of the EPAP graphical user interface and EPAP overall design and operation.
- Chapter 3, *"EPAP Graphical User Interface,"* describes how to log into the EPAP user interface and how to use the EPAP user interface menus.
- Chapter 4, *"Messages, Alarms, and Status Reporting,"* describes EPAP status, alarms, and error messages.
- Chapter 5, *"EPAP Software Configuration,"* describes the text-based user interface that performs EPAP configuration and initialization.
- Appendix A, “EPAP Software Configuration,” explains how to perform EPAP software initialization, configure IP addresses, and create the Provisioning Databases (PDBs).

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 Packaging, Delivery, and Updates

Customer documentation is provided with each system in accordance with the contract agreements. It is updated whenever significant changes that affect system operation or configuration are made. Updates may be issued as an addendum, or a reissue of the affected documentation.

The document part number appears on the title page along with the current revision of the document, the date of publication, and the software release that the document covers. The bottom of each page contains the document part number and date of publication.

Two types of releases are major software releases and maintenance releases. Maintenance releases are issued as addenda with a title page and change bars. On changed pages, the date and document part number are changed; on unchanged pages that accompany the changed pages, the date and document part number are unchanged.

When the software release has a minimum affect on documentation, an addendum is provided. The addendum contains an instruction page, a new title page, a change history page, and replacement chapters with the date of publication, the document part number, and change bars.

If a new release has a major impact on documentation, such as a new feature, the entire documentation set is reissued with a new part number and a new release number.

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. This manual has three admonishments, listed in descending order of priority.

	**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 Assistance

The Tekelec Customer Care Center offers a point of contact through which customers can receive support for problems. The Tekelec Customer Care Center is staffed with highly-trained engineers to provide solutions to technical questions and issues seven days a week, twenty-four hours a day. A variety of service programs are available through the Tekelec Customer Care Center to maximize the performance of Tekelec products that meet and exceed customer needs.

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

  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.

Once a CSR is issued, Customer Care Services 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 Technical Services 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 Tekelec Customer Care Services twenty-four hours a day, seven 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 Tekelec Customer Care Services.

Acronyms

ACK	Acknowledgment message
ANSI	American National Standards Institute
ASCII	American Standard Code for Information Interchange
CC	Country Code
CCGT	Cancel Called Global Title
CD-ROM	Compact Disk Read Only Memory
CEIR	Central Equipment Identity Register
CPA	Client provisioning application
CPU	Central Processing Unit
DA	Digit Action
DB	Database
DCB	Device Control Block
DN	Dialed Number (DN can refer to any mobile or wireline subscriber number, and can include MSISDN, MDN, MIN, or the wireline Dialed Number.)
DSM	Database Services Module
EIR	Equipment Identity Register
ELAP	Eagle LNP Application Processor
EPAP	Eagle Provisioning Application Processor
FTP	File Transfer Protocol
GB	Gigabyte
GDB	G-Flex/G-Port Data Base
G-Flex	GSM Flexible Numbering feature
GPL	Generic Program Load
G-Port	GSM Number Portability feature
GPDB	G-Port Database
GSM	Global System for Mobile Telecommunication
GTA	Global Title Address
GTT	Global Title Translation

GUI.....Graphical User Interface

GWS.....Gateway Screening

HTML .....Hypertext Markup Language

HTTP .....Hypertext Transfer Protocol

HTTPS .....Secure Hypertext Transfer Protocol

ID.....Identifier

IMEI .....International Mobile Equipment Identity

IMEISV .....International Mobile Equipment Identity Software Version Number

IMSI .....International Mobile Subscriber Identity

IMSI .....International Mobile Station Identifier

INAP.....Intelligent Network Application Protocol

INP.....INAP-based Number Portability feature

IP .....Internet Protocol

IS-ANR .....In Service - Abnormal

ISDN .....Integrated Services Digital Network

IS-NR .....In Service - Normal

KB.....Kilobyte

LAN .....Local Area Network

LIM .....Link Interface Module

LNP.....Local Number Portability

LSMS.....Local Service Management System

MAP.....(1) Mobile Application Part
(2) Mated Application

MB.....Megabyte

MDM .....Mobile Dialed Number

MIN.....Mobile Identification Number

MMI .....Man-Machine Interface

MNP.....Mobile Number Portability

MNPSMS.....Portability Check for Mobile Originated SMS

MPS.....Multi-Purpose Server

MSC ..... Mobile Switching Center

MSISDN ..... Mobile Switching Integrated Services Digital Network Number

MSU ..... Message Signal Unit

MTS ..... Message Transfer System

MTSU ..... Message Transfer System Utilities

MTT ..... Mapped Translation Type

NAK ..... Negative Acknowledgment message

NE ..... (1) Network Entity
(2) Network Element

NEBS ..... Network Equipment Building Standards

NTP ..... Network Time Protocol

OAM ..... Operation Administration & Maintenance

OAP ..... Operation System Support/Application Processor

OOS-MT-DSBLD ..... Out of Service - Maintenance Disabled

PAP ..... Previously Active PDBA (the PDBA that fails)

PC ..... Point Code

PDB ..... Provisioning Database

PDBA ..... Provisioning Database Application

PDBI ..... Provisioning Database Interface

PID ..... Process Identifier

PP ..... PDBA Proxy

PPP ..... Point-to-Point Protocol

RFC ..... Request for Comment document

RI ..... Routing Indicator

RMTP ..... Reliable Multicast Transport Protocol

RN ..... Routing Number

RTDB ..... Real-Time Database

SCCP ..... Signaling Connection Control Part

SEAC ..... Signaling Engineering and Administration Center

SFTP ..... Secure File Transport Protocol

SNCC	Signaling Network Control Center
SP	Signalling Point
SRF	Signaling Relay Function
SRI	Send Routing Information
SRI_SM	Send Routing Information for Short Message
SS7	Signaling System #7
SSH	Secure Shell
SSN	Subsystem Number
STP	Signaling Transfer Point
TAP	Temporarily Active PDBA (the formerly Standby PDBA)
TCP	Transmission Control Protocol
TDM	Terminal Disk Module
TKLC	Tekelec
UAM	Unsolicited Alarm Message
UDP	User Datagram Protocol
UIM	Unsolicited Information Message
UTC	Universal Time Coordinated
VSCCP	VxWorks Signaling Connection Control Part

2

Functional Description

General Description

The Multi Purpose Server (MPS) hardware platform supports high speed provisioning of large databases for the EAGLE 5 ISS. The MPS is composed of hardware and software components that interact to create a secure and reliable platform. MPS supports the EAGLE Provisioning Application Processor (EPAP).

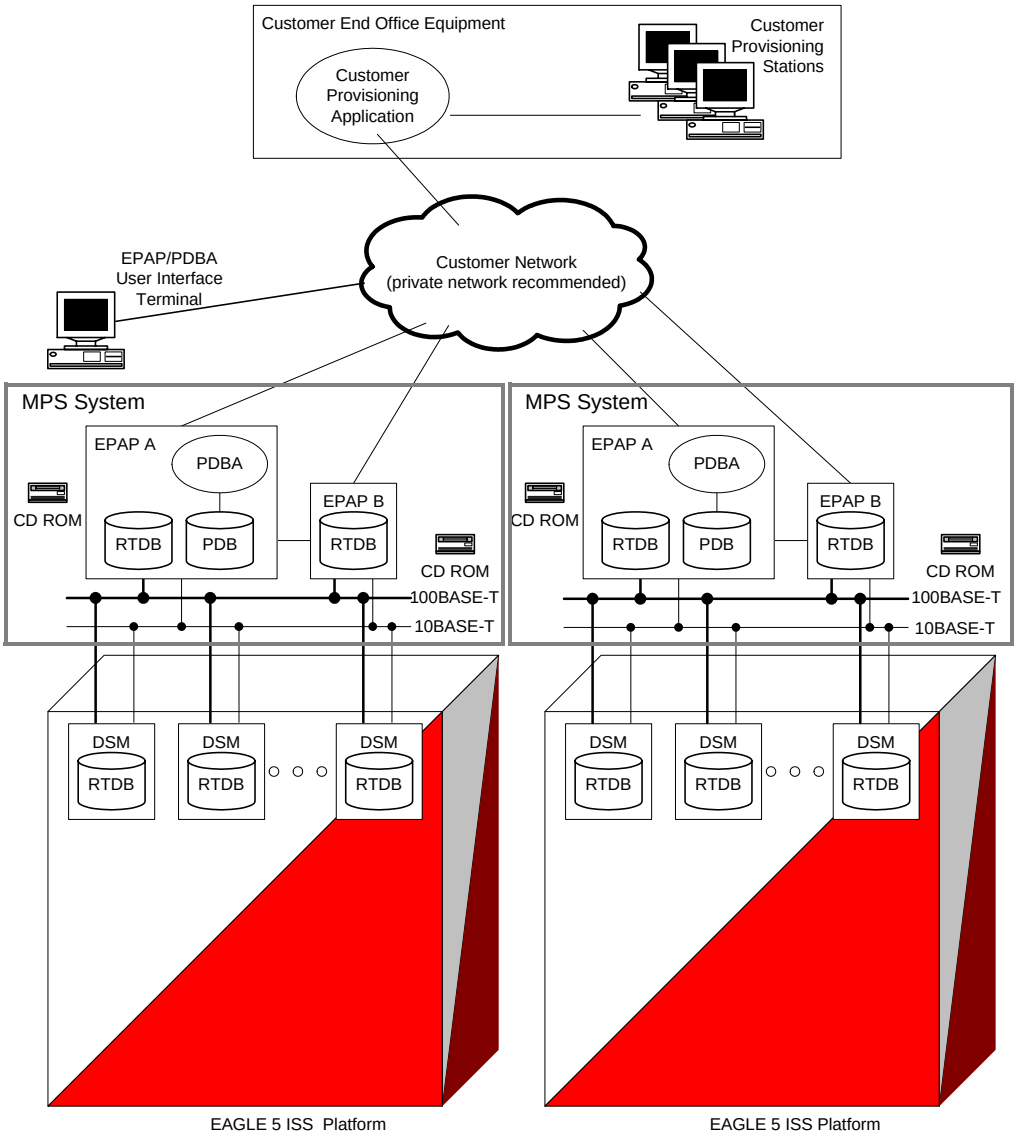
The EPAP platform, coupled with the Provisioning Database Application (PDBA), facilitates and maintains the database required by advanced services such as A-Port, G-Flex, G-Port, INP and EIR. The EPAP serves two major purposes:

- Accept and store data provisioned by the customer
- Update customer provisioning data and reload databases on the DSM (Database Service Module) cards in the EAGLE 5 ISS

NOTE: The EAGLE 5 ISS supports more than one model of DSM card. The cards differ in the size of database and the transactions/second rate that they support. In this manual, the term DSM is used to mean any model of DSM, unless a specific model is mentioned. For more information about the supported DSM models, refer to the *Hardware Manual - EAGLE 5 ISS*.

During normal operation, information flows through the EPAP/PDBA with no intervention. Each EPAP has a graphical user interface that supports maintenance, debugging, and platform operations. The EPAP user interface includes a PDBA user interface for configuration and database maintenance. Chapter 3, *"EPAP Graphical User Interface,"* describes the EPAP and PDBA GUI menus. (Also see Chapter 5, *"EPAP Software Configuration,"* for a description of the text-based user interface that performs initial EPAP configuration.)

Figure 2-1. Mated EAGLE 5 ISS Platform Example



Overall Design

An EPAP system consists of two mated EPAP processors (A and B) installed as part of an EAGLE 5 ISS. A set of DSMs, which hold a copy of the real-time database (RTDB), is part of the EAGLE 5 ISS.

Two high-speed Ethernet links, referred to as the main and backup DSM networks, connect the DSMs and the EPAPs. Another Ethernet link connects the two EPAPs; it is referred to as the EPAP Sync network.

Figure 2-2 shows the network layout along with examples of typical IP addresses of the network elements. The shaded portion represents a second EAGLE 5 ISS and mated EPAPs deployed as a mated EAGLE 5 ISS.

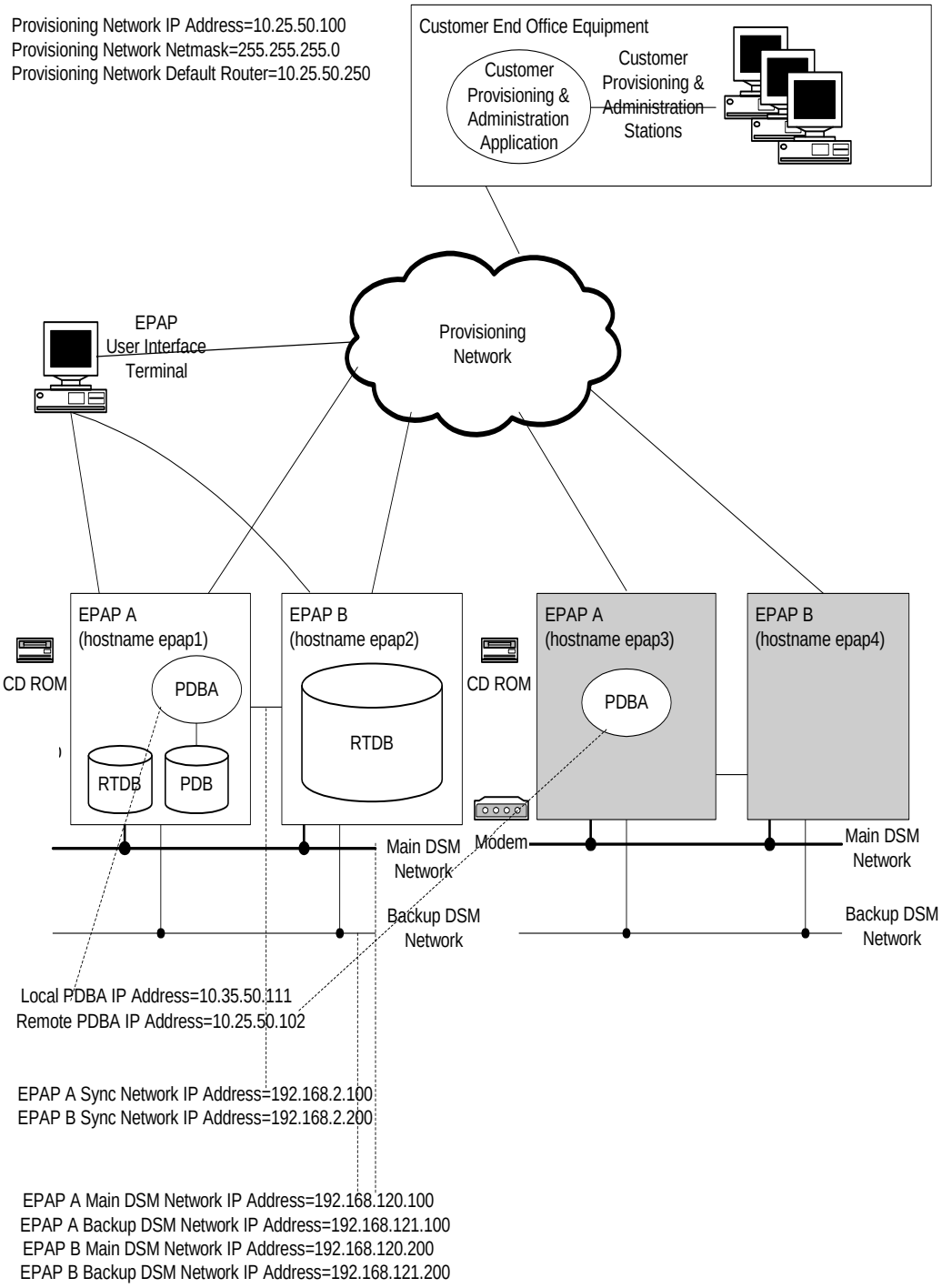
The EPAP system maintains the real-time database (RTDB) required to provision the EAGLE 5 ISS DSM cards, and maintains redundant copies of both databases on each mated EPAP.

One EPAP runs as the Active EPAP and the other as the Standby EPAP. In normal operation, the DSM database is provisioned through the main DSM network by the Active EPAP.

In case of failure of the Active EPAP, the Standby EPAP will take over the role of Active EPAP and continue to provision the database. In the case where the main DSM network fails the Active EPAP will switch to the backup DSM network to continue provisioning the DSMs. At any given time there will be only one Active EPAP using one DSM network per EPAP system.

NOTE: The Provisioning Multiple EPAPs Support feature provides the ability to connect to a single active EPAP A / PDB and have that PDB provision up to four MPS devices (each of which contains an EPAP A and EPAP B). For more information about this feature, see "Provisioning Multiple EPAPs Support" on page 2-17.

Figure 2-2. Example EPAP Network IP Addresses



NOTE: The IP addresses in Figure 2-2 are only examples; they can be different in your network.

EPAP Switchover

EPAPs assume an Active or a Standby role through negotiation and algorithm. This role impacts the way the EPAP handles its various external interfaces. External provisioning is allowed only through the Active EPAP. Only the Active EPAP can provide maintenance information to EAGLE 5 ISS. The EPAP role also plays an important part in many design details of the individual software components. The EPAP role *does not* affect the Active/Standby role of the PDBA.

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

1. The EPAP maintenance component becomes isolated from the maintenance component on the mate EPAP 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 maintenance task across the EPAP Sync network

   – The mate maintenance task across the main DSM network

   – Any DSM 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 EPAP is forced to Standby by the user interface Force to Become Standby operation.

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

Table 2-1. EPAP 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 EPAP is not visible on the DSM networks, the EPAP assumes an Active role if *any* DSMs are visible on the DSM networks.

2. If the EPAP GUI menu item is used to force an EPAP to Standby role, no condition will cause it to become Active until the user removes the interface restriction with another menu item. (See “Force Standby” on page 3-24 and “Change Status” on page 3-25.)

If none of the Standby conditions exist for either EPAP, the EPAPs will negotiate an Active and a Standby. The mate will be considered unreachable after two seconds of attempted negotiation.

For information about the effect of asynchronous replication on switchover, see “Asynchronous Replication Serviceability Considerations” on page 2-24.

EPAP Component Overview

The major components that run on the EPAP are

- The PDBA task
- The PDB database
- The RTDB task
- The RTDB Audit
- The maintenance task
- The DSM provisioning task

The PDB is the provisioning "golden copy" database. The database records are continuously updated to the PDB from the customer network. The customer uses the Provisioning Database Interface (PDBI) to move data over the customer network to the EPAP PDBA. The subscription and entity object commands used by PDBI are described in the *Provisioning Database Interface Manual*.

The PDBA task writes customer data into the PDB, which is reformatted to facilitate fast lookups. After conversion, the data is written to the RTDB.

The DSM provisioning task resides on both the EPAP A and the EPAP B. It communicates internally with the RTDB task, and the EPAP maintenance task. The DSM provisioning task uses RMTP to multicast provisioning data to connected DSM cards across the two DSM networks. The RTDB audit runs as part of the RTDB task.

One EPAP is equipped with both the PDB and RTDB views of the database; the mate EPAP has just the RTDB view. An EPAP with just the RTDB view must be updated by an EPAP that has the PDB view.

The DSM database can go out of sync (incoherent) due to missed provisioning or card reboot. Out-of-sync DSMs are re-provisioned from the RTDB on the Active EPAP.

The maintenance task is responsible for reporting the overall stability and performance of the system. The maintenance task communicates status and alarm information to the primary DSM.

Provisioning Database Interface

Provisioning clients connect to the EPAPs through the Provisioning Database Interface (PDBI). PDBI contains commands that allow the provisioning and retrieving of all provisioning data. PDBI is described in the *Provisioning Database Interface Manual*.

Network Connections

This section describes the four types of EPAP network connections.

DSM Networks

These networks carry provisioning data from the RTDBs on the EPAP to the RTDBs on the DSMs. They also carry reload and maintenance traffic to the DSMs. The main DSM network runs at 100BASE-T and the backup DSM network runs at 10BASE-T. Each network connects EPAP A and EPAP B to each DSM on a single EAGLE 5 ISS platform.

The first two octets of the EPAP 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 EPAP is configured as EPAP A, the fourth octet has a value of 100.
- If the EPAP is configured as EPAP B, the fourth octet has a value of 200.

Table 2-2 summarizes the derivation of each octet.

The configuration menu of the EPAP user interface contains menu items for configuring the EPAP network addresses. (See “EPAP Configuration Menu” on page 5-16).

Table 2-2. 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 EPAP A 200 for EPAP B 1 - 25 for DSM networks

EPAP Sync Network

The EPAP Sync network is a point-to-point network between the MPS servers. This network provides a high-bandwidth dedicated communication channel for MPS data synchronization. This network runs at full-duplex Gigabit Ethernet.

The first two octets of the EPAP 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 EPAP Sync network address is set to 2 as the default. It can be changed if necessary. It is important to follow the instructions in “EPAP Sync Network” on page 2-9 if you change this octet value.

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

Dialup PPP Network

The Dialup Point-To-Point Protocol (PPP) Network (not shown in Figure 2-2) allows multiple user interface sessions to be established to the EPAP from a remote workstation.

This provides support for one modem per MPS server, each of which can be configured for PPP (TCP/IP and UDP/IP). With this capability, multiple networked applications can be run across the modem link simultaneously. Logging in as the root user is not supported across the modem link directly, but once a PPP session is established root logins can be accomplished via secure shell.

Two entries are required in the `/etc/hosts` file to properly configure the PPP Network:

192.168.1.101 server_ppp0

192.168.1.102 client_ppp0

The default configuration allows a dial-in session to make connections to the local server once connected. Each application deployed on the MPS Server can customize these entries to match their specific network configuration and can allow connections to additional nodes on the network.

The internal modem adapter is installed in either PCI slot 7 or 8 in the MPS server. The modem card is automatically detected and configured to allow dial-in access without any additional configuration.

Customer Network

The customer network (the provisioning network) carries the following traffic:

- Customer queries and responses to the PDB (PDBI)
- Updates between PDBAs on mated EPAP systems
- Updates between PDBAs and RTDBs when the PDBA and the RTDB are not on the same platform

  This occurs if the RTDBs on one EPAP system cannot communicate with their local PDBA. Those RTDBs would then attempt to communicate with the PDBA on the mate EPAP system.
- RTDB reload traffic if the Active PDBA is not located on the same EAGLE 5 ISS as the RTDB

  This occurs if the RTDBs on one EPAP system cannot communicate with their local PDBA. Those RTDBS would then attempt to communicate with the PDBA on the mate EPAP system.
- PDBA import/export (file transfer) traffic
- Traffic from a PDBA reloading from its mate
- EPAP and PDBA user interface traffic

A dedicated network is recommended, but it is possible that unrelated customer traffic could also use this network.

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 EPAP application have the option to be configured through the EPAP GUI, to communicate and synchronize time with a customer defined NTP time server. The prefer keyword is used to prevent clock-hopping when additional MPS or NTP servers are defined.

The core MPS platform provides a default NTP configuration file. The MPS configuration entails adding an NTP hostname alias **ntppeerA** and **ntppeerB** to the `/etc/hosts` file.

If the network is equipped with firewalls, configure the firewall(s) to pass NTP protocol on IP port 123 (both TCP and UDP) between the MPS server(s) and the NTP servers/peers. The program `ntpdate` uses TCP while `ntpd` uses udp.

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 EPAP system, MPS servers are also configured to share their time with their remote PDBA server.

ITU Duplicate Point Code Support

The EPAP ITU Duplicate Point Code Support feature for PDBI allows point codes to be provisioned in the PDB using a two character "group code." This feature works in concert with the EAGLE ITU Duplicate Point Code feature, which allows an EAGLE 5 ISS mated pair to route traffic for two or more countries with overlapping (identical) point code values.

NOTE: Using the EPAP ITU Duplicate Point Code Support requires the activation of the EAGLE ITU Duplicate Point Code feature (ITUDUPPC). For information about activating any feature in the EAGLE 5 ISS, refer to the `chg-feature` command in the *Commands Manual*.

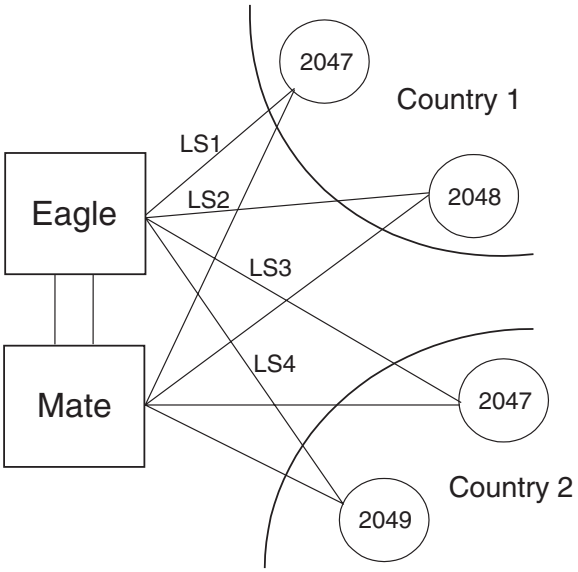
The EPAP feature allows group codes to be entered for a network entity (that is, SP or RN) point codes via the PDBI. The PDBI supports the provisioning of a two-character group code having a suffix to a point code of a PDBI network entity.

For example, a point code of 1-1-1 can be provisioned in the PDBI as **1-1-1-ab**, where **1-1-1** is the true point code and **ab** is the group code. This usage allows the EAGLE 5 ISS to discriminate between two nodes in different countries with the same true point code. The EAGLE 5 ISS uses the group code to distinguish

between the two nodes. The group code is used internally in the EAGLE 5 ISS only and is assigned to an incoming message based on the linkset on which it was received.

For example, Figure 2-3 shows a network that includes two countries, Country 1 and Country 2. Both countries have SSPs with a point code value of 2047.

Figure 2-3. Example of a Network with DPC and Group Codes



Users must divide their ITU-National destinations into groups. These groups are usually based on the country. However, one group could have multiple countries within it, or a single country could be divided into multiple groups. The requirements for these groups are:

- No duplicate point codes are allowed within a group.
- ITU-National traffic from a group must be destined for a PC within the same group.
- The user must assign a unique two-letter group code to each group.

For example, in the network shown in Figure 2-3, Country 1 can only have 1 point code with a value of 2047. Traffic coming from SSP 2047 in Country 1 can only be destined to other nodes within Country 1. In this example, the user assigns a group code of **`ab`** to Country 1, and a group code of **`cd`** to Country 2.

When the user enters an ITU-National point code, he or she must also enter the group code, using the format “point code - group code”. This group code must be used for any command that uses an ITU-N point code.

The ITU Duplicate Point Code Support feature for EPAP and PDBI allows group codes to be entered for a Network Entity (that is, SP or RN) point codes via PDBI commands. These commands are described in the *Provisioning Database Interface Manual*.

The PDBI supports the provisioning of a two-character group code suffixed to a point code of a PDBI Network Entity (NE). You can provision a group code to any valid NE, for example, RN or SP.

NOTE: The PDB does not check for uniqueness of point codes provisioned into the G-Flex, G-Port, EIR, or INP databases.

All routing for PDB-based features (that is, G-Port, G-Flex, EIR, and INP) specify group codes stored with the NE's point codes in accord with the EAGLE Duplicate Point Code feature.

NOTE: This should already be the case for the protocol side of these features, but you should system test it when provisioning to the PDB with group codes to ensure the group code is being used by the features for message relay.

For more about group codes, refer to "ITU Duplicate Point Code Routing" in both the *Provisioning Database Interface Manual* and the *Previously Released Features* manual.

Asynchronous Replication

Asynchronous replication is the method used to synchronize the various PDB databases in a client network. Asynchronous replication means the active PDB database receives an update, commits to accept the change, returns to the client a code indicating success or failure. This series occurs before the active PDB forwards the update to the replicated database, in this case the standby PDB.

Only successful updates are replicated. As a result, the response turnaround on the Active PDB is shortened, and the overhead involved in keeping the databases in sync is reduced.

Potential Lag Introduced by Asynchronous Replication

A potential exists under any asynchronous data replication scheme that the receivers of replicated data may lag behind. In this case, the standby PDB and, depending upon the homing policy in effect, the RTDB applications are susceptible to lag. Here, 'lag' denotes how the database level of the standby PDB is lower than the database level of the active PDB.

It is reasonable to expect that, during continual provisioning traffic, the active PDB will be a small number of levels ahead of the standby PDB. Likewise, any RTDB that is homed to the standby PDB can be expected to have a level lower than the active PDB. For more information, refer to "Selective Homing of EPAP RTDBs" on page 2-19.

Asynchronous Replication Alarms

The amount of lag in database levels between PDBs that EPAP accepts is an internal value. If the replication lag between PDBs rises to an unacceptable level, alarms are raised.

The alarms to announce lags in the database replication are:

- PDBA Replication Failure, a major alarm, indicates a failure of PDBA replication. The user should call Tekelec customer support; refer to "Customer Assistance" on page 1-4.
- Standby PDBA Falling Behind, a minor alarm, does not indicate data loss or corruption. This alarm condition signals that one EAGLE 5 ISS of the pair may have received updates at a longer interval than the other EAGLE 5 ISS.

EPAP Security Enhancements

The EPAP Security Enhancements feature controls access to an EPAP GUI to specific IP addresses. The specified allowed IP addresses are kept in an EPAP 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 EPAP.

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 EPAP GUI (refer to "Authorized IPs" on page 3-155). The IP mechanism implemented in this feature provides the user a means of further enhancing EPAP privilege control.

The EPAP Security Enhancements feature is available through the EPAP 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 EPAP 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.

EPAP 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 EPAP GUI. Attempts from any unauthorized address are rejected.

NOTE: No IP addresses are restricted from accessing the EPAP 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 EPAP GUI.

EPAP 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 EPAP 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 EPAP GUI (described in Chapter 3), but not from the EPAP text-based UI (described in Chapter 5).

Backup Provisioning Network Interface

The Backup Provisioning Network Interface feature adds an alternative connection for redundancy between the EPAP A server and the customer's PDBI. This additional interface provides a backup path for the PDBI to continue communicating with the EPAP A if the primary connection is lost.

A PDBI client normally uses port **`eth0`** on the active EPAP to provision the PDB (using the Configure Provisioning Network option 1 of the Configure Network Interfaces Menu). If a failure occurs in the normal connection, the Backup Provisioning Network Interface feature allows the customer to use secondary port **`eth4`** (using option 4 of the Configure Network Interfaces Menu). No automatic switchover occurs. The customer simply observes the communications failure, and then begins addressing the secondary port defined by the configuration procedure.

The Configure Network Interfaces Menu in Chapter 5, *"EPAP Software Configuration,"* describes how to configure the primary and secondary provisioning network interface connections. For more about this feature, refer to:

- "Configure Backup Provisioning Network" on page 5-23 for an description of the configuration option.
- Step 16 on page 5-44 for the configuration step that defines the address for the Backup Provisioning Network.

Provisioning Multiple EPAPs Support

The Provisioning Multiple EPAPs Support feature provides the ability for a single PDBI connection to provision up to four MPSs (each of which contains an EPAP A and B). The PDBI connects to and provisions an EPAP A / PDB, and then the

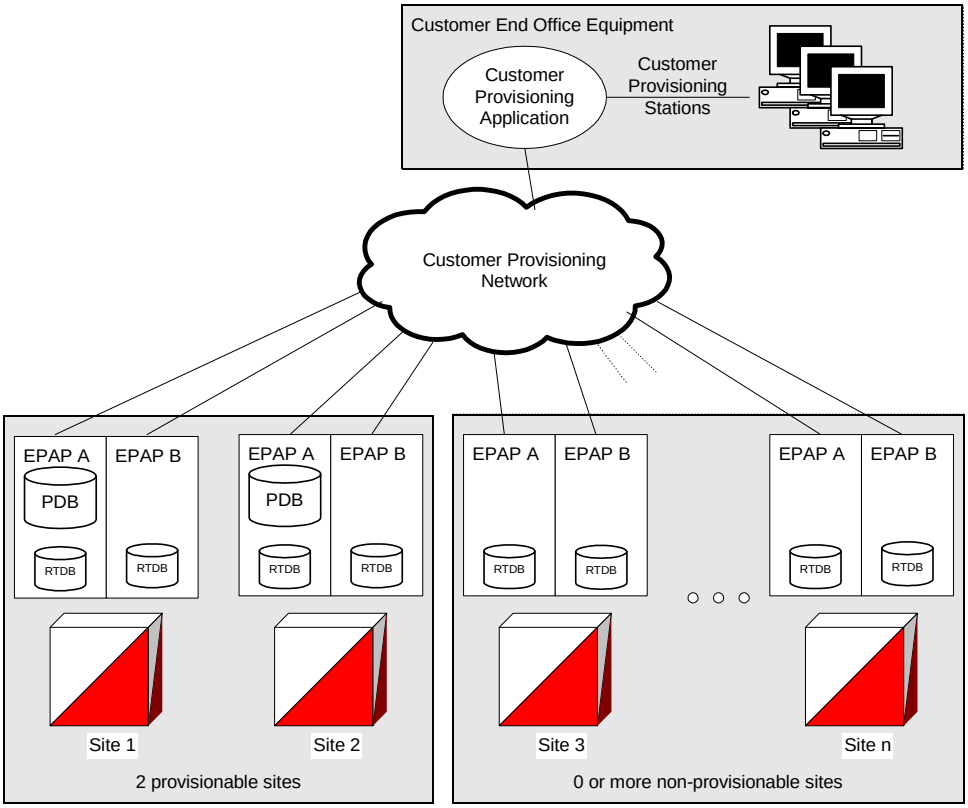
remaining three MPSs are automatically provisioned from the active EPAP A. This means the user can add more EAGLE 5 ISS without having to change their provisioning system or without having to provision them from multiple sources.

This feature allows users to add more MPSs without having to change their provisioning system or to provision from multiple sources. This feature is transparent to the PDBI clients. Clients can provision their data in the same manner regardless of whether they are provisioning a single MPS pair or multiple MPS pairs. The provisioning client connects to one PDB for provisioning. The remaining MPSs in the customer network automatically remain in sync.

This feature does not affect which PDBA the RTDBs connect to for receiving updates. Receiving updates continues to be under the control of the EPAP user interface.

With the Provisioning Multiple EPAPs Support feature, customers can add EAGLE 5 ISS to their network without changing the way they provision data. EPAP software updates the real-time databases at the additional sites. The two MPSs that contain the PDB are called “provisionable” because the customer provisioning application connects to and updates these sites; remaining MPSs are called “non-provisionable.” See Figure 2-4 for a view of the provisionable and non-provisionable EPAPs.

Figure 2-4. Support for Provisioning Multiple EPAPs



Selective Homing of EPAP RTDBs

The Selective Homing of EPAP RTDBs feature allows users to select the PDB from which they receive updates. The homing selection is an option at EPAP configuration. Users can choose whether the RTDBs on a given MPS node receive updates by either:

- The IP address, a specific PDBA process (which may be active or standby) or
- The PDB state, the active or standby PDBA process (which may or may not be local).

The terminology 'specific PDBA' is used instead of 'local PDBA' because the architecture can result in an MPS without a PDB on EPAP A. In this case, the RTDBs on that node have no 'local PDBA.' Selective homing specifies the IP addresses of the MPSs with the first and second choices of PDBA. Of course, in a two-node MPS system, this corresponds directly to 'local' homing, but with more than two nodes, the user selects a specific PDBA without designating it as 'local' or 'remote.'

The terminology 'active PDBA' refers to the PDBA selected by the user to receive updates from the user's provisioning system via the PDBI.

This feature permits all RTDBs within an MPS system (both nodes of a mated pair or multiple nodes within several mated pairs) to always receive updates from a specific PDB, or from the active or standby PDB. Updates would always be received from the selected PDBA process, irrespective of whether it is the local or remote PDBA.

An EPAP configuration option allows the user to select whether that EPAP's RTDB will normally receive updates (i.e., to be "homed" to a specific PDBA or the active or standby PDBA.) If the user selects specific homing for the RTDB, that RTDB will receive updates from the specified PDBA, regardless of whether it is active or standby.

If the RTDB cannot communicate with the specified PDBA, it will automatically begin to receive updates from its alternate PDBA. (Previously, updates were received from the remote PDBA.)

NOTE: For a given RTDB, the "remote" PDBA is a PDBA on a different MPS node. This also may or may not be the "active" PDBA.

If the user selects 'active' homing for the RTDB, that RTDB will always receive updates from the active PDBA. If the RTDB loses its connection with the active PDBA, it will automatically begin to receive updates from a 'standby' PDBA; the reverse is true for 'standby' homing. This automatic switchover is a configurable option. See "Switchover PDBA Status" on page 3-67.

The homing of each RTDB is independently selectable and allows some RTDBs to be homed to their local PDBA, to the active PDBA, or to the standby PDBA.

The PDB selected by the RTDB is known as the 'preferred PDB.' The RTDB is 'homed' to that PDB. The PDB not selected is called the 'alternate PDB.' When either active or standby PDB homing is selected, the RTDB has the option to receive updates from the alternate PDB if the preferred PDB is unreachable. (For more about standby PDB homing, see "Asynchronous Replication Serviceability Considerations" on page 2-24.) When specific RTDB homing has been selected, the RTDB will receive updates from the alternate PDB if the preferred PDB is unreachable.

These configurations of each RTDB in the system are possible:

- "Specific PDB Homing with Alternate PDB" on page 2-20
- "Active PDB Homing with Alternate PDB" on page 2-21
- "Active PDB Homing without Alternate PDB" on page 2-21
- "Standby PDB Homing with Alternate PDB" on page 2-22
- "Standby PDB Homing without Alternate PDB" on page 2-23

Specific PDB Homing with Alternate PDB

This RTDB configuration specifies the IP address of the PDB from which the RTDB will receive updates. In the event that the specified PDB is not reachable, the RTDB will receive updates from the alternate PDB. Table 2-3 shows the condition of each possible connection to the PDB from the RTDB point of view. The shaded boxes indicate the PDB from which the RTDB will receive updates.

Table 2-3. Specific PDB Homing with Alternate PDB (RTDB Configuration 1)

Site 1 PDB		Site 2 PDB		RTDB Data Source
Reachable?	**State**	**Reachable?**	**State**	
Yes	Active	Yes	Standby	Site 1 PDB
Yes	Standby	Yes	Active	Site 1 PDB
Yes	Active	No	-	Site 1 PDB
Yes	Standby	No	-	Site 1 PDB
No	-	Yes	Active	Site 2 PDB
No	-	Yes	Standby	Site 2 PDB
No	-	No	-	None

Note 1: Site 1 = Preferred PDB Site 2 = Alternate PDB

Note 2: Shaded boxes show which PDB the RTDB receives updates from

See "RTDB Homing Considerations" on page 2-24 to determine if this configuration is the most appropriate match for your installation.

Active PDB Homing with Alternate PDB

This RTDB configuration specifies the RTDB will receive updates from the active PDB. In the event that the active PDB is not reachable, the RTDB will receive updates from the standby PDB. Table 2-4 shows the condition of each possible connection to the PDB from the RTDB point of view. The shaded boxes indicate the PDB from which the RTDB will receive updates.

Table 2-4. Active PDB Homing with Alternate PDB (RTDB Configuration 2)

Site 1 PDB		Site 2 PDB		RTDB Data Source
Reachable?	**State**	**Reachable?**	**State**	
Yes	Active	Yes	Standby	Site 1 PDB
Yes	Standby	Yes	Active	Site 2 PDB
Yes	Active	No	-	Site 1 PDB
Yes	Standby	No	-	Site 1 PDB
No	-	Yes	Active	Site 2 PDB
No	-	Yes	Standby	Site 2 PDB
No	-	No	-	None

Note 1: Active = Preferred PDB Standby = Alternate PDB

Note 2: Shaded boxes show which PDB the RTDB receives updates from

See “RTDB Homing Considerations” on page 2-24 to determine if this configuration is the most appropriate match for your installation.

Active PDB Homing without Alternate PDB

This RTDB configuration specifies the RTDB will receive updates from the active PDB. No alternate PDB is specified. Table 2-5 shows the condition of each possible connection to the PDB from the RTDB point of view. The shaded boxes indicate the PDB from which the RTDB will receive updates.

Table 2-5. Active PDB Homing without Alternate PDB (RTDB Configuration 3)

Site 1 PDB		Site 2 PDB		RTDB Data Source
Reachable?	**State**	**Reachable?**	**State**	
Yes	Active	Yes	Standby	Site 1 PDB
Yes	Standby	Yes	Active	Site 2 PDB
Yes	Active	No	-	Site 1 PDB
Yes	Standby	No	-	None
No	-	Yes	Active	Site 2 PDB
No	-	Yes	Standby	None
No	-	No	-	None

Note 1: Active = Preferred PDB Standby = Alternate PDB

Note 2: Shaded boxes show which PDB the RTDB receives updates from

See "RTDB Homing Considerations" on page 2-24 to determine if this configuration is the most appropriate match for your installation.

Standby PDB Homing with Alternate PDB

This RTDB configuration specifies the RTDB will receive updates from the standby PDB. In the event that the standby PDB is not reachable, the RTDB will receive updates from the active PDB. Table 2-7 shows the condition of each possible connection to the PDB from the RTDB point of view. The shaded boxes indicate the PDB from which the RTDB will receive updates.

Table 2-6. Standby PDB Homing with Alternate PDB (RTDB Configuration 4)

Site 1 PDB		Site 2 PDB		RTDB Data Source
Reachable?	**State**	**Reachable?**	**State**	
Yes	Standby	Yes	Active	Site 1 PDB
Yes	Active	Yes	Standby	Site 2 PDB
Yes	Standby	No	-	Site 1 PDB
Yes	Active	No	-	Site 1 PDB
No	-	Yes	Standby	Site 2 PDB
No	-	Yes	Active	Site 2 PDB
No	-	No	-	None

Note 1: Standby = Preferred PDB Active = Alternate PDB

Note 2: Shaded boxes show which PDB the RTDB receives updates from

See "Asynchronous Replication Serviceability Considerations" on page 2-24 to determine if this configuration is the most appropriate match for your installation.

Standby PDB Homing without Alternate PDB

This RTDB configuration specifies the RTDB will receive updates from the standby PDB. No alternate PDB is specified. Table 2-7 shows the condition of each possible connection to the PDB from the RTDB point of view. The shaded boxes indicate the PDB from which the RTDB will receive updates.

Table 2-7. Standby PDB Homing without Alternate PDB (RTDB Configuration 5)

Site 1 PDB		Site 2 PDB		RTDB Data Source
Reachable?	**State**	**Reachable?**	**State**	
Yes	Standby	Yes	Active	Site 1 PDB
Yes	Active	Yes	Standby	Site 2 PDB
Yes	Standby	No	-	Site 1 PDB
Yes	Active	No	-	None
No	-	Yes	Standby	Site 2 PDB
No	-	Yes	Active	None
No	-	No	-	None

Note 1: Standby = Preferred PDB Active = Alternate PDB

Note 2: Shaded boxes show which PDB the RTDB receives updates from

See "Asynchronous Replication Serviceability Considerations" on page 2-24 to determine if this configuration is the most appropriate match for your installation.

General Homing Considerations

The Selective Homing of EPAP RTDBs feature requires additional configuration at installation and when new non-provisionable nodes are added. The configuration of all affected sites must be planned before they are being installed.

Each MPS must be configured as provisionable or non-provisionable. There must be exactly two provisionable MPSs. (See Figure 2-4, on page 2-18.) These MPSs must then be configured with a replicated PDB, which is described in Chapter 5, *"EPAP Software Configuration"*. If used, non-provisionable MPSs are added after the provisionable MPSs are installed and configured.

Before the first MPS can be installed, this information must be known:

- How many MPSs are involved?
- Which sites will be provisionable?
- How will each RTDB be homed?

For the configuration on each site, this information must be available:

- What are the IP addresses of the A sides of the two provisionable sites?
- What is the RTDB homing policy for this site?

RTDB Homing Considerations

Although RTDB homing allows a wide variety of configurations, two overall configurations cover the needs of most customers.

1. Configuration for Load Sharing and High Availability

In this configuration, all RTDBs are configured for specific RTDB homing. The alternate PDB is an acceptable provisioning source in the case where the preferred PDB is unavailable. The RTDBs at the provisionable MPS prefer the local PDB. The remaining non-provisionable MPSs should be divided evenly to prefer one PDB or the other. See “Specific PDB Homing with Alternate PDB” on page 2-20 for more information on this RTDB Homing configuration.

2. Configuration for Deterministic Provisioning

In this configuration, all RTDBs are configured for active homing. The alternate PDB is not an acceptable provisioning source. See “Active PDB Homing without Alternate PDB” on page 2-21 for more information about this RTDB homing configuration.

Asynchronous Replication Serviceability Considerations

The type of RTDB homing policy selected can affect serviceability by the user. We recommend for asynchronous PDB replication using Standby PDB Homing (RTDB configuration 4 or 5). Though this policy means that the time for updates to propagate from the PDB to the RTDB may be slightly greater, this delay is actually beneficial in disaster recovery situations.

Keeping the RTDB homed to the standby PDB ensures that, apart from external intervention, every level present in the RTDB is also present in both PDBs. Both active and specific RTDB homing methods will continue to be valid; they will provide proper function under every normal operating circumstance. It is possible under these homing policies, however, for the RTDB to reach a database level that is higher than the PDB to which it may home to in response to a PDBA switchover. If this occurs, the RTDB must be recreated from the PDB it currently points to.

Active and specific homing complicate things in disaster situations. For instance, if a failure forces the active PDB to become unavailable for a non-trivial amount of time and the user forces switchover to Standby (bypassing the protocol that syncs the databases prior to switchover), it is possible for the dataset of the RTDB to conflict with the dataset of the only remaining PDB. This situation would necessitate a RTDB reload from the remaining PDB, which can be a time-consuming process for any PDB having a large amount of data.

Asynchronous replication makes one important change in EPAP behavior. PDBA switchover can no longer be forced when the PDBAs are able to communicate and the standby is not current. Switchover now involves allowing some definable amount of time for the standby PDB to be brought up to the level of the active PDB.

If the standby PDB fails to achieve the equal database level in the allotted time, switchover does not occur, and the standby PDB returns with the number of levels still remaining to be replicated. This design is a safeguard to prevent database inconsistency. However, if the standby PDB cannot reach the active PDB to determine its level, the EPAP does allow PDBA switchover to be forced.

Socket-Based Connections

The EPAP receives PDBI messages through a TCP/IP socket. The client application is responsible for connecting to the PDBA well-known port and being able to send and receive the defined messages. It is also the responsibility of the customer's provisioning system to detect and deal with socket errors. Tekelec recommends that the TCP 'keep alive' interval on the customer's socket connection be set such that a socket disconnection problem is promptly detected and reported.

There is a limit to the number of PDBI connections; the default is 16 clients. If an attempt is made to connect more than the current client limit, a response is returned to the client: PDBI_TOO_MANY_CONNECTIONS. After the response is returned, the socket is automatically closed.

NOTE: Although the default limit is 16 PDBI connections, Tekelec is able to configure and support up to 128 connections. If more than 16 concurrent client connections are required, contact Tekelec for information.

File Transfer Options

Import Files

The manual import and automatic import are the available import file options. Both import options will only accept data in the PDBI format.

Valid commands to include in an import file are:

- **ent_sub**
- **upd_sub**
- **dlt_sub**
- **ent_entity**
- **upd_entity**
- **dlt_entity**
- **ent_eir**
- **upd_eir**
- **dlt_eir**

NOTE: Do not include rtrv_sub, rtrv-entity, or rtrv_eir commands in an import file. The inclusion of rtrv commands causes an import to take a very long time to complete. During an import, a write transaction lock is in place for the entire import for a manual import, and intermittently in place for an automatic import. While the write transaction lock is in place during an import, no other updates to the database can be made.

Manual Import

The manual import mode is used to import data typically on a one-time basis or as needed and is configured by the Import File to PDB Screen. The selected file is processed immediately. A manual import locks the PDB write transaction; other users will not be able to obtain the write transaction until the import operation is complete.

Automatic Import File Set-up

As long as the PDB is active, the automatic import searches the */var/TKLC/epap/free/pdbi_import* directory for new files on a remote system for import every 5 minutes. If a file exists in the directory and it is not being modified or in the process of being transferred when it is polled, the import will run automatically at that time. If the file is being modified or is in the process of being transferred, the automatic import tries again after five minutes. Delaying when a file is being modified or in the process of being transferred prevents the import of incomplete files.

The automatic import option can import up to 16 files at a time. This is limited by the available number of PDBI connections. If more than 16 files exist in the directory, as soon as one file completes, another file is started until all files have completed the files are imported sequentially. The results of the import are automatically exported to the remote system specified by the Configure File Transfer Screen.

Once the import is complete, the data file is automatically removed and a results file is automatically transferred back to the remote system.

An automatic import obtains the PDB write transaction and processes 10 of the import file commands. Then the write transaction is released, allowing other connections to provision data. An automatic import obtains the write transaction repeatedly until all the import file commands have been processed.

Automatic Import Status

When using the automatic import function, the following informational banner messages will appear on the UI browser screen in the Message Box described in Figure 3-13.

`Import of <filename> in progress - xx.xx%`	(while in-progress)
`Import of <filename> completed`	(when complete)

If the import fails for any reason the following informational banner message will appear on the UI browser screen in the Message Box described in Figure 3-13.

```
Import of <filename> failed - no PDBA
```

In the event of an automatic import failure, an automatic retry will occur every 5 minutes.

Export Files

The manual export and automatic export are the available export file options. Data can be exported in both the PDBI and CSV formats. Refer to the *Provisioning Database Interface Manual* for more information.

The Manual File Export allows data to be exported to a specified location on a one-time basis, or as needed, and is configured by the Export PDB to File Screen.

Automatic File Export

The Automatic File Export function allows the scheduling of the data export at a specific day and time. The export can be scheduled at a specific time for each of the following repeat periods: every N number of days (N can be up to 365), on specified days of the week, on a specified day of the month, or on a specified day of the year.The Schedule Export screen is used to display any existing PDB export tasks and to create a task by specifying the data type, the export format (PDBI or CSV), the export mode (blocking, snapshot, or real-time) as well as the time and repeat period. In addition, a Comment field is available to describe the task.

The PDBA must be active at the scheduled time of export for the file to be exported.

Automatic PDB/RTDB Backup

The Automatic PDB/RTDB Backup is used to backup all data stored in the PDB/RTDB, including G-Port, G-Flex, INP, and EIR data. The Automatic PDB/RTDB Backup feature automates the process of creating backups of the PDB and RTDB databases at the time, frequency, and to the destination configured by the user. The PDB database backup is created on EPAP A and RTDB database backup is created on the standby EPAP (A or B). Approximately 17 GB of disk storage space is required per backup.

The following options are available for configuring a destination for the backup file:

- Local (data is saved to the local disk on the same EPAP server as the PDB/RTDB being backed up).
- Mate (data is created on the local server and then sent via SCP to the mate EPAP server).
- Remote (data file is created on the local EPAP server and then sent via SFTP to a remote server configured by the user. SFTP must be installed at this remote server. This server may or may not run EPAP software and can be any machine on the network).

In the case of mate and remote backup destinations, the option exists to save a copy of the backup to the local drive. For these two options, even if the user has selected the option not to save the local copy, it will be saved if the transfer of file fails after the backup has been created on the local machine.

Both the PDB and RTDB backups are scheduled together but execute separately. Based on the input parameters, RTDB backup will always start 1 hour ahead of the PDB backup. The time selected when setting up the feature determines the time the RTDB backup starts. PDB backup will start 1 hour later.

There is no link between backups of one MPS system with backup of the other MPS system. Backups can only be scheduled and created on provisionable pairs. PDB/RTDB Automatic Backup is not allowed and cannot be scheduled on a non-provisionable pair.

Normal provisioning is allowed during the PDB/RTDB Automatic Backup. This includes provisioning from the customer network to the PDB, provisioning from the PDB to the active EPAP RTDB, and provisioning from the active EPAP RTDB to the DSM RTDB. RTDB backups are always created from the standby EPAP RTDB (A or B).

If there are backup failures, alarms and error messages are generated and logged. There are 2 kinds of backup failures:

- **Backup operation failures:** This is the failure to create backup files on either of the machines - local or mate. There are possibly 2 alarms in this case - one for the PDB and one for the RTDB.
- **Backup transfer failures**: This is the failure to transfer a backup file to the mate or remote site. In this case, backup files exist on the local machine. There is the possibility of 2 alarms in this case - one for the PDB and one for the RTDB.

There is the possibility of a delay of up to 5 minutes after the scheduled time before the actual start of the scheduled backup.

The effects of cancelling a backup midstream follow:

- If the automatic backup is in progress (RTDB backup has started), it will complete and the PDB backup will not start.
- If the RTDB backup has completed but the PDB has not started (It is delayed by one hour form the RTDB backup). The PDB backup will not start.
- If the RTDB backup has completed and the PDB has started (It is delayed by one hour form the RTDB backup), it will also complete.

This feature is supported and configured by using the web-based GUI. Refer to "Automatic PDB/RTDB Backup" on page 3-31 for details on setting-up the Automatic PDB/RTDB Backup feature.

EPAP Automated Database Recovery

The EPAP Automated Database Recovery (ADR) feature is used to restore the EPAP system function and facilitate the reconciliation of PDB data following the failure of the Active PDBA.

The automated recovery mechanism provided by this feature allows 1 PDBA to become Active when 2 PDBAs think they are active and have updates that have not been replicated to the mate PDBA. The software selects the PDBA that received the most recent update from it's mate to become the Active PDBA (the PDBA that was the Standby most recently will become the Active). No automatic reconciliation is performed because the system has insufficient information to ensure that the correct actions are taken.

In order to return the system to normal functionality, a manual PDB copy from the PDBA the software picked to be Active to the PDBA that is in the replication error (ReplErr) state must be performed. However, provisioning can resume until a maintenance period is available to do this.

It is **STRONGLY RECOMMENDED** that the Customer Care Center be contacted before performing the PDBA Copy procedure

This feature uses a replication error list that consists of updates that exist as a result of a failure during the database replication process from the active-to-standby PDB. These updates have not been propagated (reconciled) throughout the system and require manual intervention to ensure the EPAP systems properly process the updates.

Example EPAP Automated Database Reconciliation

Starting with PDBAs in the following current configuration.

Updates 701, 702, and 703 on Node 1 have not been replicated to Node 2.

Active PDBA (Node 1)	Standby PDBA (Node 2)
DB Level-704	DB Level-700
Updates to replicate to standby PDBA	
701	
702	
703	

Now assume there is a fault that takes down the Node 1 PDBA before the replication process is complete. Node 2 has become the Active PDBA and is now receiving provisioning updates.

Failed PDBA (Node 1)	Active PDBA (Node 2)
DB Level-704	DB Level-700
Updates on replication error list	Processing DB Level updates
701	701 (different than 701 on node 1)
702	702 (different than 702 on node 1)
703	703 (different than 703 on node 1)

- Updates 701-703 on Node 1 have not been replicated to Node 2 and,
- Updates 701-703 on Node 1 are different from updates 701-703 on Node 2.

The PDBA that took an update with the latest timestamp (in this example the Node 2 PDBA) will automatically become the Active PDBA and continue taking provisioning updates. The Node 1 PDBA is put in a "REPL_ERR" state and "PDBA Replication Failure" alarm initiates on this PDBA.

A replerr file (REPL_ERR PDBA) with the replication log lists from the Node 1 PDBA is created. This file contains the lost Node 1 provisioning updates (701-703) and is in the format of a PDBI import file. The customer can examine the file and decide whether he wants to reapply these updates to the Active PDBA.

Anytime after the Node 1 PDBA becomes available, the customer will have to temporarily suspend provisioning and perform a PDB copy of the Node 2 PDBA to the Node PDBA to reconcile the PDBs before the Node 1 PDBA can be made active again.

This feature is enabled through the text-based EPAP user interface.

EPAP PDBA Proxy Feature

The EPAP PDBA Proxy feature provides a more reliable connection to the EPAP PDBA in the event of a failure of the active PDBA. Connection redundancy is accomplished by allowing the customer's provisioning system to still use a single IP address, even though the connection may logically be to the previously standby PDB.

During normal provisioning operations, one PDBA is active and the other PDBA is in standby. However, from the customer's provisioning system perspective, the active and standby PDBAs are accessible through a single IP address. If the active PDBA fails, the local EPAP B box will forward provisioning updates to the mated PDB.

When the previously active PDBA recovers, it is aware that the standby PDBA has become active and now both active PDBAs need to be reconciled.

The advantages this feature provides are:

1. The customer's EPAP network can absorb a single EPAP failure and automatically transfer provisioning to the standby PDBA using the same IP address.

2. A means of reconciling both active PDBAs when the failed PDBA becomes available again.

Example EPAP PDBA Proxy

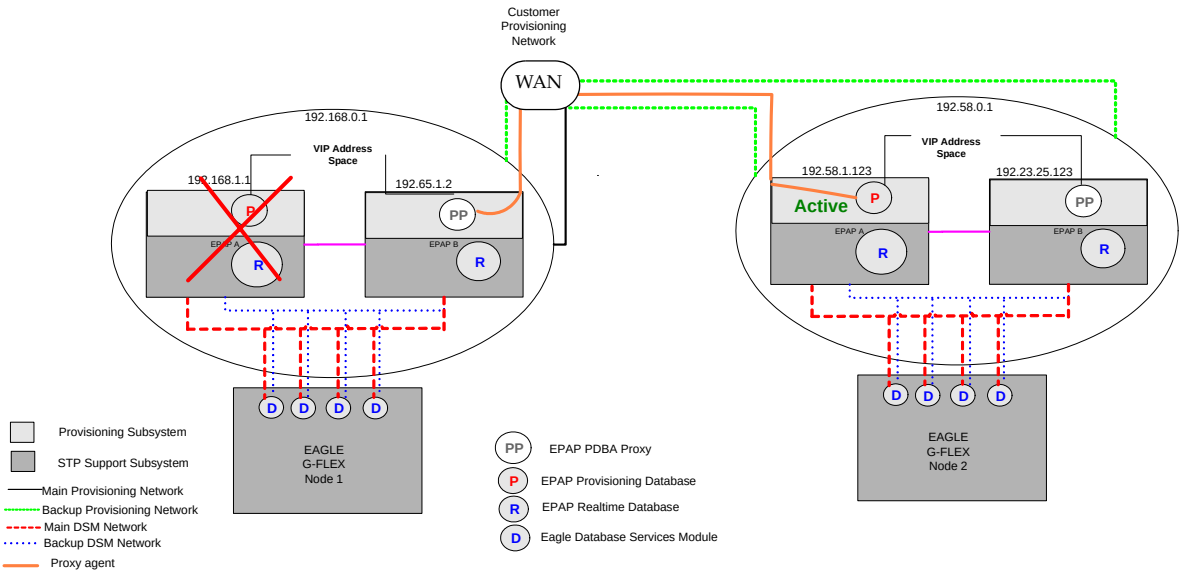
During normal provisioning operations, the flow of information is as follows:

- The customer's provisioning system sends provisioning updates to the Active PDBA on Node 1.
- The Active PDBA checks syntax and writes to the Active PDB.
- The Active PDBA writes to a replication log on the EPAP A and mate EPAP B.
- The Active PDBA sends an ACK response to the customer's provisioning system.
- The Standby PDBA on Node 2 queries the EPAP A replication logs and updates the PDB on Node 2.

In the event of a fault (e.g. server failure) on the Node 1 PDBA as shown in Figure 2-5.

- If the Standby PDBA on Node 2 is reachable, the EPAP B machine on Node 1 will forward any replication logs to the Node 2 PDBA.
- When the Node 2 PDBA has all the replication logs from the EPAP B machine, on Node 1, it now becomes the Active by proxy PDBA.
- The customer's provisioning system can continue provisioning because the EPAP B will be using the proxy to forward the updates to the newly Active PDBA on Node 2.

Figure 2-5. Virtual IP-Failure of Active PDBA



When the Node 1 PDBA is restored to service,

- Any updates that were sent to the Node 2 PDBA while the Node 1 PDBA was down, are forwarded to the Node 1 PDB.
- When all the records are replicated, the Node 1 can become the Active PDBA, and Node 2 reverts back to being the Standby PDBA.

This feature is enabled through the text-based EPAP user interface.

Allow Write Commands on EPAP During Retrieve/Export Feature

This feature allows an EPAP user to provision data via the GUI or PDBI while simultaneously performing a data export via the GUI or PDBI. There are three modes of operation:

1. Blocking mode - Blocks all write requests while an export is in progress.

2. Snapshot mode - Allows writes to continue during the export, and provides the export as a complete snapshot of the database at the time the export started. (Changes made to the DB after export has started are not reflected in the export file.) This mode provides a file that would be most applicable for importing back into the database later.

3. Real time mode - Allows writes to continue during export, but provides the export file in real-time fashion rather than as a snapshot. (Changes to the DB after the export has started may or may not be reflected in the export file, depending whether the changes are to an area of the DB that has already been exported.) This mode also provides a file that could be imported back into the database later, but is less than ideal, since it is not a complete snapshot of a given time.

EPAP 30-Day Storage or Export of Provisioning Logs Feature

This feature will allow the EPAP to store provisioning logs on the EPAP hard drive for a configurable amount of time (up to 30 days), provided the disk partition does not become full within that time. The maximum value selectable is 30 days. If the user does not select a specific value, the default is 1 day.

This feature will also allow configuration of storage time for error logs and debug logs. Error logs are configurable from 1 to 30 days with 1 day as the default. Debug logs are configurable from 1 to 7 days, with 1 day as the default.

Alarms will notify the user when the log drive is 80% or 90% full.

1. If the disk where the logs are stored becomes 80% full before the configured time period has elapsed, the EPAP will issue a minor alarm. No files will be pruned at this point.

2. If the disk where the logs are stored becomes 90% full before the configured time period has elapsed, the EPAP will issue a major alarm. No files will be pruned at this point.

3. If the disk where the logs are stored becomes 95% full before the configured time period has elapsed, the EPAP will issue a major alarm. The EPAP will begin pruning the oldest entries in the log to make room for new entries.

4. The alarms are cleared when the disk space in use decreases to less than 80% or 90% respectively.

NOTE: The 80% and 90% alarms do not coexist. If the 80% alarm is active when the 90% alarm is triggered, it is replaced by the 90% alarm until that alarm clears. Then the 80% alarm remains on till it too clears.

1100 TPS/DSM for ITU NP Feature

This feature for EAGLE 5 ISS systems that support G-Flex and G-Port expands the TPS capacity of each DSM card from the current 850 to 1100 per card. The maximum capacity per DSM is 1700 tps for non-G-Port/G-Flex features. Increasing the TPS of the cards moves the maximum capacity of 25 DSM cards from 20,400 to 26,400 TPS.

EPAP Support for SSH on PDBI

The EPAP Support for SSH on PDBI feature provides support for Secure Shell (SSH) on the EPAP Provisioning Database Interface (PDBI) for customers who want additional security protection.

Automatic PDB Export Enhancement

The Automatic PDB Export Enhancement feature provides more flexible scheduling for automatic PDBA exports. Scheduling an automatic PDBA export is very similar to the way tasks or appointments can be scheduled in a calendar manager.

EPAP Support for HTTPS on GUI

The EPAP Support for HTTPS on GUI feature allows the user to choose whether the connection from the web server to the EPAP GUI supports only standard HTTP (Hypertext Transfer Protocol), only secure HTTP (HTTPS), or both.

In standard HTTP protocol, the data transfer between the web server and the GUI is not encrypted. Therefore, it can be captured and viewed by any network analyzer with access to the TCP/IP connection.

Secure HTTP (HTTPS) supports encryption of the data exchanged between the web server and the browser to facilitate data privacy.

Support Java 1.5 on EPAP

The EPAP GUI requires Java 1.5 or later.

RTDB Retrieve

The RTDB Retrieve feature allows the user to query (from the web GUI) data that resides in the RTDB (Real-Time Database). This feature enables the user to compare data in the PDB (Provisioning Database) with data in the RTDB to verify that they are consistent. This feature also enables the user to compare data in the RTDB with data on the DSM card in the EAGLE 5 ISS (using the **rtrv-data-rtdb** command on the EAGLE 5 ISS).

The ability to retrieve RTDB data assists in troubleshooting cases where data is absent on EAGLE 5 ISS, but present in the PDB.

Data returned from RTDB is presented on the EPAP GUI in a format that is similar to data from the PDB. This similarity makes it easier to compare data between the two databases when a discrepancy is suspected.

The comparisons can indicate data that exists in one database but not in another, or data that is different between the databases. The user must determine which database has the correct data.

The PDB is considered the master database. Therefore, if one or both RTDBs has different data, extra data, or absent data, the RTDB is usually considered to be wrong .If a discrepancy is found, check the levels of the RTDB and PDB. In general, the PDB and RTDB data should not be different unless the levels of the RTDB are far behind the PDB level and data has been changed during the interval. If the RTDB and PDB levels are the same and the data is still different, contact the Customer Care Center (see page 1-4).

EPAP User Interface Menus

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

Chapter 3, *"EPAP Graphical User Interface,"* describes EPAP operations, that is, how to log into the interface, how to use the GUI menu items, and any associated output for each menu item.

Chapter 5, *"EPAP Software Configuration,"* describes the text-based user interface that provides the EPAP Configuration menu to perform the initial configuration.

DSM Provisioning

One of the core functions of the EPAP is to provision the DSM cards with database updates.

The DSM provisioning task resides on both EPAP A and EPAP B. It communicates internally with the real-time database (RTDB) task, and the EPAP maintenance task. The DSM provisioning task broadcasts provisioning data to connected DSM

cards across two Ethernet networks (see "Network Connections" on page 2-9). The DSM provisioning network architecture is shown in Figure 2-6 and the DSM provisioning task interface is shown in Figure 2-7.

Figure 2-6. DSM Provisioning Network Architecture

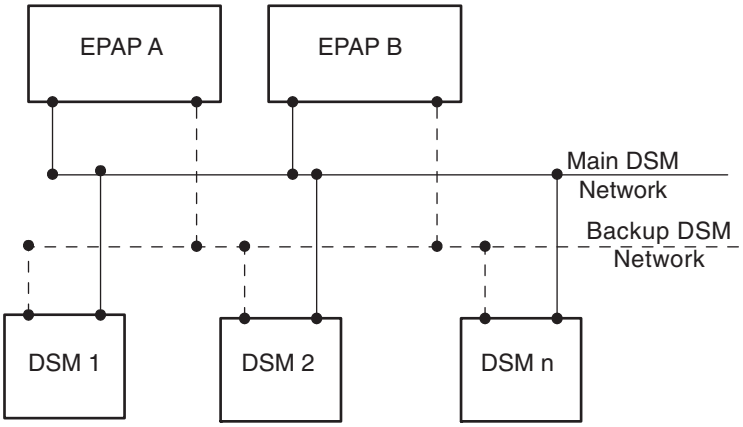
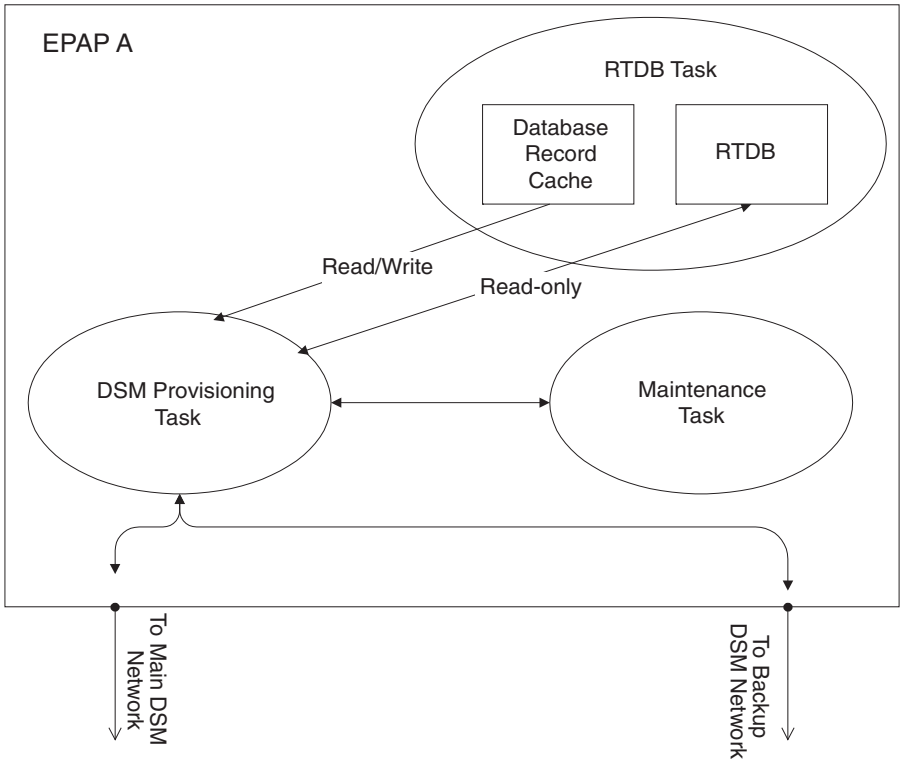


Figure 2-7. DSM Provisioning Task Interfaces



In order to handle the redundancy requirements for this feature, a separate RMTP channel is created on each interface from each EPAP:

- EPAP A, Main DSM network
- EPAP A, Backup DSM network
- EPAP B, Main DSM network
- EPAP B, Backup DSM network

Provisioning and other data is broadcast on one of these channels to all of the DSM cards. Provisioning is done by database level in order to leave DSM tables coherent between updates.

In addition to a constant stream of current updates, it is necessary to provision back-level DSM cards with incremental update streams that use the same delivery mechanism as the current provisioning stream.

Provisioning Model

For the purpose of this discussion, provisioning originates from the PDB task in coordination with the RTDB task. At initiation, the provisioning task initiates a session with the RTDB using a null database level. The RTDB initializes the session using the actual current database level. At regular 1.5 second intervals, the provisioning task sends a data request to the RTDB. The RTDB responds even if the no new data is available. The provisioning task sends a provisioning message on the DSM network.

Incremental Loading Model

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

The DSM detects that the current database level is higher than the update it expected, and indicates its current DB level to the maintenance task. The maintenance task requests that the DSM provisioning task begin a new incremental loading stream at the requested DSM level.

Once an incremental loading stream is set up, the following incremental loading transaction is repeated until the DSMs reach the current RTDB level:

The DSM provisioning task requests records associated with the database level for this stream. The RTDB task returns records associated with that level and sequentially higher levels (up to the maximum message size or the current RTDB level). The DSM provisioning task provisions the DSMs with the records.

NOTE: Incremental loading and normal provisioning are done in parallel. The DSM 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. DSM cards accept *any* stream with the "next" sequential database level for that card.

DSM Reload

The stages of database reload for a given DSM are given the following terminology:

Stage 1 loading - The database is being copied record for record from the Active EPAP to the DSM RTDB. The database is incoherent during stage 1 loading.

Incremental update – The database is receiving all of the updates missed during stage 1 loading or some other reason (such as network outage, processor limitation, or lost communication). The database is coherent but back level during incremental update.

Current – The database is receiving current updates from the DSM provisioning task.

Coherent – The database is at a whole database level; it is not currently updating records belonging to a database level.

DSM cards may require a complete database reload in the event of reboot or loss of connectivity for a significant amount of time. The EPAP provides a mechanism to quickly load a number of DSM cards with the current database. The database on the EPAP is large and may be updated constantly. The database sent to the DSM card or cards will likely be missing some of these 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 one to send all of the updates missed since the beginning of the first stage.

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

Continuous Reload

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

DSM Database Levels and Reloading

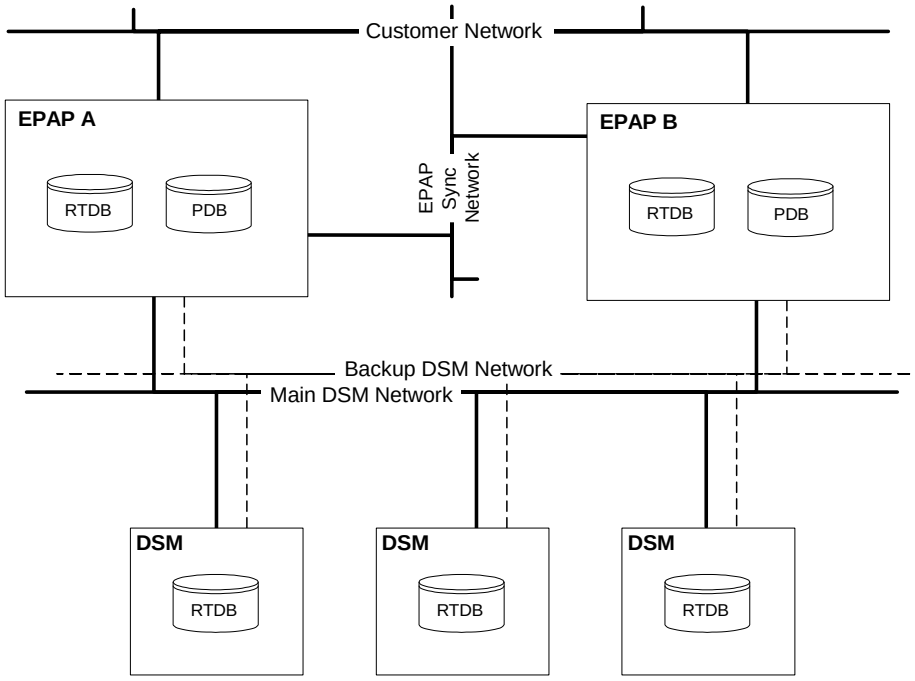
The current database level when the reload started is of special importance during reload. When a DSM detects that the last record has been received, it sends a status message back to the EPAP indicating the database level at the start of reload. This action will start incremental loading. The DSM cannot, however, use the database until the DB level reaches the database level at the end of reload. As real-time database records are sent to the DSMs during reload, normal provisioning can change those records. All of the records affected between the start and end of reloading must be incrementally loaded before the database is coherent.

MPS/DSM RTDB Audit Overview

General Description

The fact that the EPAP advanced services use several databases, some of which are located on different platforms, 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 Provisioning Database (PDB) and Real-time DSM databases (RTDB). The active EPAP machine validates the database levels for each of the DSM cards. Refer to Figure 2-8 for the MPS hardware interconnection diagram.

Figure 2-8. MPS Hardware Interconnection



Functional Description

MPS RTDB Audit

This audit maintains 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" on page 3-24).

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 PDB is halted until the condition is corrected via RTDB Reload

EPAP-to-DSM Network Card DB Level

Each DSM card validates its own database level against the received EPAP database level. An inconsistent alarm is generated at the EAGLE 5 ISS for every inconsistent DSM card. The command **rept-stat-db** displays the G-Port/G-Flex/EIR/INP database on the DSM card as *Diff* level. See Table 2-8.

Table 2-8. 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 (Table 2-9) 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 2-9. 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 2-10. 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 EPAPs have no direct means of displaying output messages on EAGLE 5 ISS terminals. Maintenance, measurements, status, and alarm information are routed from the Active EPAP to an arbitrarily selected DSM card, known as the primary DSM. Static information is exchanged across this interface at initialization and dynamic information is exchanged on occurrence.

While much of the traditional OAM provisioning and database function is implemented on the EPAP, the maintenance reporting mechanism is still the OAM. The maintenance commands and alarms available from the OAM are described in Chapter 4, *"Messages, Alarms, and Status Reporting."*

The EPAP sends two types of messages to the DSM: EPAP Maintenance Blocks, and DSM Status Requests.

Alarm Handling

All the alarms on the EPAP are reported to the maintenance task in a common message format. The maintenance task forwards the alarms to the primary DSM in the Maintenance Block message (see "Maintenance Blocks" on page 4-2), which is reported on the EAGLE 5 ISS terminal by the OAM. The various alarm messages are described in Chapter 4, *"Messages, Alarms, and Status Reporting."*

Status Reporting

The Active EPAP generates and sends Maintenance Blocks to the primary DSM. One Maintenance Block will be sent as soon as the IP link is established between the Active EPAP and the primary DSM. Additional Maintenance Blocks will be sent whenever the EPAP 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`** and **`rept-stat-sccp`** commands (see "Commands" on page 4-9).

Whenever the EPAP desires to know the status of a DSM, it can send a DSM Status Request to that DSM (see"DSM Status Requests" on page 4-3). The EPAP broadcasts the DSM Status Request over UDP, and all DSMs return their status. DSMs also send a DSM status message to the EPAP when certain events occur in the DSM.

EPAP status reporting is discussed in detail in Chapter 4, *"Messages, Alarms, and Status Reporting."*

3

EPAP Graphical User Interface

Overview of the EPAP User Interface

The EAGLE Provisioning Application Processor (EPAP) User Interface contains two user interfaces:

- The Graphical User Interface provides GUI menus that maintain, debug, and operate the platform; the GUI and its associated error messages are described in this chapter.
- The text-based User Interface has the Configuration menu to initialize and configure the EPAP; the text-based UI is described in Chapter 5, *"EPAP Software Configuration"*.

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

To communicate with the EPAP graphical user interface, you use a PC with a network connection and a network browser. For information about using the EPAP GUI, see "EPAP Graphical User Interface" on page 3-2.

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

EPAP Graphical User Interface

EPAP 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® Internet Explorer, version 5.0 or later, and on Mozilla® Firefox®, version 1.0.2 or later. When using Firefox, you will encounter the following message when logging into the EPAP 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.

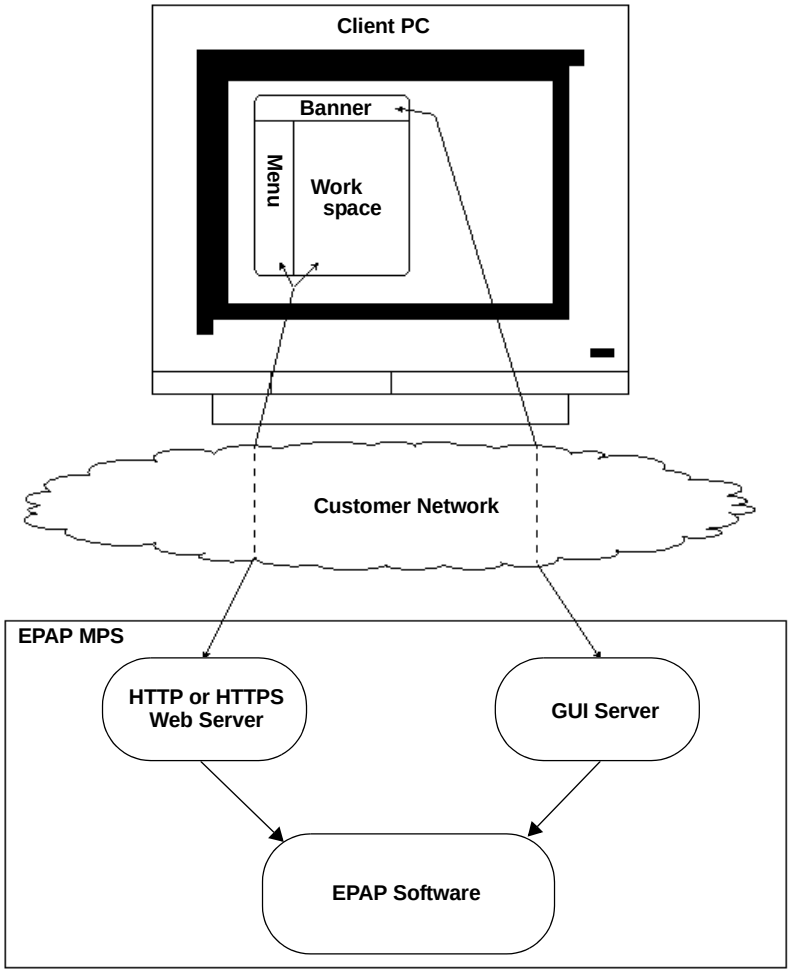
- A banner header section for displaying the real-time status of the MPS servers
- A menu section for selecting desired actions
- A work area section for filling out requested information and displaying results.

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 (Hypertext Transfer Protocol) or https (Secure Hypertext Transfer Protocol) 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 or https web server just returns the document to the browser. The EPAP software may also connect with the GUI server to request that actions be performed. HTML output from the script is then returned to the browser and displayed.

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

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



This section describes the various screens, screen structure and layouts, and input prompts of the EPAP user interface (UI). It describes the login screen and the contents of the main screen. It explains the three frames comprising the browser window in the EPAP user interface.

EPAP Support for HTTPS on GUI

The EPAP Support for HTTPS on GUI feature allows users to configure whether the GUI can be accessed only by standard HTTP (Hypertext Transfer Protocol) or only by HTTPS (Secure Hypertext Transfer Protocol) or by both.

In standard HTTP protocol, the data transfer between the web server and the GUI is not encrypted; therefore, it can be captured by any network analyzer and viewed.

Secure HTTP (HTTPS) supports encryption of data exchanged between the web server and the browser. This facilitates data privacy.

EPAP allows any user who belongs to the admin user group to configure the use of either HTTP or HTTPS, or both, for the EPAP GUI. The admin group user can disable HTTP. The ability to configure HTTP and HTTPS and the ability to disable HTTP can be limited to a specific user class or group. For more information about configuring the use of HTTP or HTTPS or both, see “HTTP(S) Support” on page 3-159.

Starting the Non-secure Web-based GUI

To start the non-secure web GUI, first start a web browser (Internet Explorer). In the Address field, enter either of the following URLs and press Go:

- `http://<EPAP_server_IP_address>/`
- `< EPAP_server_IP_address>`
- `< EPAP_server_hostname>`

If the HTTP interface is disabled, the browser displays an error page "The page cannot be displayed".

Starting the Secure Web-based GUI

To start the secure web-based GUI, first start a web browser (Internet Explorer). In the Address field, enter any of the following URLs and press 'Go':

- `https://<EPAP_server_IP_address>/`
- `https://<EPAP_server_hostname>/`

If the HTTPS interface is disabled, the browser displays an error page "The page cannot be displayed".

Importing a Security Certificate for HTTPS

When the HTTPS interface is used for the first time, the security certificate needs to be imported to the client machine, using the following procedure:

Procedure

1. Obtain the URL for the EPAP server from your network administrator.
2. Open a web browser and type the following in the address field (where `<EPAP_server_IP_address>` is the URL of the EPAP server):

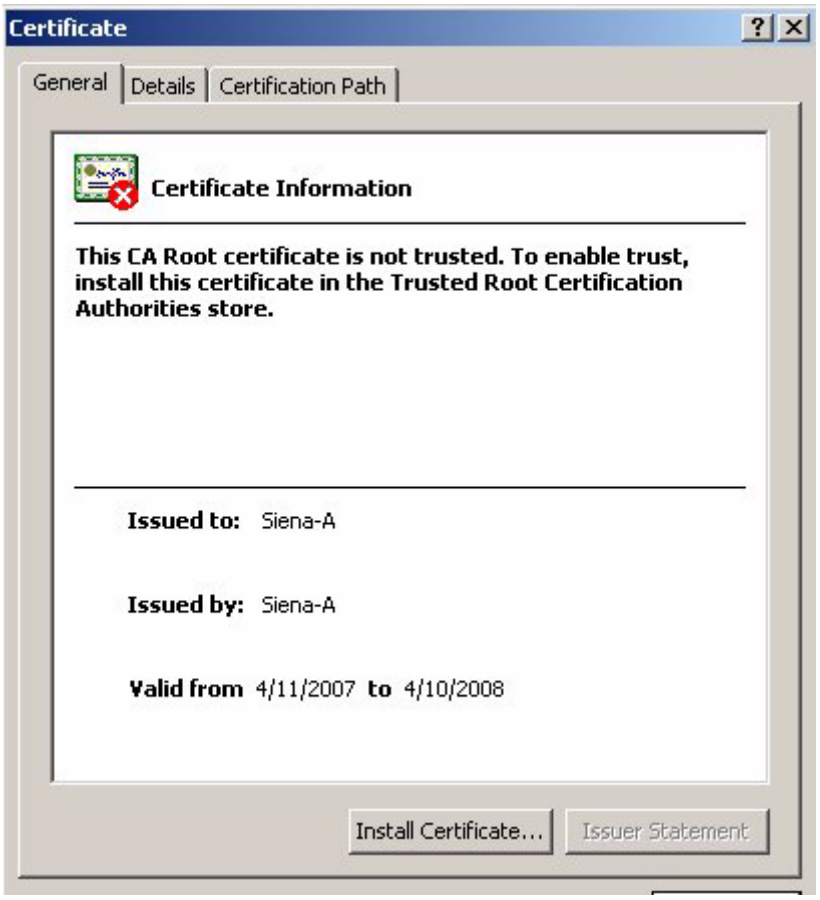
   `https://<EPAP_server_IP_address>`

   The window shown in Figure 3-2 is displayed.

Figure 3-2. HTTPS Security Alert Window

3. Click **View Certificate**. The window shown in Figure 3-3 is displayed.

Figure 3-3. Certificate Information Window

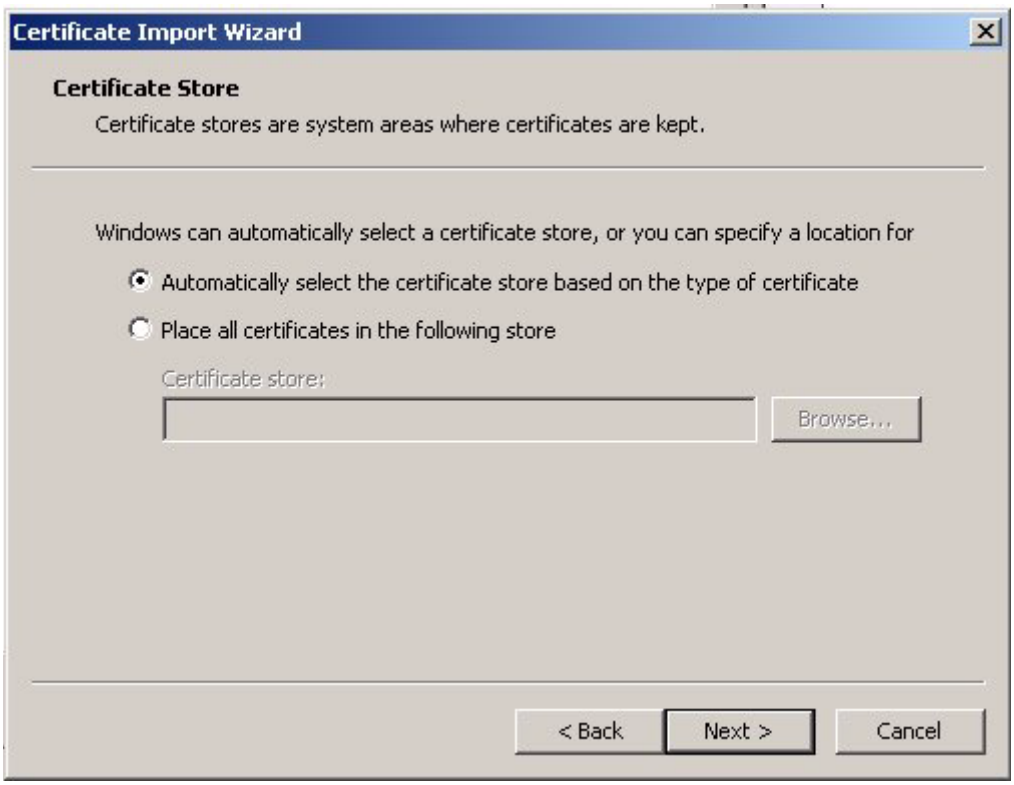


4. Click **Install Certificate**. The window shown in Figure 3-4 is displayed.

Figure 3-4. Certificate Manager Import Wizard

5. Click **Next**. The window shown in Figure 3-5 is displayed.

Figure 3-5. Select a Certificate Store Window



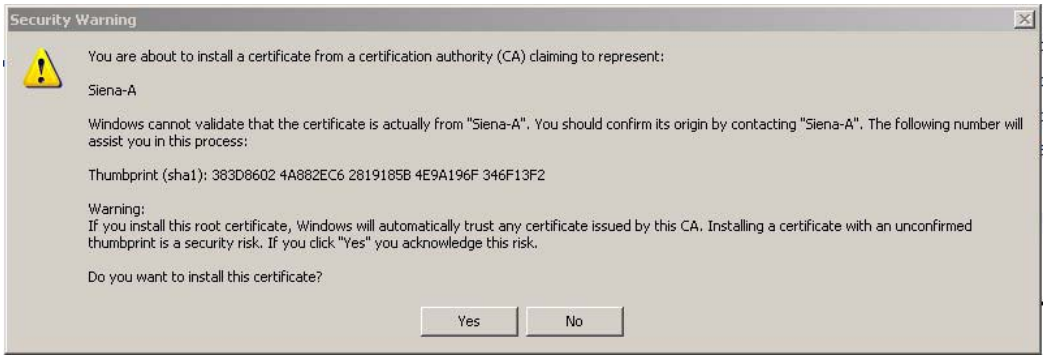
Ensure that the radio button "Automatically select the certificate store based on the type of certificate." is selected.

6. Click **Next**. The window shown in Figure 3-6 is displayed.

Figure 3-6. Completing the Certificate Manager Import Wizard

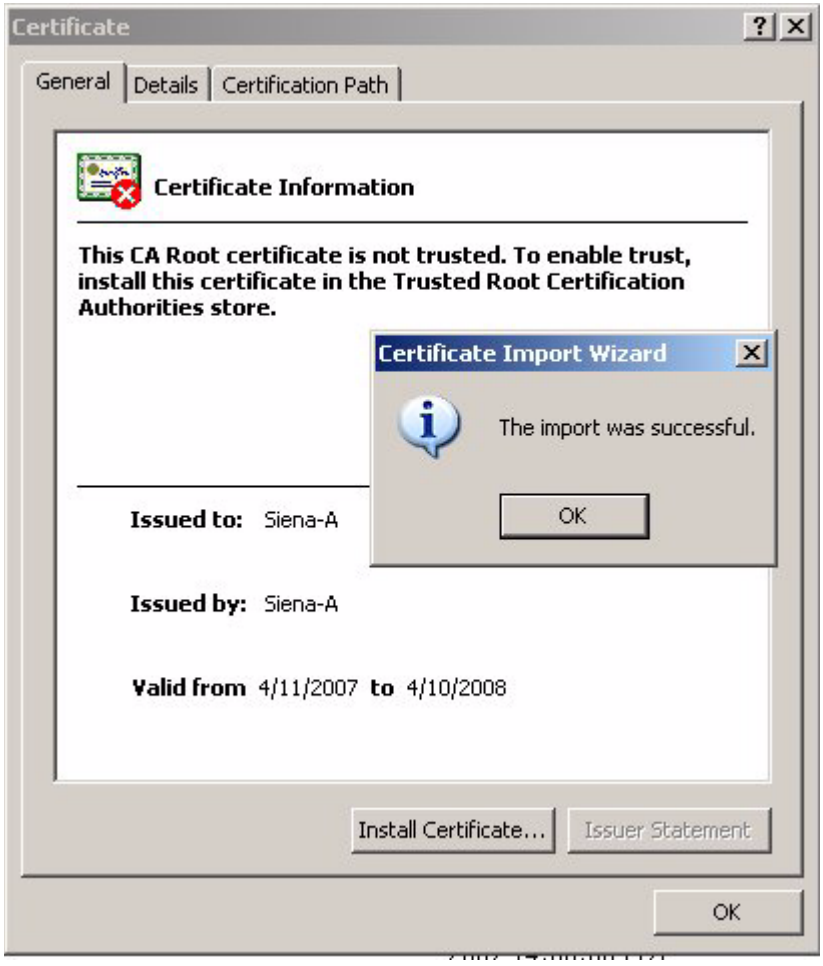
7. Click **Finish**. The window shown in Figure 3-7 is displayed.

Figure 3-7. Security Warning



8. Click **Yes**. The window shown in Figure 3-8 is displayed.

Figure 3-8. Completing the Certificate Manager Import Wizard

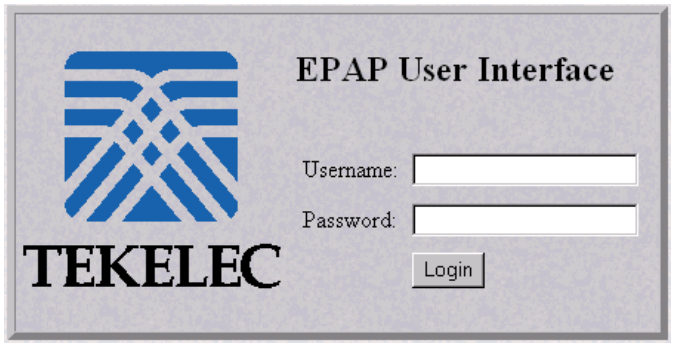


9. Click **OK**.

Login Screen

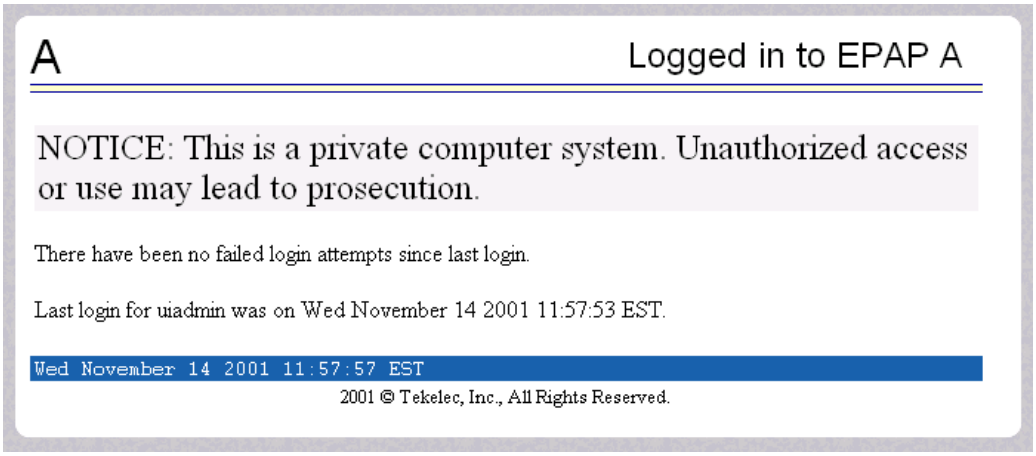
The first screen in the EPAP User Interface is the login screen. Two fields are prompted for on this screen: **Username** and **Password**. To log in, enter a valid user name and password, and click the Login button. These fields provide the user identification and verification. See Figure 3-9.

Figure 3-9. EPAP UI Login Screen



When a user logs in successfully, the screen workspace indicates the user is logged in, as shown in Figure 3-10.

Figure 3-10. Successful Log In to EPAP UI



When a user logs into the EPAP UI, he does not need to log in again so long as the web browser session remains and so long as no user in the admin user group changes the HTTPS configuration. If the HTTPS configuration does not change, the user does not need to log in again because 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. If a user in the admin user group changes the HTTPS configuration from only HTTP to only HTTPS, all users logged in are disconnected. Similarly, If a user in the admin user group changes

the HTTPS configuration from only HTTPS to only HTTP, all users logged in are disconnected. For more information, see “EPAP Support for HTTPS on GUI” on page 3-4.

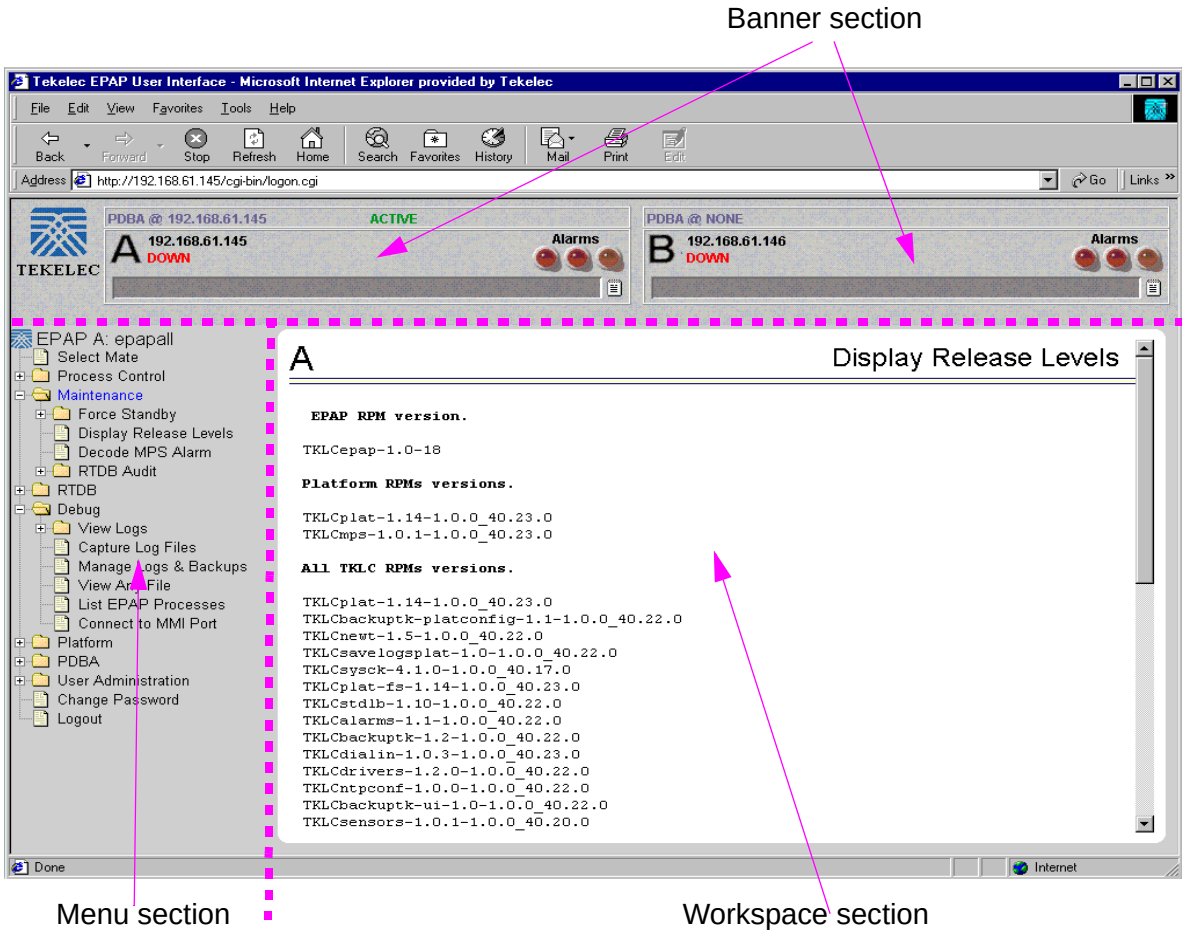
The user uses the Logout menu option to terminate the session and invalidate the cookie. Alternatively, the user can be logged out by session inactivity (defined by User Administration), by disabling in the HTTP or HTTPS configuration, terminated by the administrator, and by selecting another window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

EPAP GUI Main Screen

The EPAP 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 called the workspace section. See Figure 3-11 for a view of the EPAP GUI main screen.

Figure 3-11. EPAP GUI Main Screen



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

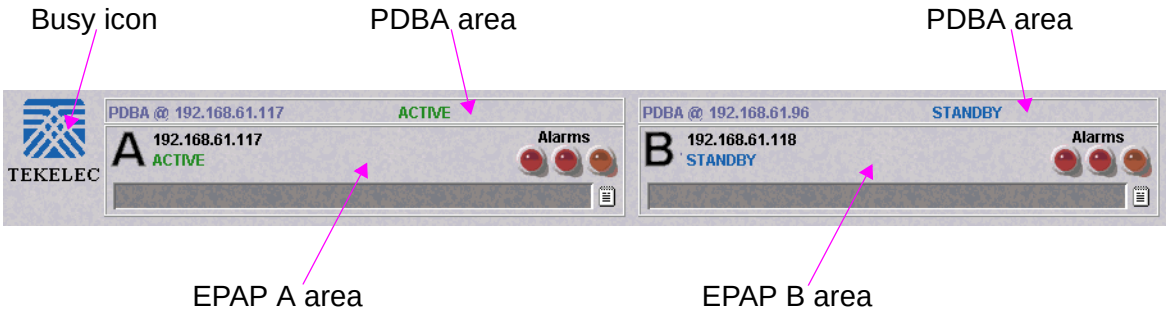
- “Banner Section” on page 3-13
- “Menu Section” on page 3-17
- “Workspace Section” on page 3-18

Banner Section

In order to display real time status information, the banner section (the top area of the UI screen shown in Figure 3-11) has a Java applet that remains in constant communication with the EPAP program. The banner applet displays current status of the EPAP, state of the alarms, etc.

The banner applet contains the EPAP A and B areas, both PDBA areas, and the busy icon. See Figure 3-12.

Figure 3-12. EPAP Banner Applet

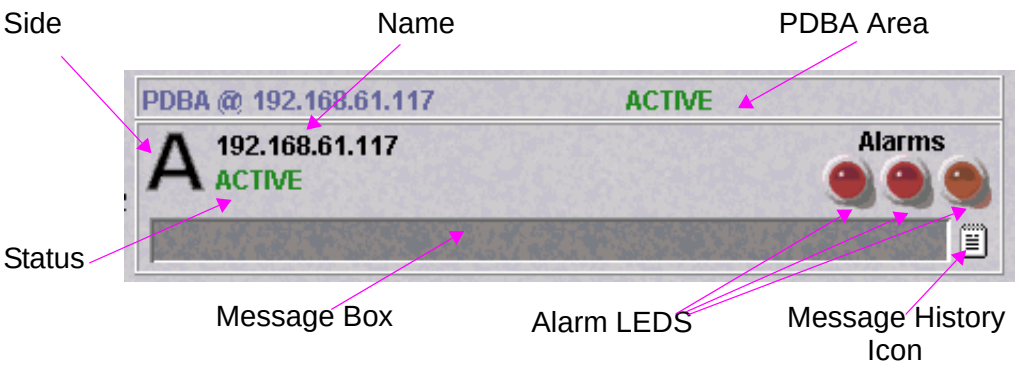


The Tekelec company logo is located at the top left of the banner applet and performs as the busy icon. Its purpose is to serve as an indicator of activity in progress. When an action is being performed, the Tekelec icon moves; when the action ends, the icon is at rest.

EPAP Areas

The EPAP A and EPAP B areas contain information and displays to inform the user about the status and operation of the servers. See Figure 3-13.

Figure 3-13. EPAP Area



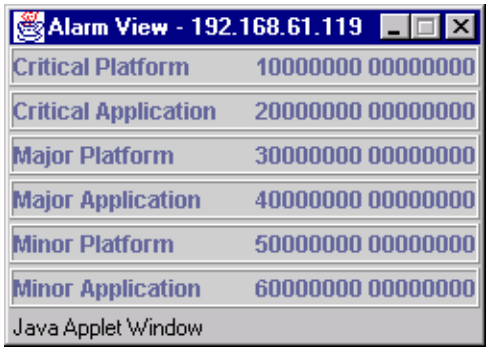
EPAP A and EPAP B each have their own sections in the applet, but are structured similarly. The EPAP areas are described:

- EPAP Server - This indicator simply shows which side of the EPAP (A or B) is represented by this area. There is no action available via click or mouse-over for this field.
- Name - The Name field displays the name of the EPAP represented by this area.

- Status - The Status field displays the current status of the EPAP. The following values can be displayed:
  - NONE: No established connection exists to the EPAP GUI Server. This can result because of connectivity problems or because the EPAP 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 EPAP is capable of being the active EPAP but is not for some reason. Valid reasons are either its mate EPAP is active, or there are no DSMs to provision. In the latter case, both EPAPs are STANDBY.
  - FORCED STANDBY: This EPAP has been forced into the standby state by the user.
  - ACTIVE: This EPAP 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 EPAP state. This indicator on the browser indicates that the client browser's Java policy file is incorrect. For details, see “Installing Java Policy File” on page 5-7.
- Alarm LEDs - The three Alarm LED 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 3-14.

Figure 3-14. 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 MPS Alarm” on page 3-27.

- Message Box - The message box is 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 EPAP machine.

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

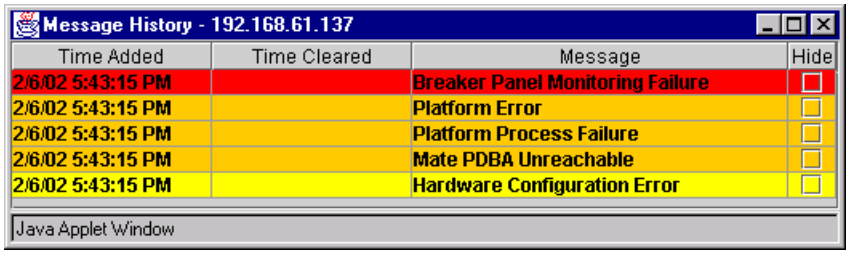
  - `Backup file system successful`
  - `Restore RTDB in progress`
  - `RTDB synchronization in progress`

  See “EPAP Banner Messages” on page 3-169 for the complete list of messages appearing in the message box.

- 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. Figure 3-15 has a sample Message History box.

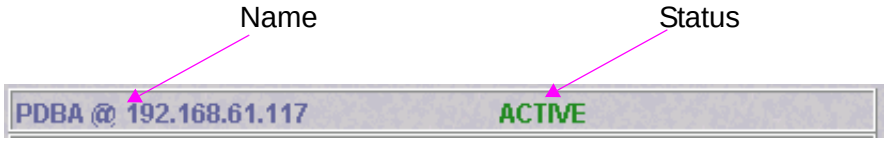
Figure 3-15. Example of Message History



PDBA Area

The PDBA areas each occupy a part of the banner applet, and have the following indicators and displays. See Figure 3-16.

Figure 3-16. PDBA Area



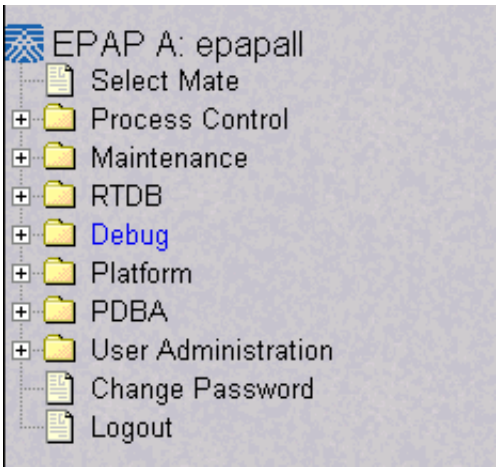
- Name - The Name field displays the name of the MPS in this area.
- Status - The Status field displays the current status of the EPAP in this area. The Status field values are:
  - NONE: No established connection currently exists to the EPAP GUI server. This can result because of connectivity problems or because the GUI server is not running.
  - DOWN: EPAP was contacted, but the PDBA software is not running.
  - STANDBY: PDBA software is running as Standby.
  - ACTIVE: PDBA software is running as Active.
  - REPLERR: PDBA detected presence of an PDB replication failure.

Menu Section

The EPAP graphical user interface menu is located in the left frame of EPAP browser interface. At the top of the frame is the software system title, EPAP, 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 EPAP browser interface. An example of a menu in the menu section is shown in Figure 3-17.

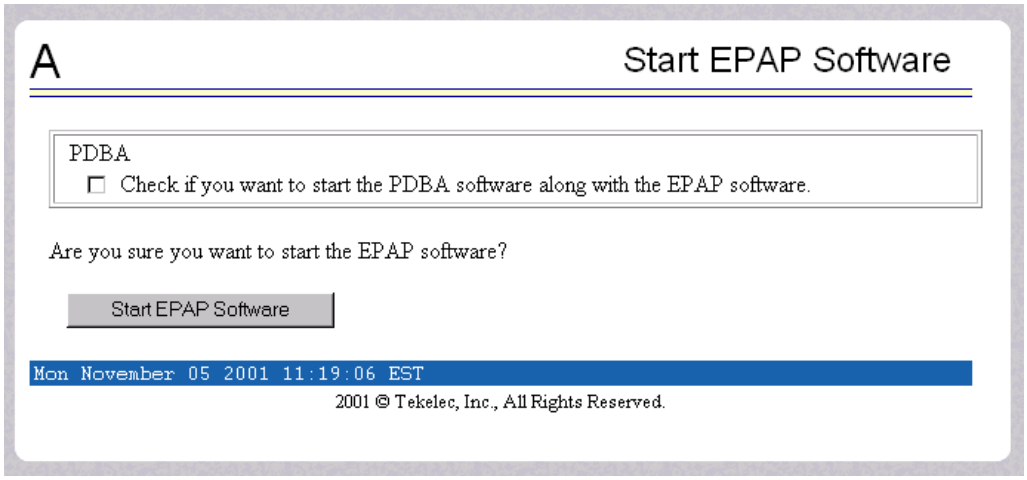
Figure 3-17. Example of an EPAP Menu



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 Figure 3-18.

Figure 3-18. 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

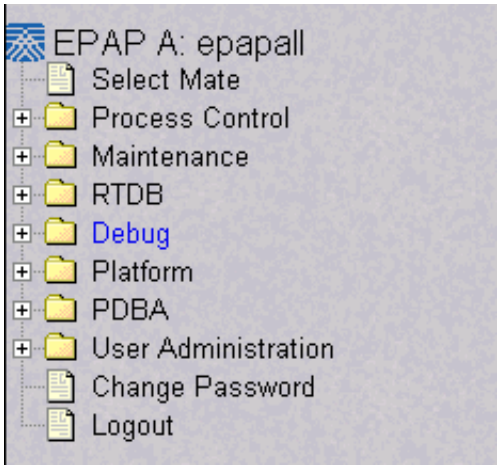
The web browser user interface uses layers of syntax checking to validate user input for text-entry fields.

- 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.

EPAP User Interface Menus

The EPAP menu is the main menu of the EPAP application. It provides the functions of the EPAP User Interface. Figure 3-19 shows the EPAP main menu.

Figure 3-19. EPAP Menu



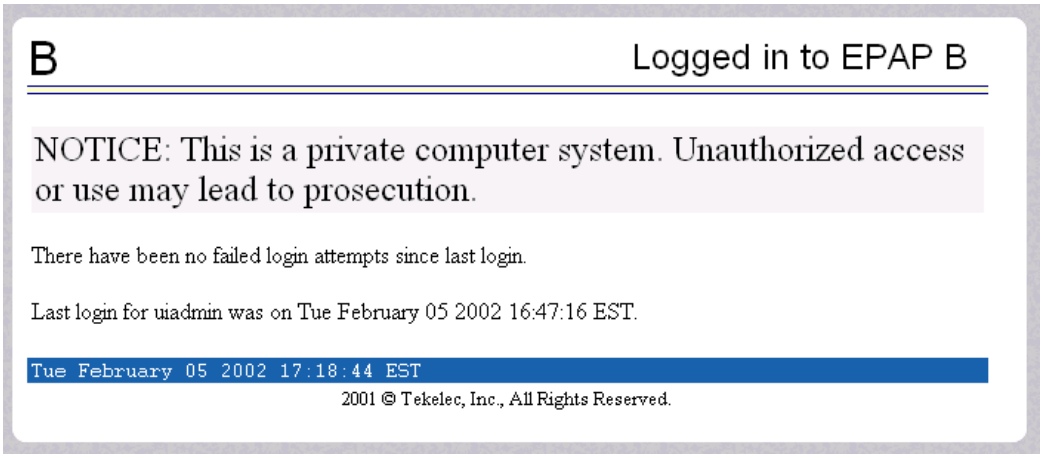
The EPAP menu provides three actions common to all users, Select Mate, Change Password, and Logout. All the remaining actions are options assignable by the system administrator to groups and individual users.

Select Mate

The Select Mate menu selection changes the menus and workspace areas to point to the EPAP mate. This selection exchanges the status of the active and standby EPAPs. This basic action is available to all users and is accessible from the main menu (Figure 3-19, on page 3-19).

If you using EPAP A at the main menu, and you want to switch to EPAP 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 3-20.

Figure 3-20. Select Mate Screen

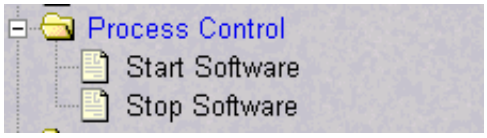


When you perform the Select Mate action, the contents of the banner do not change. However, the side (server) changes in the workspace and at the top of the menu area to indicate the active EPAP.

Process Control Menu

The Process Control menu allows the user to start and stop the EPAP software processes. See the Process Control menu in Figure 3-21.

Figure 3-21. Process Control Menu



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

- "Start EPAP Software" on page 3-21
- "Stop EPAP Software" on page 3-22

Start EPAP Software

The Process Control / Start EPAP Software menu option lets you start the EPAP software processes. The screen contains a button to confirm that you do want to start the software processes and a checkbox to start the PDBA. See Figure 3-22 for the Start EPAP Software screen, and Figure 3-23 for a successful start of the EPAP software.

Figure 3-22. Start EPAP Software Screen

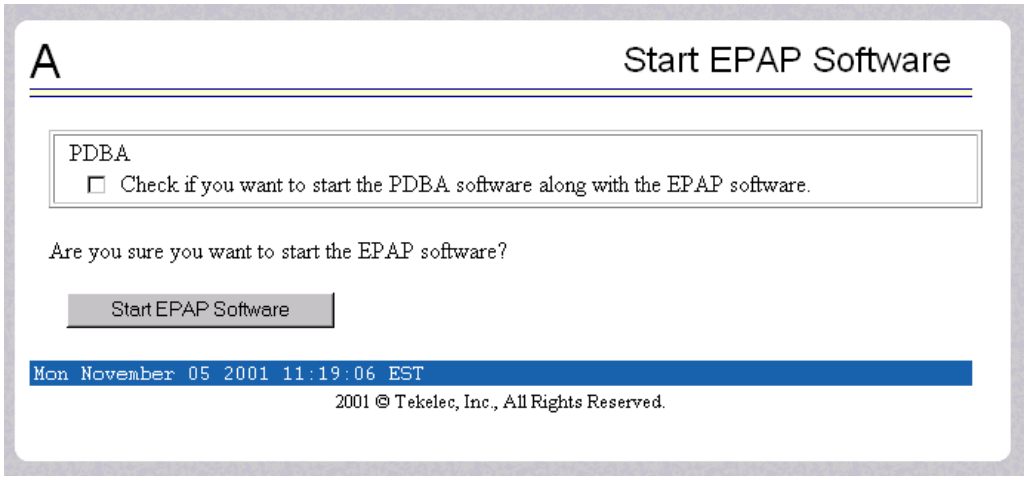
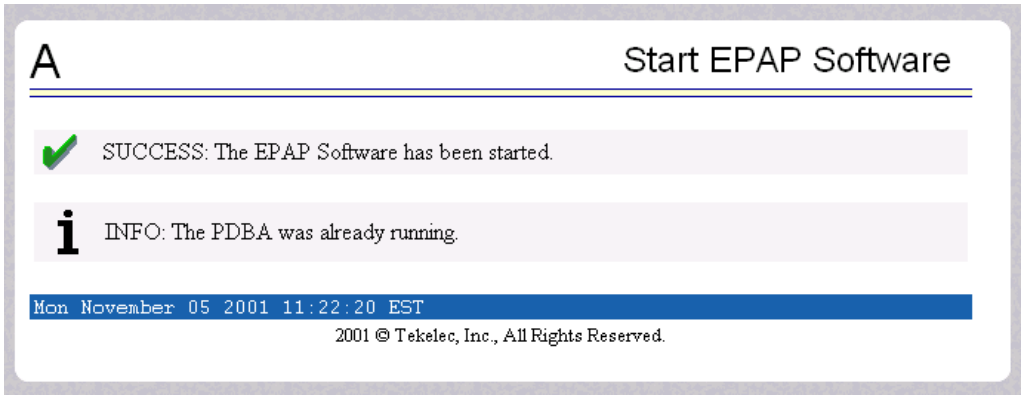


Figure 3-23. Successful Start of EPAP Software Screen



Stop EPAP Software

The Process Control / Stop EPAP Software screen lets the user stop the EPAP software processes. The screen contains a button to confirm that the user does want to stop the software processes. It also lets you choose whether the software is to restart automatically when the server reboots. See Figure 3-24 for the Stop EPAP Software screen, and Figure 3-25 for a successful stop.

Figure 3-24. Stop EPAP Software Screen

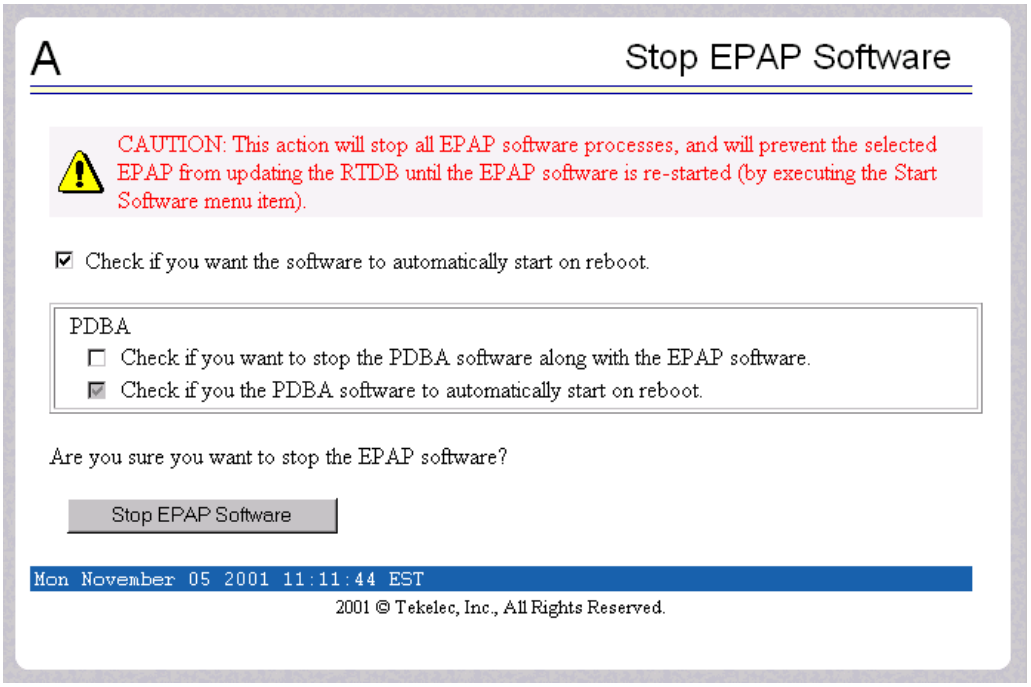
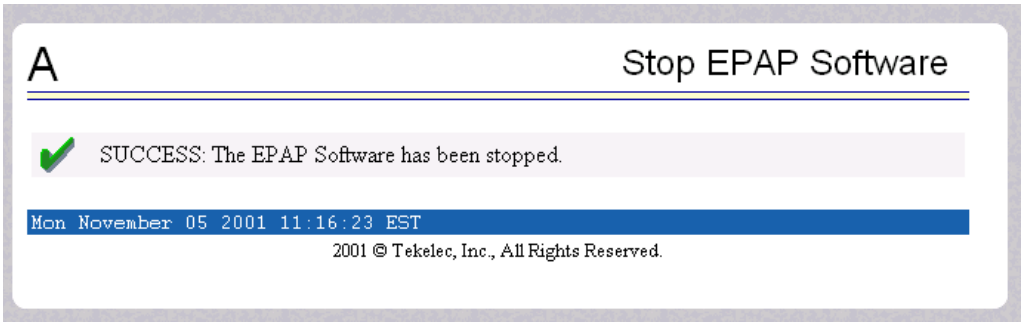


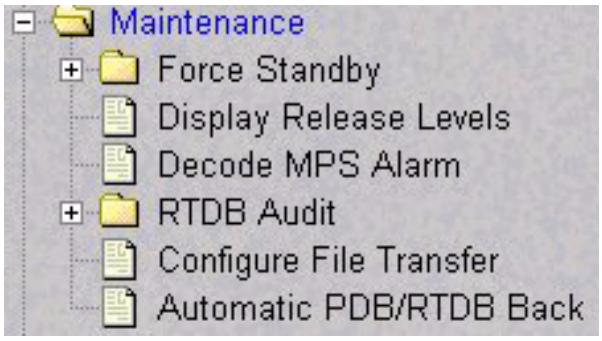
Figure 3-25. Successful Stop of EPAP Software Screen



Maintenance Menu

The Maintenance Menu lets you perform various EPAP platform tasks shown in Figure 3-26.

Figure 3-26. Maintenance Menu



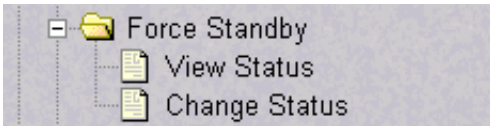
The Maintenance menu provides the following actions:

- "Force Standby" on page 3-24
- "Display Release Levels" on page 3-27
- "Decode MPS Alarm" on page 3-27
- "RTDB Audit" on page 3-28
- "Configure File Transfer" on page 3-30
- "Automatic PDB/RTDB Backup" on page 3-31

Force Standby

The Maintenance / Force Standby menu lets you view the EPAP state and change it by toggle into and out of forced standby state. See Figure 3-27.

Figure 3-27. Force Standby Menu



The Force Standby menu provides the following actions:

- "View Status" on page 3-25
- "Change Status" on page 3-25

View Status

This Maintenance / Force Standby / View Status screen displays whether or not EPAP is currently in a forced standby state. See Figure 3-28.

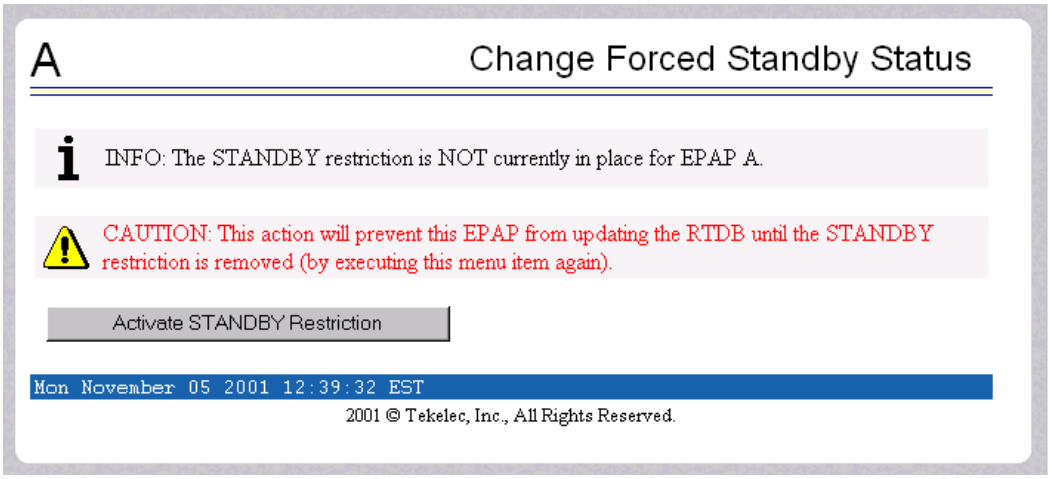
Figure 3-28. View Forced Standby Status Screen

Change Status

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

If the EPAP is currently in forced standby mode, the user can remove the standby restriction on the selected EPAP. See the Change Forced Standby Status screen in Figure 3-29.

Figure 3-29. Change Forced Standby Status Screen

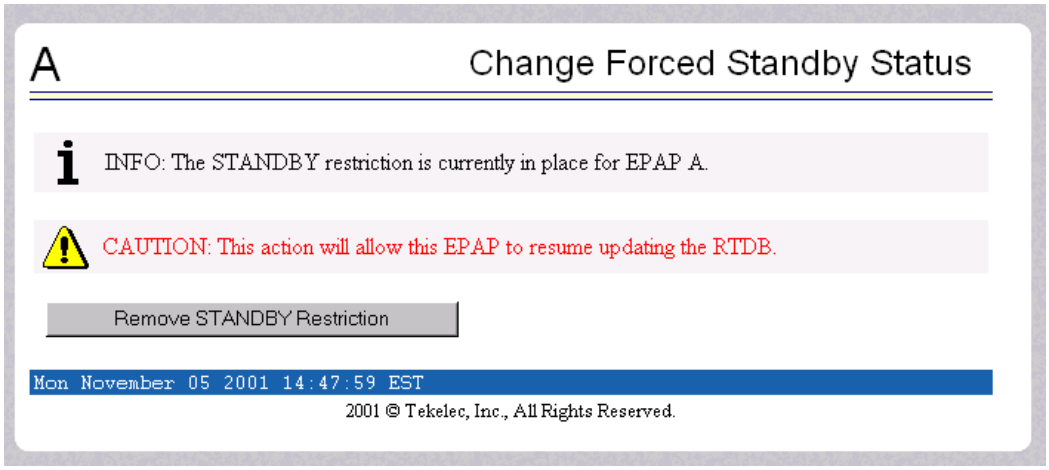


To put the current EPAP in forced standby mode, click the Activate STANDBY Restriction button. See Figure 3-30 for the screen showing successful change of status.

Figure 3-30. Successfully Changing Forced Standby Status

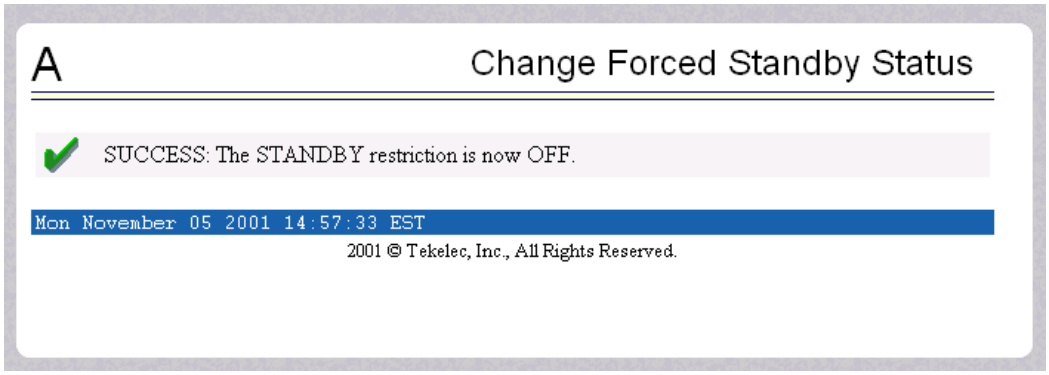
To remove the forced standby mode, click the Change Status button and see the screen that initiates the removal of the forced standby state, shown by Figure 3-31.

Figure 3-31. Removing Changing Forced Standby Status



To finish removing the forced standby status, click the Remove STANDBY Restriction button. See Figure 3-32 for the screen showing a successful change of forced standby status.

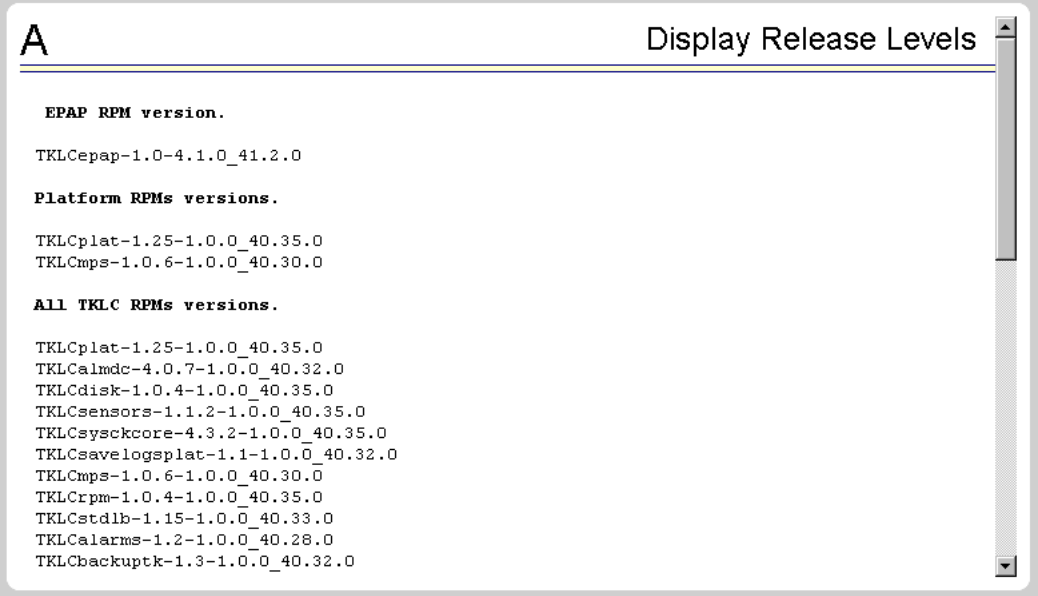
Figure 3-32. Successfully Removing Changed Forced Standby Status



Display Release Levels

The Maintenance / Display Release Levels screen displays release information, as shown in Figure 3-33.

Figure 3-33. Display Release Levels Screen



Decode MPS Alarm

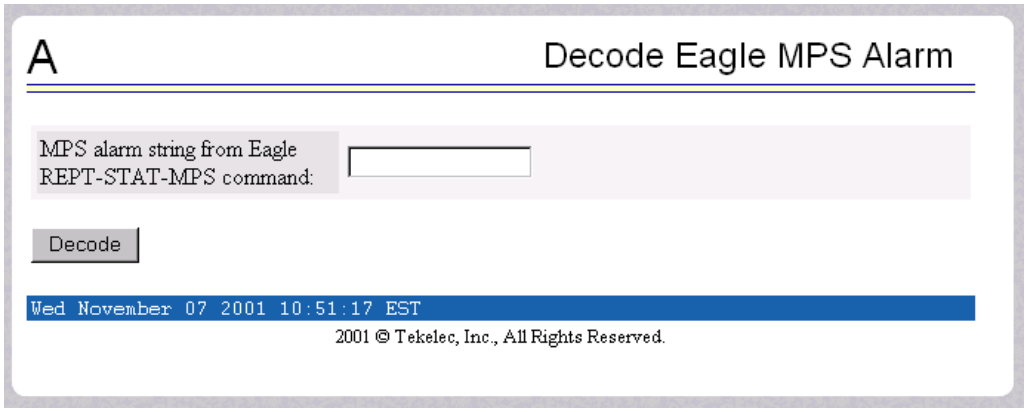
The Maintenance / Decode EAGLE 5 ISS MPS Alarm screen lets the user decode the EAGLE 5 ISS output of MPS alarms. The user enters the 16-character hexadecimal string from the EAGLE 5 ISS **`rept-stat-mps`** command. The strings are encoded from one of the following six categories, which are reported by 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. Message details can be found in the *MPS Platform Software and Maintenance Manual*.

The text for the alarms indicated by the alarm hex string is described in "MPS Platform and EPAP Application Alarms" on page 4-16. See Figure 3-34 for the Decode EAGLE 5 ISS MPS Alarm screen.

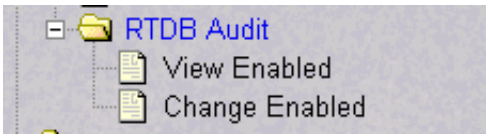
Figure 3-34. Decode EAGLE 5 ISS MPS Alarm Screen



RTDB Audit

The Maintenance / RTDB Audit menu lets the user view and change the auditing of the selected EPAP. See Figure 3-35 for the Maintenance / RTDB Audit Menu.

Figure 3-35. RTBD Audit Menu



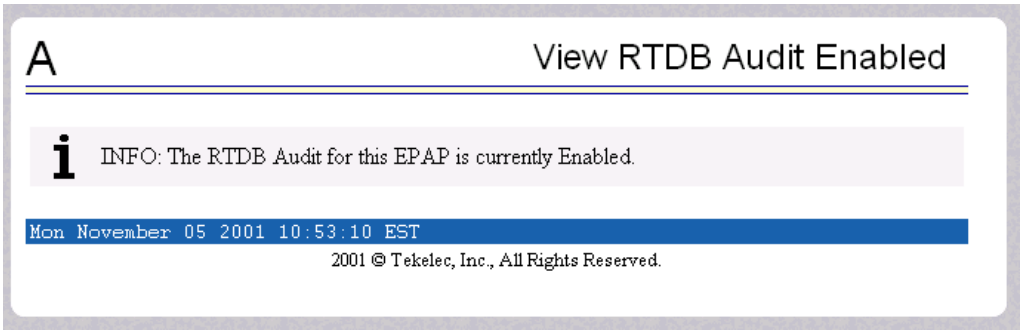
The RTDB Audit menu provides these RTDB Audit tasks:

- "View Enabled" on page 3-29
- "Change Enabled" on page 3-29

View Enabled

The Maintenance / RTDB Audit / View Enable menu selection lets the user view the status of RTDB audit enabled, as shown in Figure 3-36.

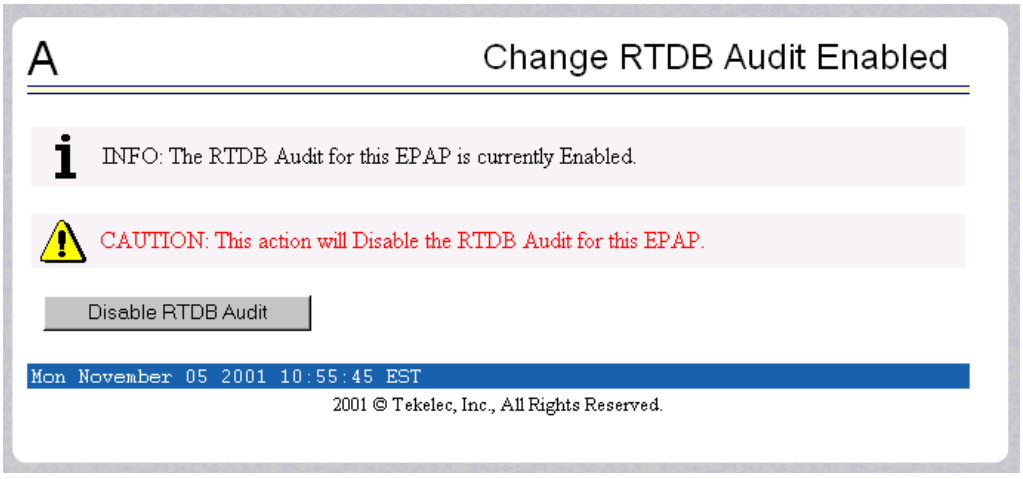
Figure 3-36. View the RTDB Status Screen



Change Enabled

The Maintenance / RTDB Audit / Change Enabled screen turns auditing on and off for the RTDB that is on the selected EPAP. The user interface detects the whether RTDB audit is engaged or disengaged, and provides the associated screen to toggle the state. In Figure 3-37, the RTDB Audit is shown as enabled. Clicking the Disable RTDB Audit button here toggles the RTDB Audit to disabled.

Figure 3-37. Change the RTDB Audit Enabled Screen



Configure File Transfer

This screen has several different functions. This screen is used as follows:

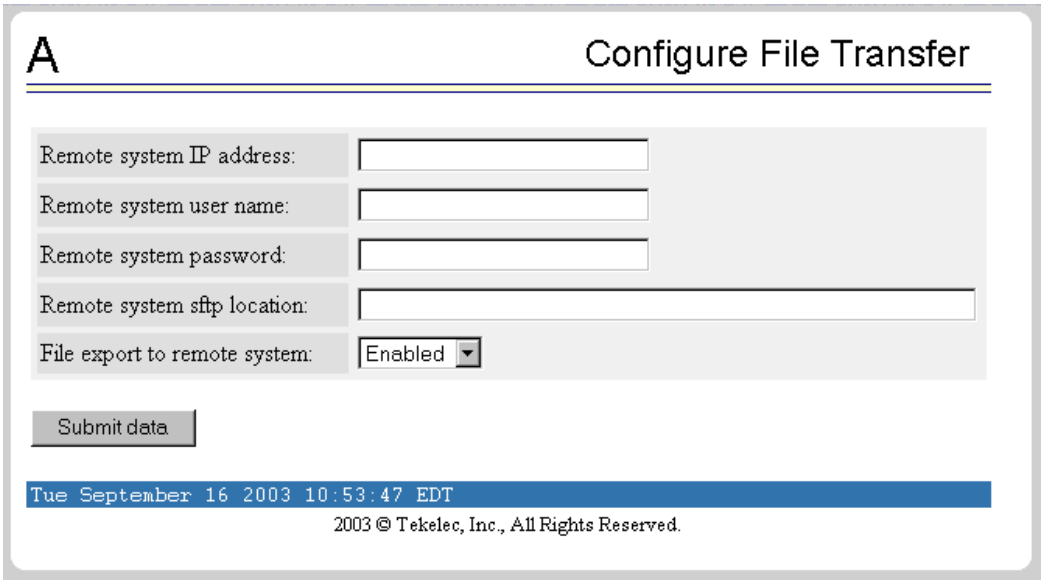
- Define the location of where the results of the automatic import are stored.
- Provide the options for enabling/disabling the Automatic Export capability.
- Provide a mechanism for testing the connection to the remote machine. This is done by using the username/ password and IP address provided to attempt to make an SFTP connection to the remote machine. The status of the connection is then displayed . This test is run anytime the data on this screen is entered or modified.

This screen consists of the following fields:

- Remote System IP Address - the IP address from where the data will be exported (customer system).
- Remote System User Name - required for logging onto the customer system
- Remote System Password - required for logging onto the customer system. This password will be stored in encrypted format.
- Remote System SFTP Location - the location of the directory on the customer system.
- File Export to Remote System - this is used to return the results of the import file (default = enabled).

The Configure File Transfer Screen is shown in Figure 3-38.

Figure 3-38. Configure File Transfer Screen



Automatic PDB/RTDB Backup

This screen is used to configure the Automatic PDB/RTDB Backup. The following are the options for backup type:

- Local - Backup is stored on the same EPAP server
- Mate - Backup is stored on the mate EPAP server
- Remote - Backup is stored on a remote server
- None - No backup is scheduled and cancel all previously scheduled backups. This will not affect a backup that is currently in progress.

NOTE: Verify there is adequate disk space (approximately 17 GB of disk space is required per backup) to store backup files locally, on the mate, or on a remote server.
If there is inadequate disk space to store 3 copies on the local or mate, stored backups will not be overwritten, and backup operation failure alarms will be generated.

Use Table 3-1 as a guide when populating the Automatic PDB/RTDB Backup screen.

Table 3-1. Mandatory verses Optional Parameters

Parameter	Backup Type		
	Local	Mate	Remote
Time of the day to start the Backup	Mandatory	Mandatory	Mandatory
Frequency	Mandatory	Mandatory	Mandatory
File Path (Directory only)	Optional	Optional	Mandatory
Remote Machine IP Address (xxx.xxx.xxx.xxx)	Not Applicable	Not Applicable	Mandatory
Login Name	Not Applicable	Not Applicable	Mandatory
Password	Not Applicable	Not Applicable	Mandatory
Save the local copies in the default path	Not Applicable	Optional	Mandatory
Do you want to delete the old backups (Local and Mate only) Note: If you choose Yes, only the last three backup files, including the current one will be kept.	Mandatory	Mandatory	Not Applicable

Tekelec recommends that this Automatic PDB/RTDB Backup be performed on a daily (24 hour) basis. If the 12-hour frequency is selected, the first backup will always be created in the AM. For example, if the Time of the day to start the backup is selected as 15:00, the first backup will be created at 3 AM and then subsequent backups at 12-hour intervals.

The default file path where subdirectories are created (in the mate and locally) is */var/TKLC/epap/free/*.

In the case of mate and remote backup destinations, a local copy is saved (even if the option not to save the local copy was selected) if the transfer of the file fails after the backup has been created on the local machine. This file is located at the default file path.

If the Automatic PDB/RTDB backups are being directed to a remote server, the following should take place before scheduling:

- SFTP must be installed at the remote server
- The connection to the remote server must be validated
- Verify there is adequate disk space (approximately 17 GB of disk space is required per backup)
- Verify user name and password.

When using the Automatic PDB/RTDB Backup screen to configure the automatic backup, the following semantic rules apply:

Backup Type - Select None to cancel Backups.

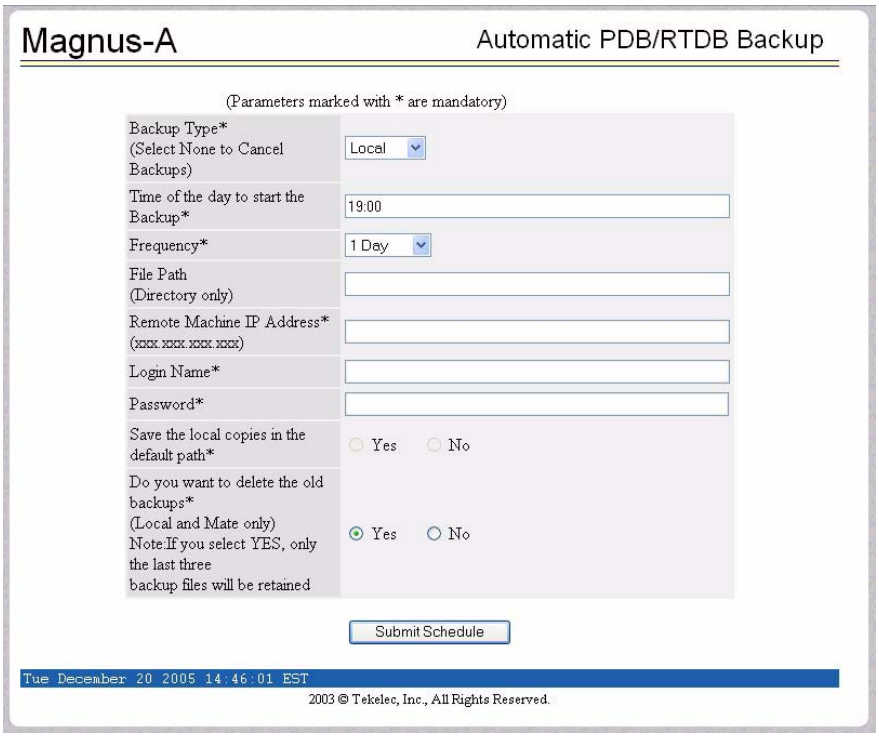
Time of the Day should be in hh:mm 24 hour (`14:03`) format.

File path (in remote only) should be the absolute path from root `/backups/xxxx`

IP address should be in xxx.yyy.zzz.aaa format (`192.168.210.111`).

Password entered by the user shall be displayed in asterisk (`*`)

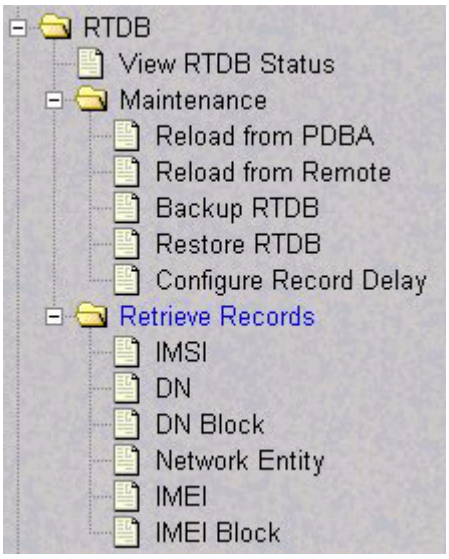
Figure 3-39. Automatic PDB/RTDB Backup Screen



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 3-40.

Figure 3-40. RTDB Menu



The RTDB menu supports viewing the RTDB and performing maintenance tasks:

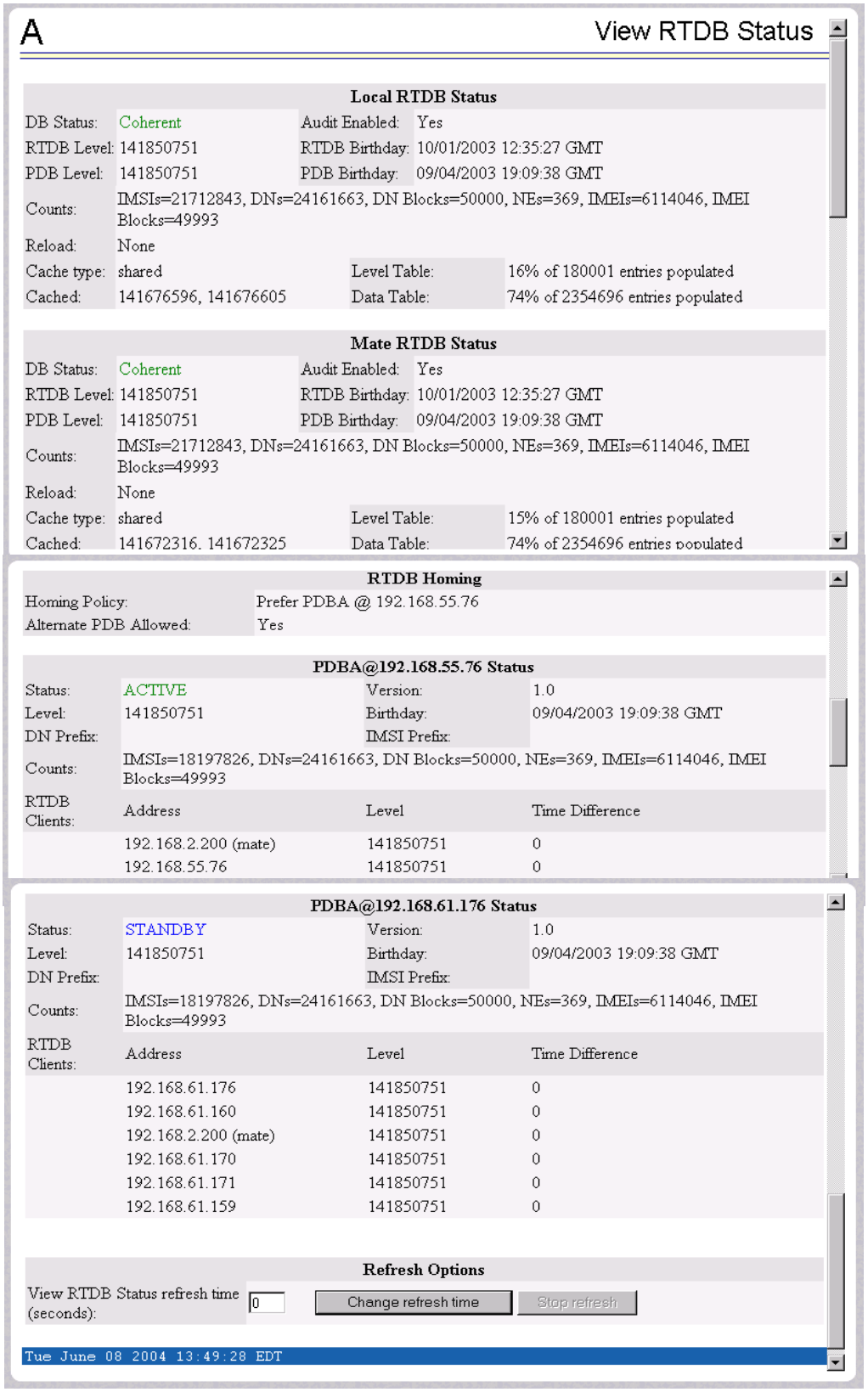
- "View RTDB Status" on page 3-33
- "Maintenance" on page 3-35
- "Retrieve Records" on page 3-39

View RTDB Status

The RTDB / View RTDB Status screen displays the current level and birthday of the EPAP RTDBs. This selection displays the RTDB status information for both the selected EPAP and its mate. The status information reports the DB level and the DB birthday (date and time of the creation of the database). The RTDB Status refresh time can be viewed and changed with this screen. See Figure 3-41.

NOTE: The IMSI count returned from the RTDB and the IMSI count returned from the PDB may not match when there is both G-Flex and EIR data. Any IMSI created for EIR that does not have a G-Flex IMSI association is not included in the IMSI counts of the PDB. The PDB reports only G-Flex IMSIs. The RTDB reports the total of G-Flex and EIR IMSIs as one count.

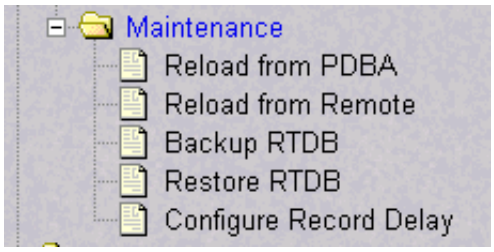
Figure 3-41. View RTDB Status Screen



Maintenance

The RTDB / Maintenance menu allows the user to perform reloads, backups, restores and specify a time limit for PDB records to arrive at the RTDB. See the RTDB / Maintenance menu in Figure 3-42.

Figure 3-42. Maintenance Menu



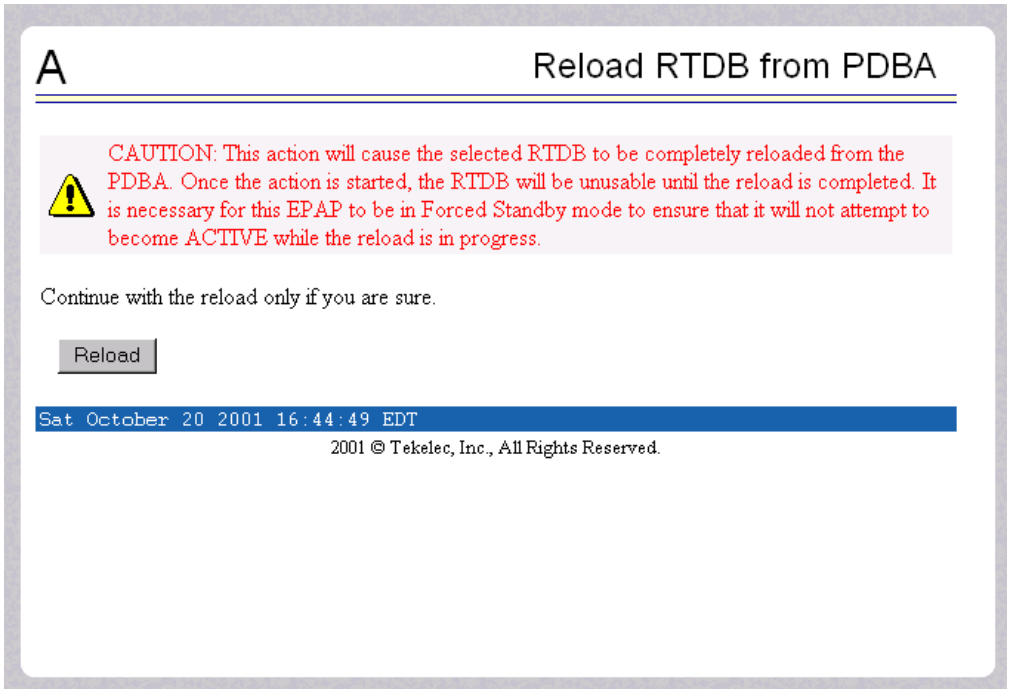
The RTDB / Maintenance menu provides the following actions:

- "Reload RTDB from PDBA" on page 3-36
- "Reload RTDB from Remote" on page 3-37
- "Backup the RTDB" on page 3-38
- "Restore the RTDB" on page 3-38
- "Configure Record Delay" on page 3-39

Reload RTDB from PDBA

The RTDB / Maintenance / Reload RTDB from PDBA screen reloads the RTDB with a copy of the data from the local PDBA. See Figure 3-43.

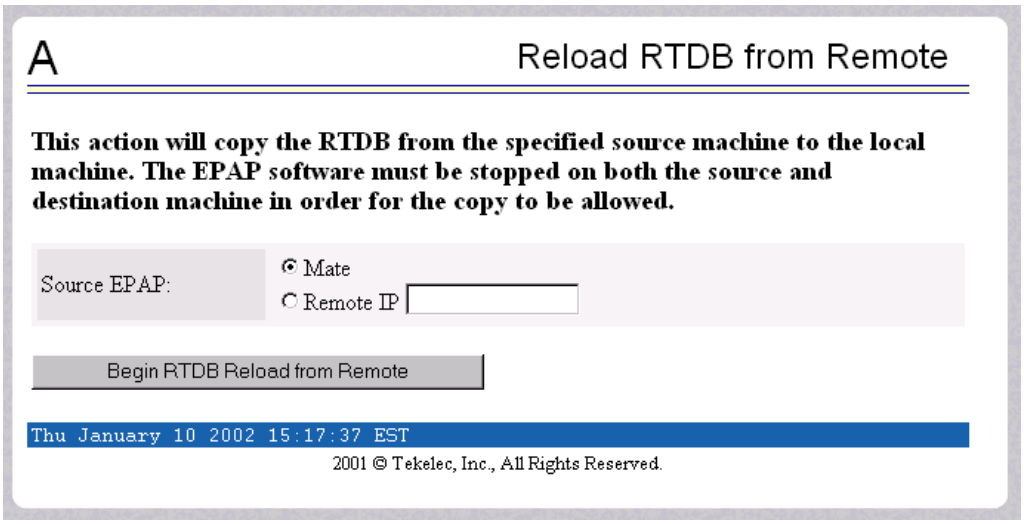
Figure 3-43. Reload RTDB from PDBA Screen



Reload RTDB from Remote

The RTDB / Maintenance / Reload RTDB from Remote screen makes a copy of the RTDB from the specified source machine, either the mate EPAP or a specified IP address. Note that the EPAP software must be stopped on both of the machines involved. See Figure 3-44.

Figure 3-44. Reload RTDB from Remote Screen

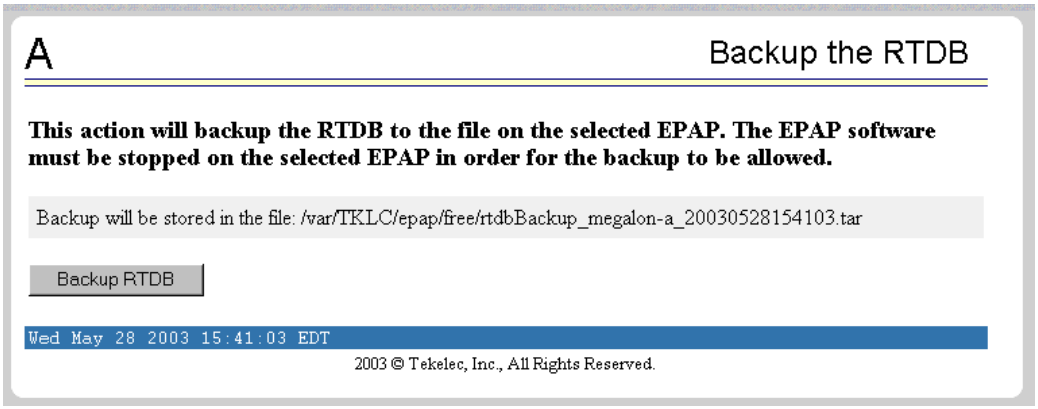


To perform the copy of the RTDB contents, select the source machine and press the Begin RTDB Reload from Remote button.

Backup the RTDB

The RTDB / Maintenance / Backup the RTDB screen allows the user to backup the RTDB to a specified file on the selected EPAP. The software must be stopped on the selected EPAP for the backup to be allowed to ensure that no updates are occurring. See Figure 3-45.

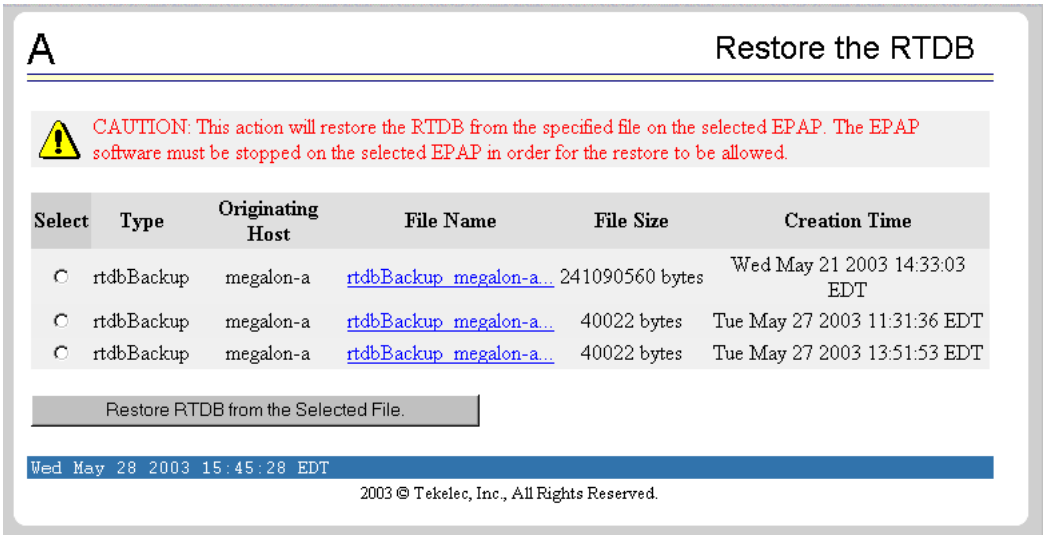
Figure 3-45. Backup the RTDB Screen



Restore the RTDB

The RTDB / Maintenance / Restore the RTDB screen allows the user to restore the RTDB from the specified file on the selected EPAP. The software must be stopped on the selected EPAP for the restore action to be allowed to ensure that no other updates are occurring. See Figure 3-46.

Figure 3-46. Restore the RTDB Screen

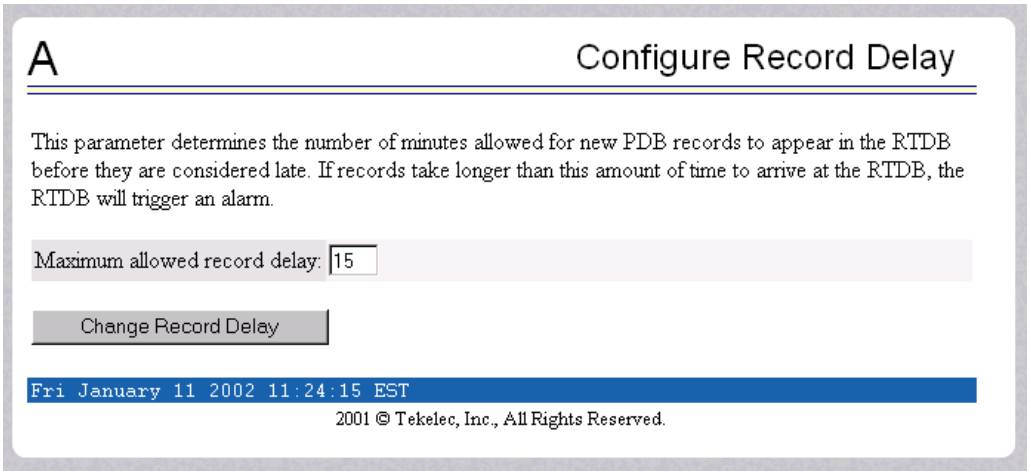


To restore the RTDB contents from a specified file on the selected EPAP, stop the selected EPAP software. Select the proper file and click the Restore RTDB from the Selected File button.

Configure Record Delay

The RTDB / Maintenance / Configure Record Delay screen allows the user to specify the time in minutes for new PDB records to appear in the RTDB. If records take longer to arrive at the RTDB than this amount of time, the records are considered late, and the RTDB triggers an alarm. See Figure 3-47.

Figure 3-47. Configure Record Delay Screen

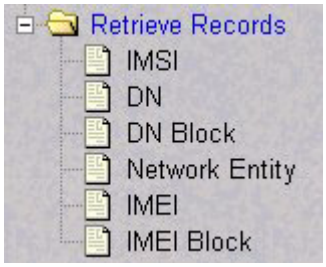


To update the time period for the new PDB records to arrive at the RTDB, enter the desired value in the entry field, and click the Change Record Delay button.

Retrieve Records

The RTDB / Retrieve Records menu allows the user to query (from the web GUI) data that resides in the RTDB (Real-Time Database). The user can compare data in the PDB (Provisioning Database) with data in the RTDB to verify that they are consistent.. See the RTDB / Retrieve Records menu in Figure 3-48.

Figure 3-48. Retrieve Records Menu



The RTDB / Maintenance menu allows the user to retrieve the following types of records:

- "IMSI" on page 3-40
- "Dialed Number" on page 3-41
- "DN Block" on page 3-42
- "Network Entity" on page 3-43
- "IMEI" on page 3-45
- "IMEI Block" on page 3-46

IMSI

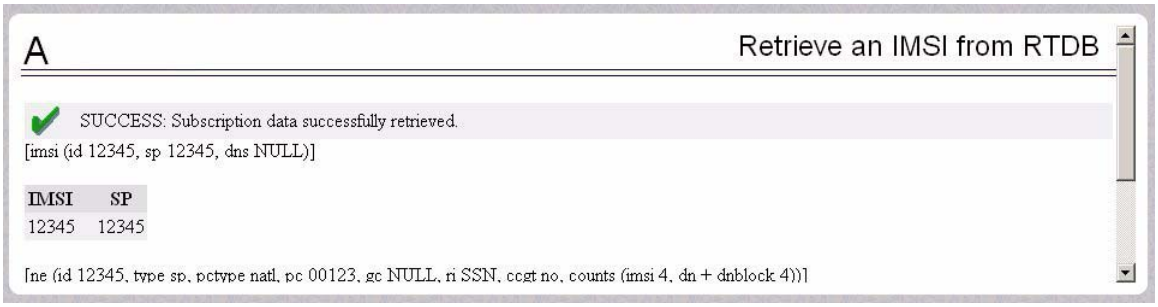
The RTDB / Retrieve Records / IMSI screen allows the user to retrieve information about about an IMSI (International Mobile Subscriber Identity). See Figure 3-49.

Figure 3-49. Retrieve an IMSI from RTDB

The output displays the following information about an IMSI, as shown in Figure 3-50:

- IMSI ID
- SP
- NE data, as described in "Network Entity" on page 3-43, for the Service Provider the IMSI is associated with.
- IMEI data, as described in "IMEI" on page 3-45, if the IMSI being retrieved is associated with an IMEI.

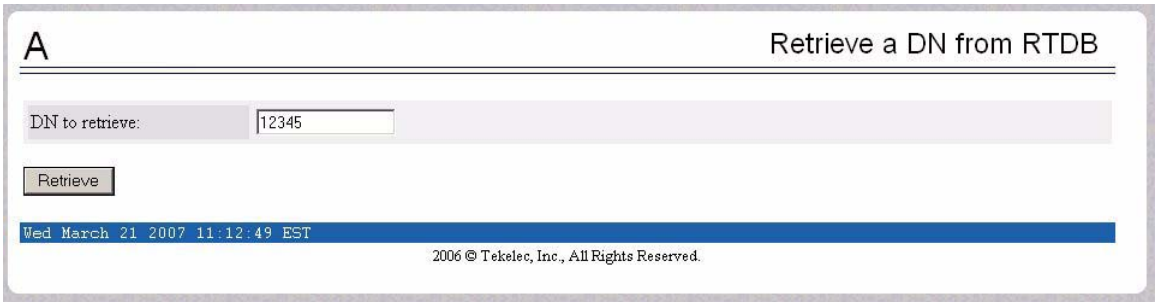
Figure 3-50. Output for Retrieve an IMSI from RTDB



Dialed Number

The RTDB / Retrieve Records / DN screen allows the user to retrieve information about a single Dialed Number (DN). See Figure 3-51.

Figure 3-51. Retrieve DN Information from RTDB

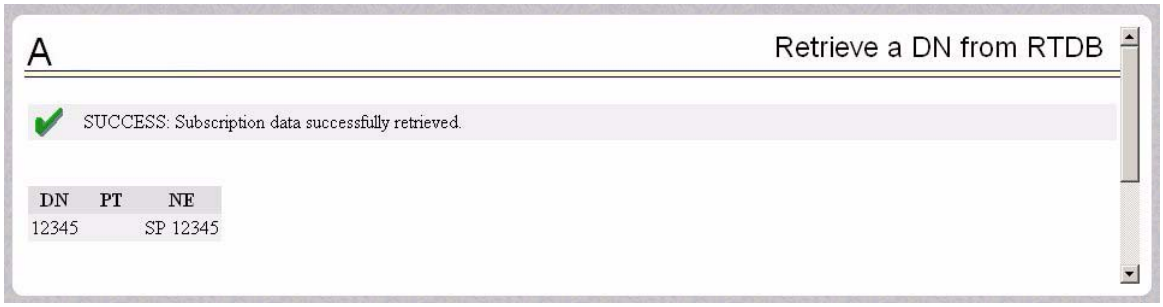


The output displays the following information about single DNs, as shown in Figure 3-52:

- ID
- Portability type (PT)
- Associated SP or RN
- Network Entity (NE) data, as described in “Network Entity” on page 3-43, if the DN being retrieved is associated with an NE.

If a DN cannot be found in the single DN database, the DN Block database is searched.

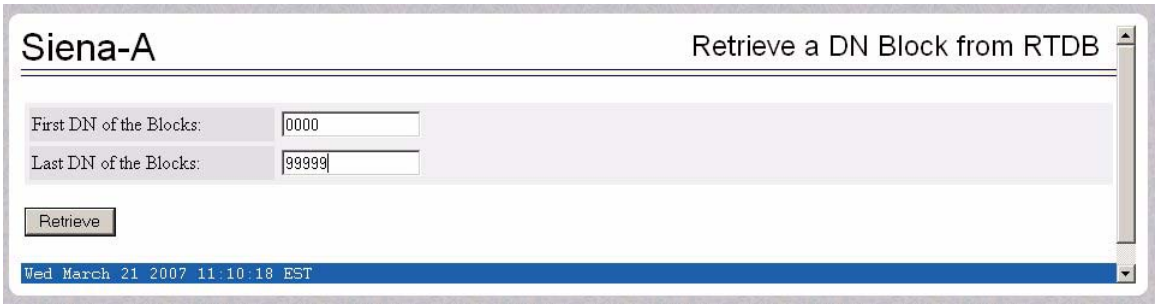
Figure 3-52. Output for Retrieve a DN from RTDB



DN Block

The RTDB / Retrieve Records / DN Block screen allows the user to retrieve information about about a DN block. See Figure 3-53.

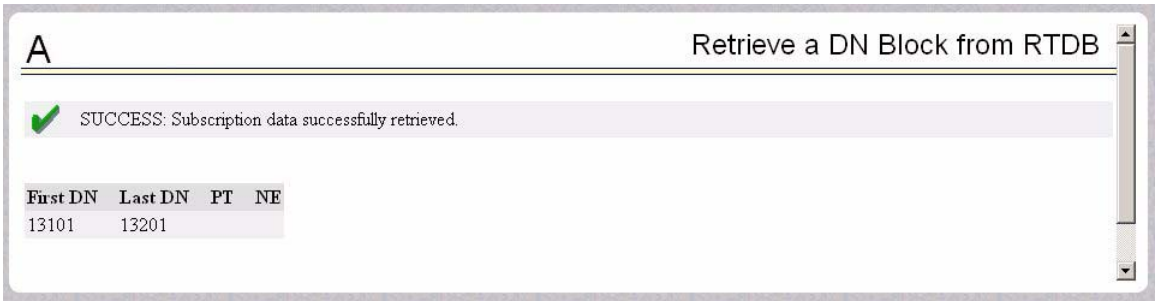
Figure 3-53. Retrieve DN Block Information from RTDB



The output displays the following information about a DN block, as shown in Figure 3-54:

- First DN
- Last DN
- Portability type (PT)
- Associated SP (Signaling Point) or RN (Routing Number)
- Network Entity (NE) data, as described in “Network Entity” on page 3-43, if the DN Block being retrieved is associated with an NE.

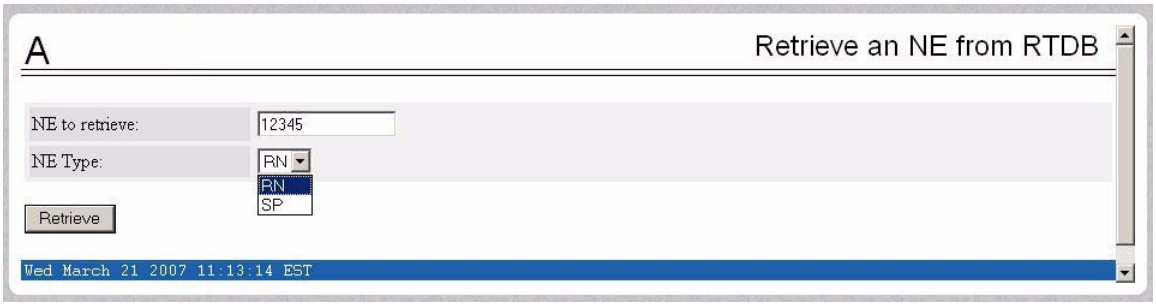
Figure 3-54. Output for Retrieve a DN Block from RTDB



Network Entity

The RTDB / Retrieve Records / Network Entity screen allows the user to retrieve information about a network entity. See Figure 3-55.

Figure 3-55. Retrieve an NE from RTDB



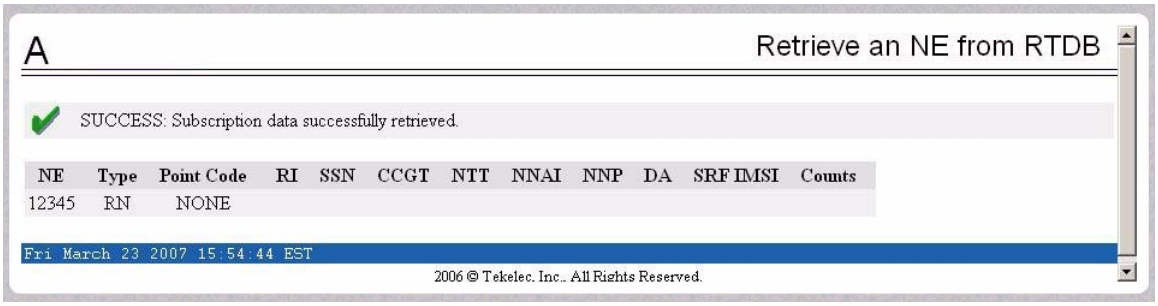
The output displays the following information about a network entity, as shown in Figure 3-56 and Figure 3-57:

- ID
- Type (RN or SP)
- Point code
- Routing indicator (RI)
- Subsystem number (SSN)
- Cancel Called Global Title (CCGT)
- New Translation Type (NTT)
- New Nature of Address Indicator (NNAI)

- New Numbering Plan (NNP)
- Digit Action (DA)
- SRF IMSI (Signaling Relay Function International Mobile Subscriber Identity)
- DN Reference Count
- IMSI Reference Count

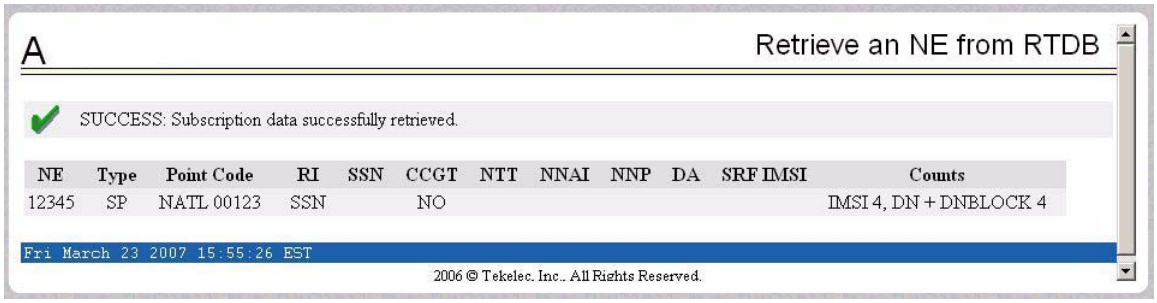
If the NE type is RN, the output displays the data shown in Figure 3-56.

Figure 3-56. Output for Retrieve an RN NE from RTDB



If the NE type is SP, the output displays the data shown in Figure 3-57.

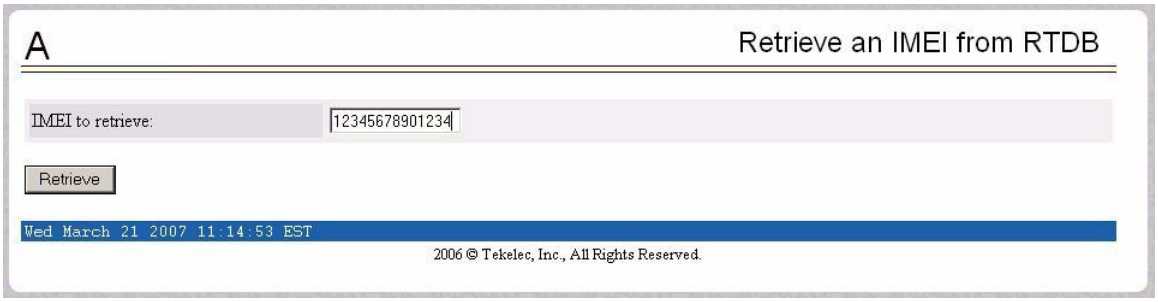
Figure 3-57. Output for Retrieve an SP NE from RTDB



IMEI

The RTDB / Retrieve Records / IMEI screen allows the user to retrieve information about a single IMEI (International Mobile Equipment Identity). See Figure 3-58.

Figure 3-58. Retrieve an IMEI from RTDB

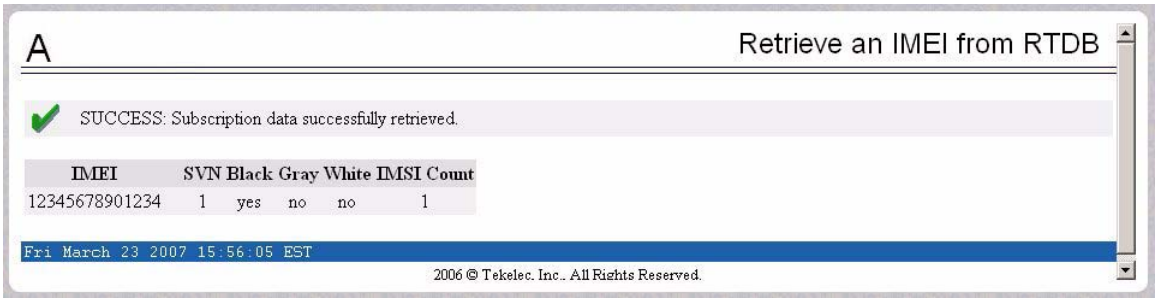


The output displays the following information about an IMEI, as shown in Figure 3-59:

- IMEI ID
- Software version (SVN)
- Black list indicator
- Gray list indicator
- White list indicator
- An IMSI reference count to show the number of IMSIs that are associated with an IMEI.

The IMEI lookup is performed on the IMEI blocks database when an IMEI is not present in the individual IMEI database.

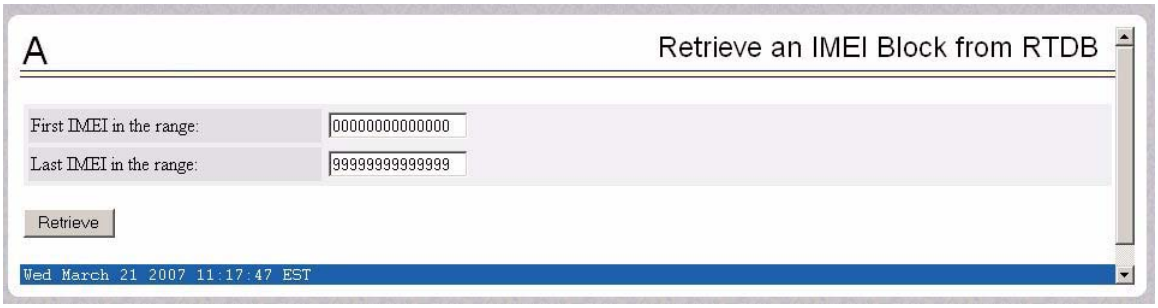
Figure 3-59. Output from Retrieve IMEI from RTDB



IMEI Block

The RTDB / Retrieve Records / IMEI Block screen allows the user to retrieve information about a single IMEI (International Mobile Equipment Identity) block. See Figure 3-60.

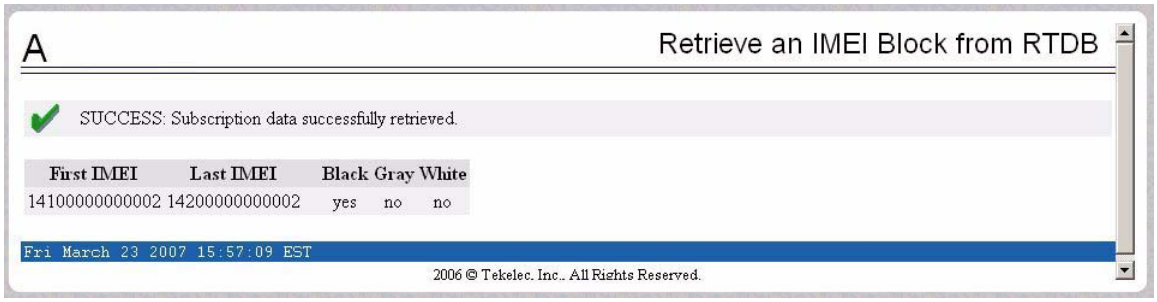
Figure 3-60. Retrieve an IMEI Block from RTDB



The output displays the following information about an IMEI block, as shown in Figure 3-61:

- First IMEI
- Last IMEI
- Black list indicator
- Gray list indicator
- White list indicator

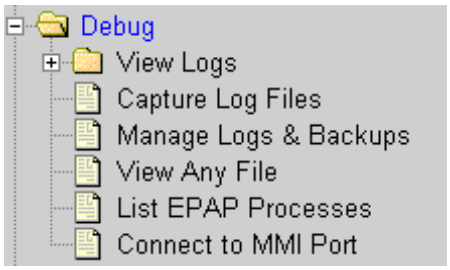
Figure 3-61. Output for Retrieve an IMEI Block from RTDB



Debug Menu

The Debug Menu allows the user to view logs, list running processes, and access the EAGLE 5 ISS MMI port. See the Debug Menu in Figure 3-62.

Figure 3-62. Debug Menu



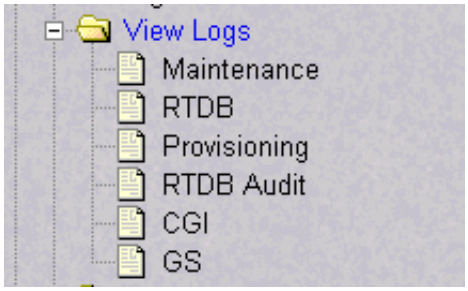
The Debug menu provides the following actions:

- "View Logs" on page 3-47
- "Manage Logs and Backups" on page 3-51
- "Manage Logs and Backups" on page 3-51
- "View Any File" on page 3-52
- "List EPAP Software Processes" on page 3-53
- "Connect to EAGLE 5 ISS MMI Port" on page 3-54

View Logs

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 3-63.

Figure 3-63. Debug / View Logs Menu



The View Logs menu provides the following actions:

- Maintenance Log
- RTDB Log
- Provisioning Log
- RTDB Audit Log
- CGI Log
- GS Log

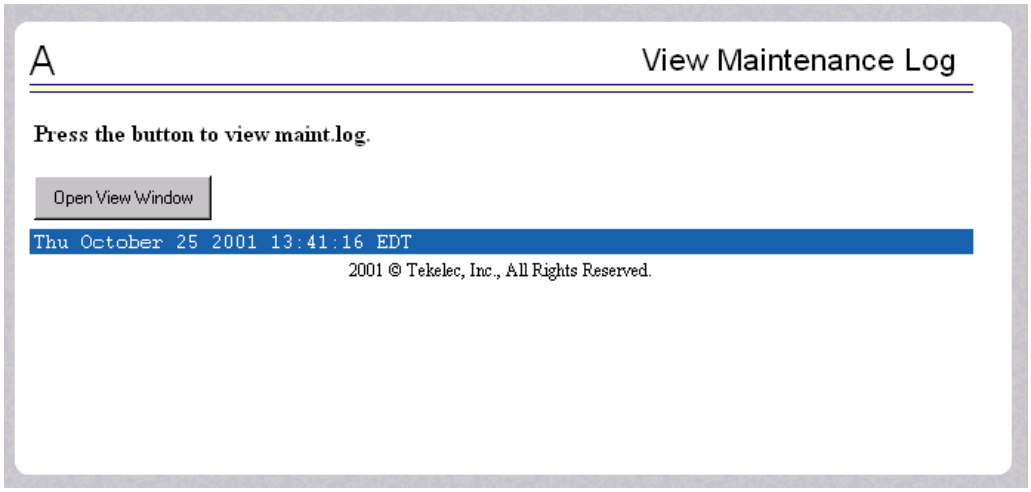
When any of the Debug / View Logs files are chosen, the process is the same. The chosen selection causes a screen similar to the View Maintenance Log screen in Figure 3-64. Press the Open View Window button to activate the View Window viewer for the log file you have selected in the View Logs menu.

Opening any log in this window displays the requested log in the log viewer window. All log view screens require an authorized login and password. All log files are viewed with the EPAP Log Viewer utility.

EPAP Log Viewer

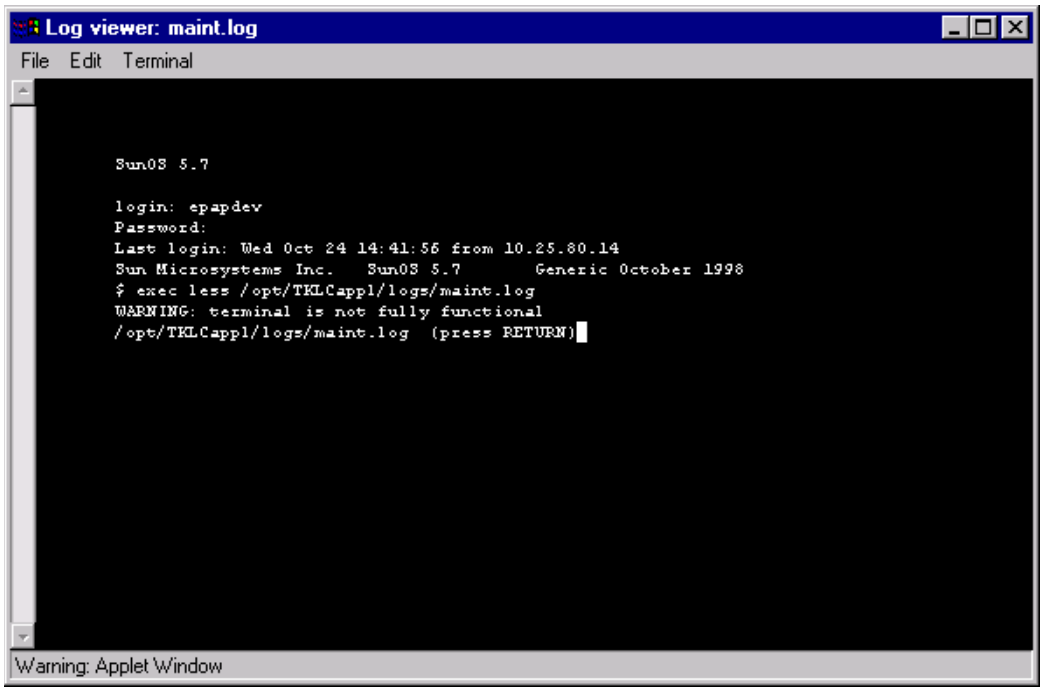
Viewing any log file involves using the Log Viewer. Menu options using the log viewer first display a request screen in the workspace, shown in Figure 3-65.

Figure 3-64. 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 3-65 for a sample Log Viewer window.

Figure 3-65. Log Viewer Window Example



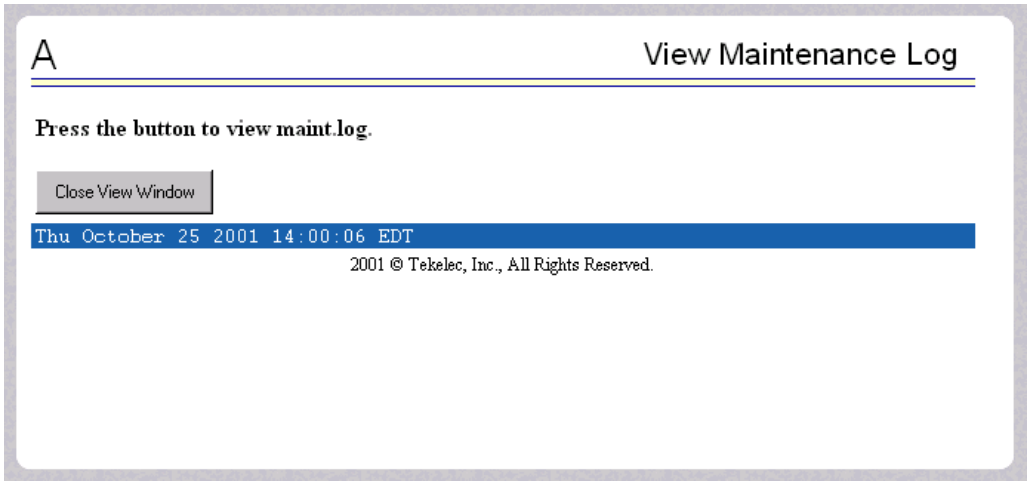
Use the log viewer navigation commands in Table 3-2 to navigate through the file displayed by the log viewer:

Table 3-2. 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 3-66.

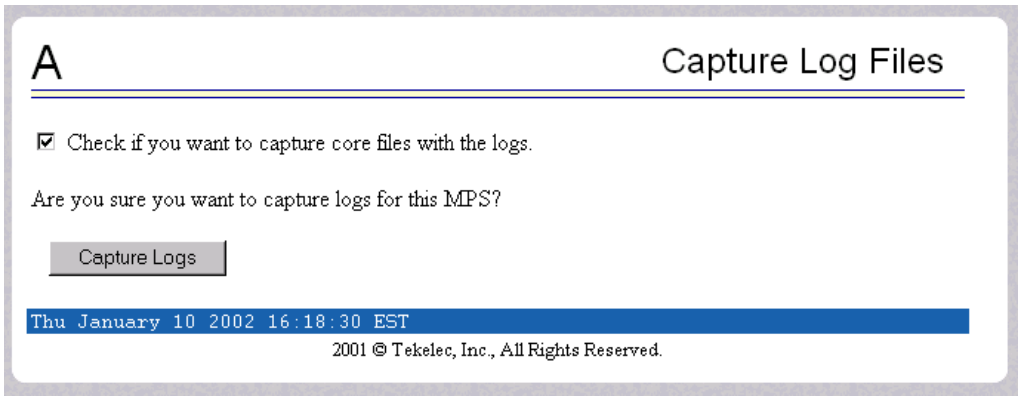
Figure 3-66. Closing the Log Viewer Window



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. See Figure 3-67 for the Capture Log Files screen.

Figure 3-67. Capture Log Files



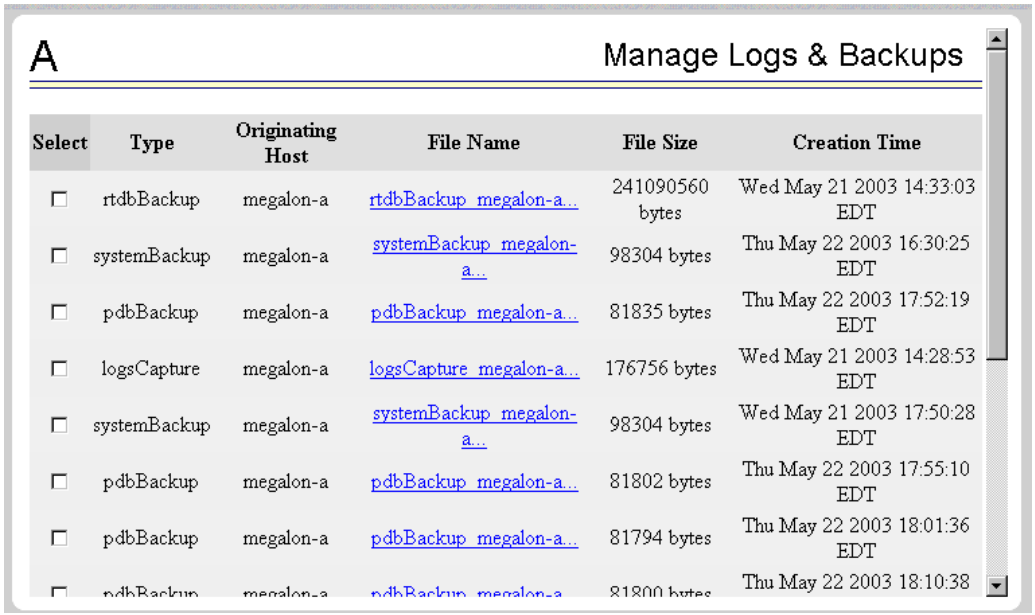
When you click the Capture Logs button, the copy of the log files occurs, and a successful completion displays the message in Figure 3-68.

Figure 3-68. Example of Successfully Capturing Log Files

Manage Logs and Backups

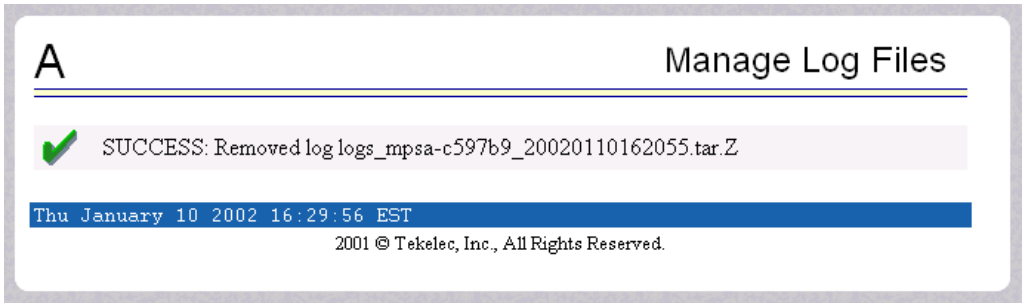
The Debug / Manage Logs and Backups displays the captured log files and allows the user to delete the copies no longer wanted or copy the selected file to the mate. See Figure 3-69 with an example of one recorded log file on the Manage Log Files screen.

Figure 3-69. Manage Log Files



In the Manage Log Files screen, you can remove a log file by clicking the Delete? button and then the Delete Selected Capture File button. A successful removal message appears in Figure 3-70.

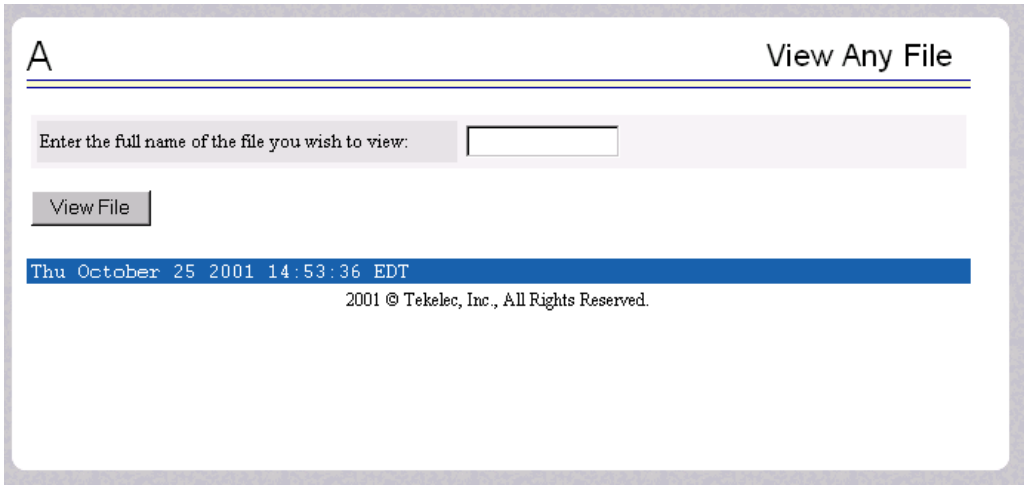
Figure 3-70. Example of Successfully Deleting a Log File



View Any File

The 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 3-71.

Figure 3-71. View Any File Screen

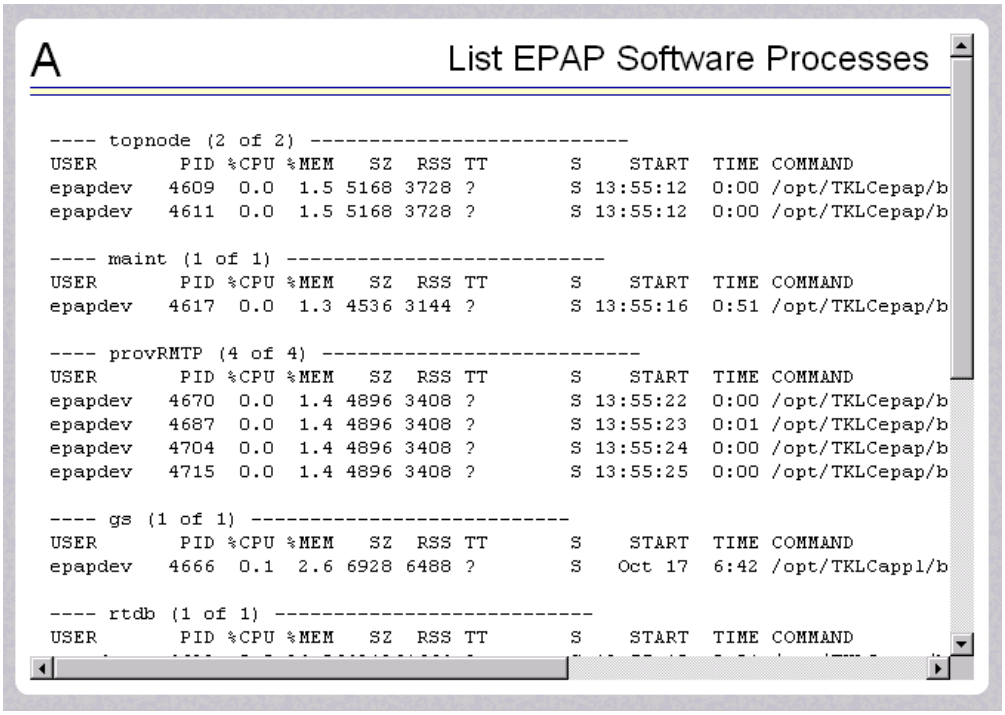


Opening any file in this window displays the requested file in the file viewer window. All files are viewed with the same file viewing utility. For details about this utility, see “Platform Menu” on page 3-56.

List EPAP Software Processes

The Debug / List EPAP Software Processes screen shows the EPAP processes started when the EPAP boots or with the "Start EPAP 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 3-72 shows an example of the format of the process list.

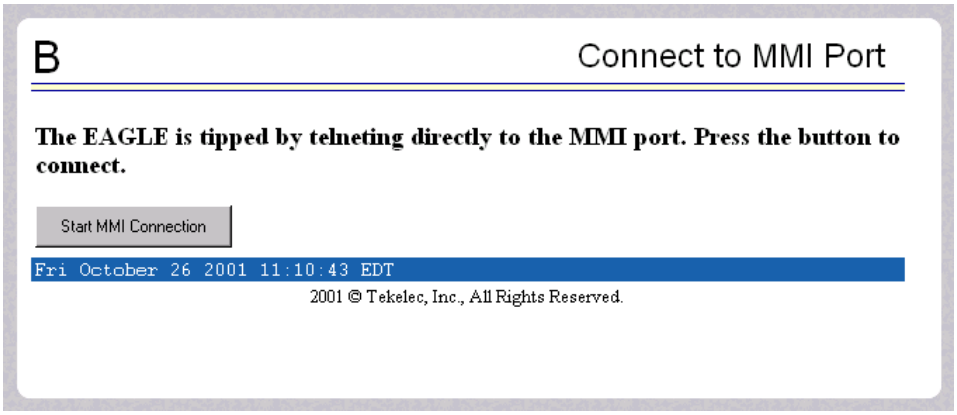
Figure 3-72. Example of View Any File



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 EPAP 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. The MMI connection requires an authorized login and password. Figure 3-73 shows the Connect to MMI Port screen.

Figure 3-73. Connect to MMI Port Screen



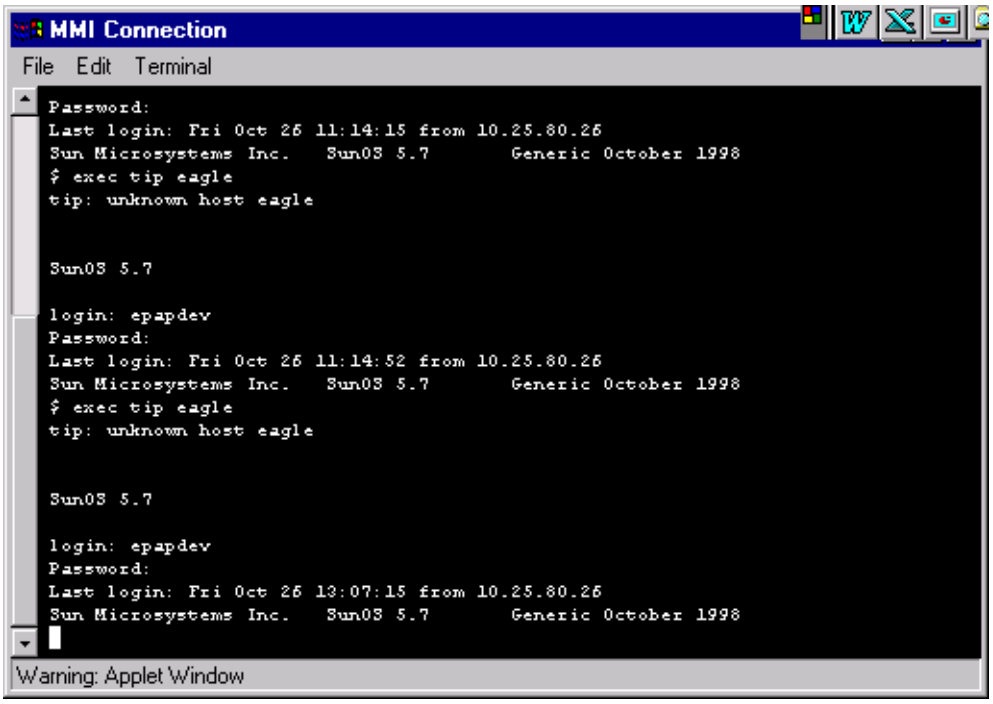
Press the Start MMI Connection button, and the SSH User Authentication window appears. Enter the User name (epapdev) and password to connect. Figure 3-74 has an example of the SSH User Authentication screen.

Figure 3-74. 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.

See Figure 3-75 for an example of the MMI window.

Figure 3-75. MMI Connection Window

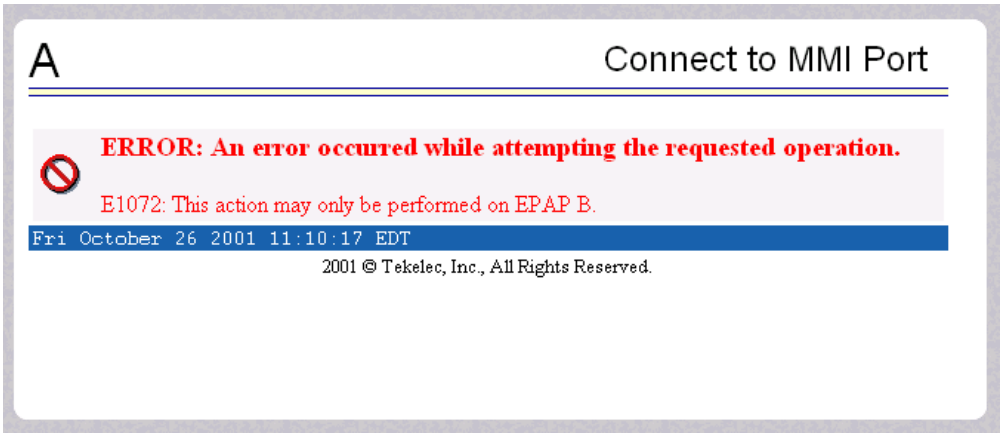


The window starts a **tip** session during which EAGLE 5 ISS commands can be issued. The session can be chosen by:

- 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 EPAP B, and you can connect to the port only when you are on EPAP B. If you were to forget and attempt to perform this command from EPAP A, you see the error screen in Figure 3-76.

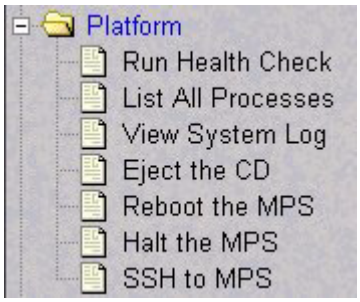
Figure 3-76. Attempting to Connect to MMI Port from EPAP A



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 Figure 3-77.

Figure 3-77. Platform Menu



The Platform menu provides these actions:

- "Run Health Check" on page 3-57
- "List All Running Processes" on page 3-59
- "View System Log" on page 3-60
- "Eject the CD" on page 3-61
- "Reboot the MPS" on page 3-62

- "Halt the MPS" on page 3-63
- "SSH to MPS" on page 3-65

Run Health Check

The Platform / Run Health Check screen allows the user to execute the health check routine on the selected EPAP. The *MPS Platform Software and Maintenance Manual* describes the health check (also called System Health Check Procedure) in detail.

The first screen presented in the workspace frame lets the user select the "normal" or "verbose" mode of output detail. Figure 3-78 shows the Run Health Check screen that begins the execution of this diagnostic tool.

Figure 3-78. Run Health Check Screen

The EPAP 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 *MPS Platform Software and Maintenance Manual*, System Health Check, for the functions performed and how to interpret the results of the normal outputs (Figure 3-79) and verbose outputs (Figure 3-80).

Figure 3-79. Normal Health Check Output

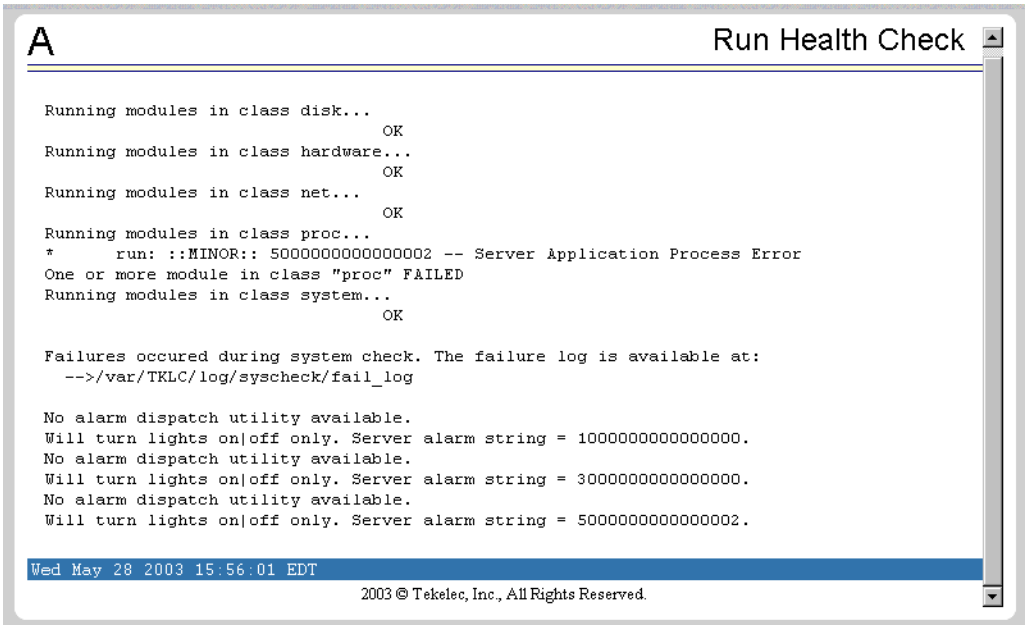
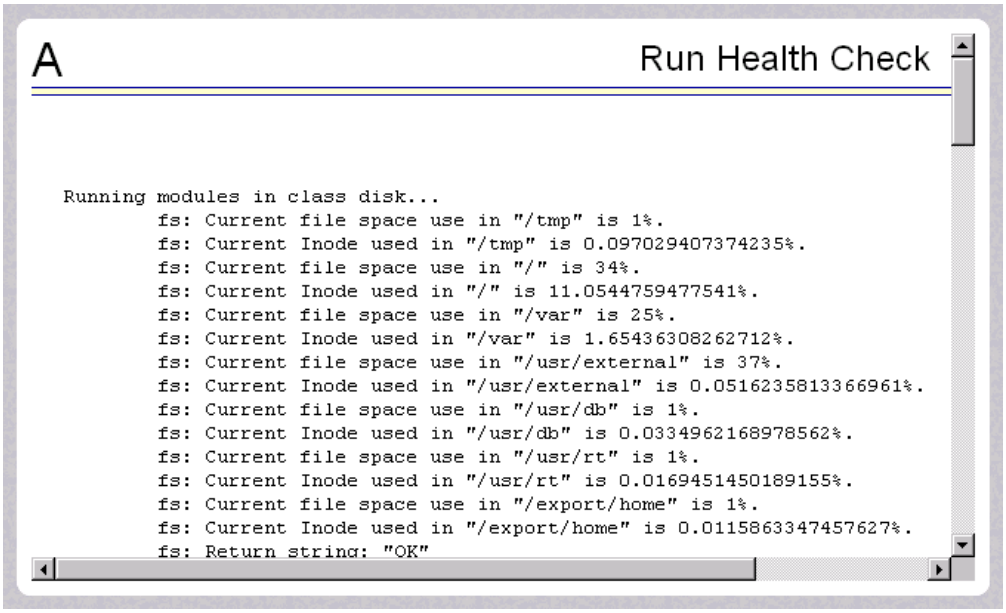


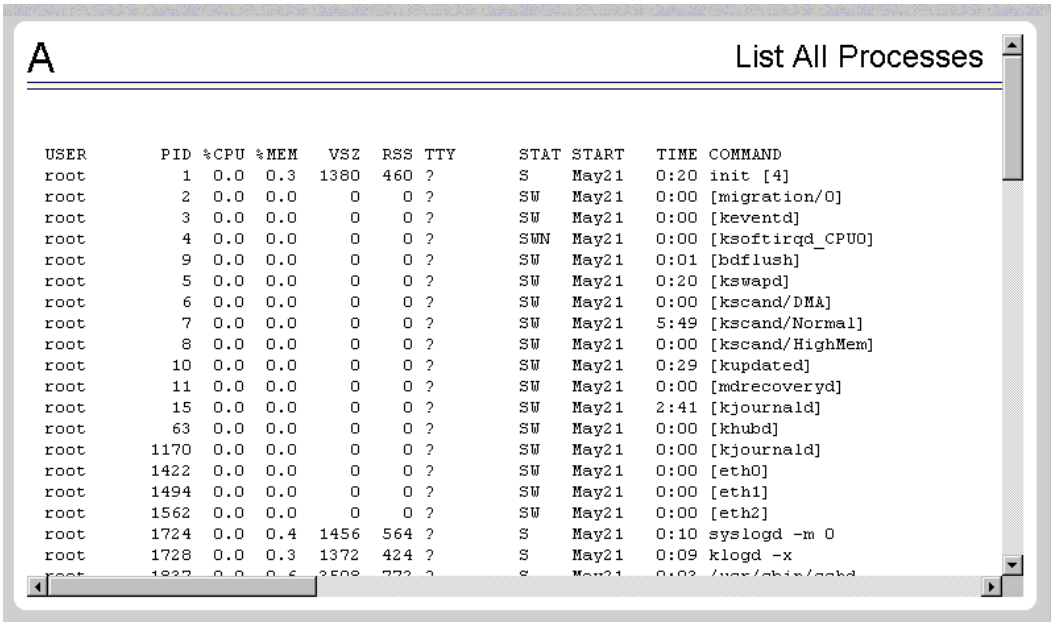
Figure 3-80. Portion of Verbose Health Check Output



List All Running Processes

The Platform / List All Running Processes screen lists all processes running on the selected EPAP. 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 3-81 shows an example of the process list.

Figure 3-81. List All Running Processes Screen

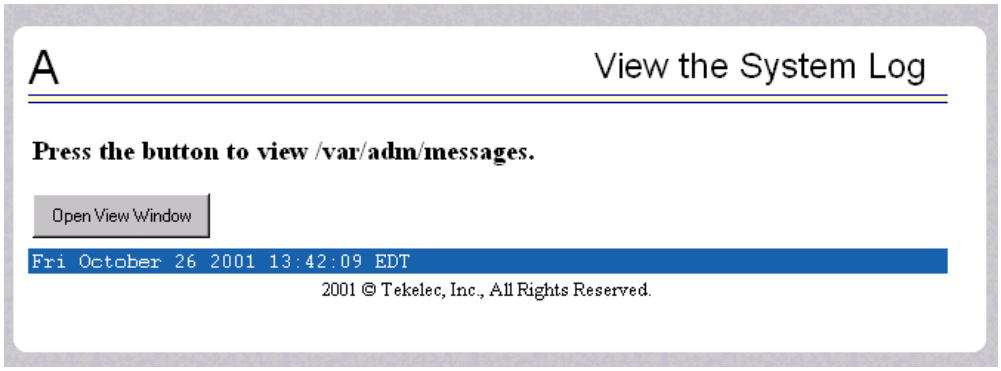


NOTE: The exact processes shown here will not be the same on your EPAP servers. The output from this command is unique for each EPAP, depending on the EPAP software processes, the number of active EPAP user interface processes, and other operational conditions.

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 3-82.

Figure 3-82. 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 "Platform Menu" on page 3-56.) See Figure 3-83 for an example of the System Log output.

Figure 3-83. 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 user to eject the CD on the selected EPAP server. Figure 3-84 shows the Eject CD screen.

Figure 3-84. Eject CD Screen

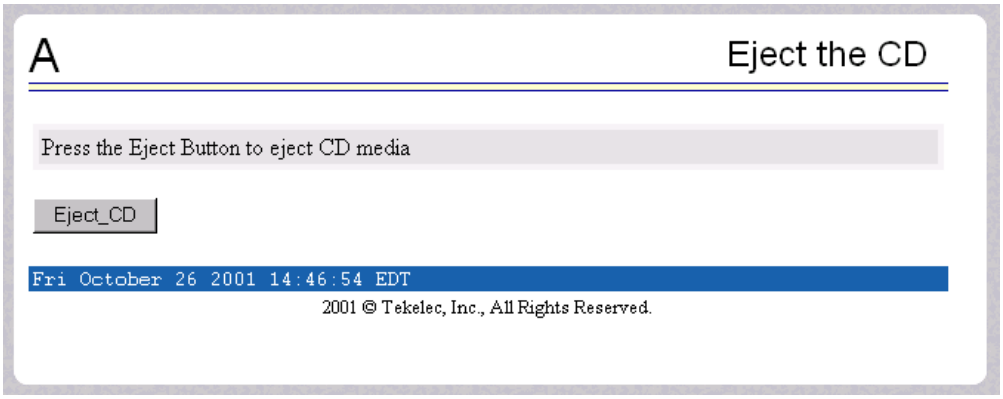
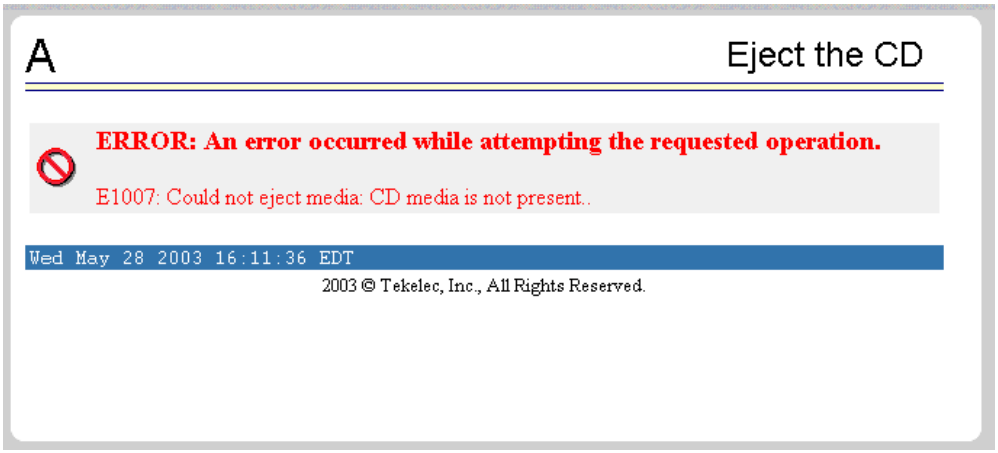


Figure 3-85 shows an example of an error reporting that CD media is missing.

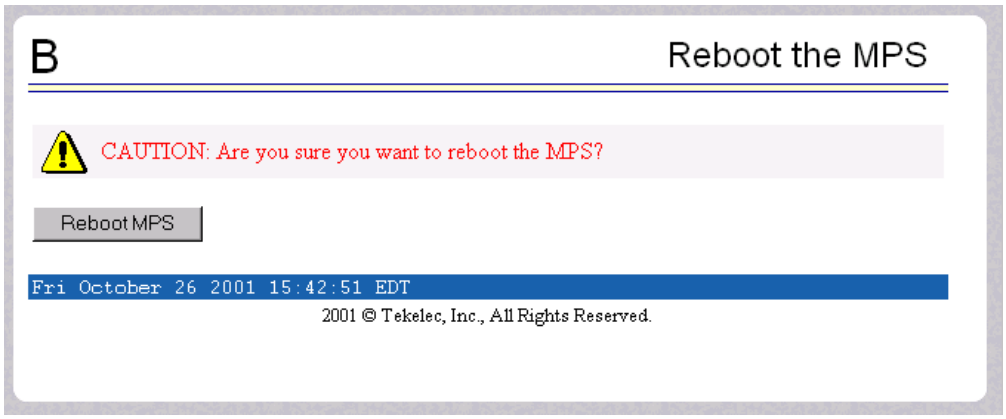
Figure 3-85. Eject CD Screen Error Message



Reboot the MPS

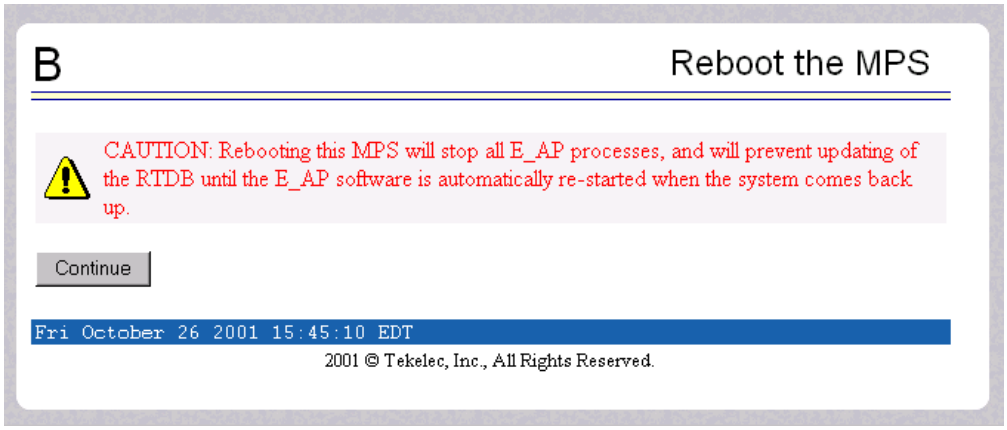
The Platform / Reboot the MPS screen allows the user to reboot the selected EPAP. All EPAP software processes running on the selected EPAP are shut down normally. Figure 3-86 shows the Reboot the MPS screen.

Figure 3-86. Reboot the MPS Screen



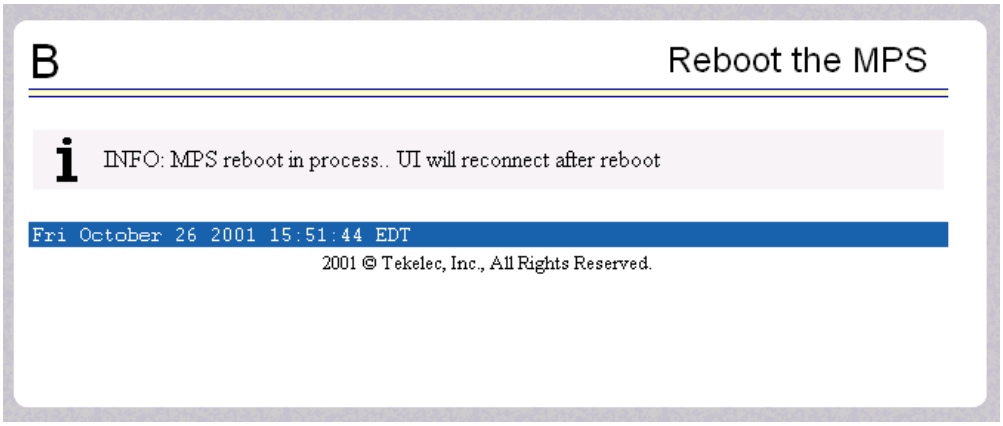
When you click the Reboot MPS button, a cautionary message appears, informing the user that this action instructs EPAP to stop all activity and to prevent the RTDB from being updated with new subscriber data. See Figure 3-87.

Figure 3-87. 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 3-88.

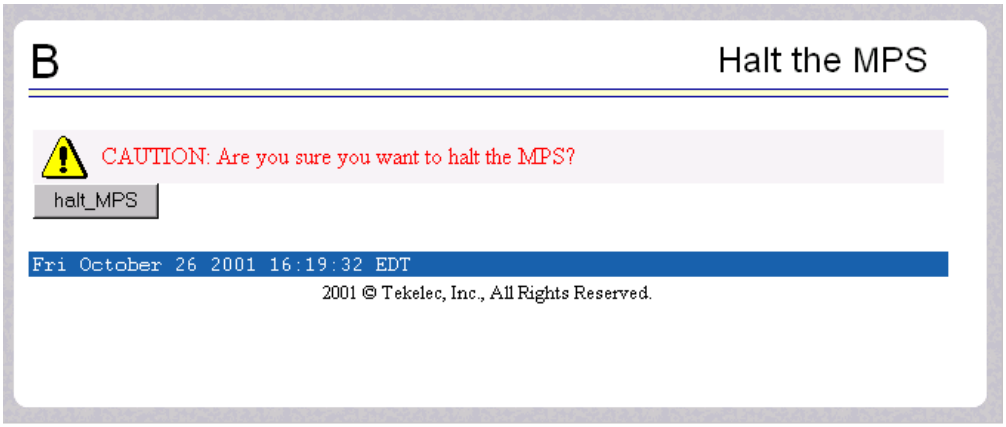
Figure 3-88. Rebooting the MPS in Process



Halt the MPS

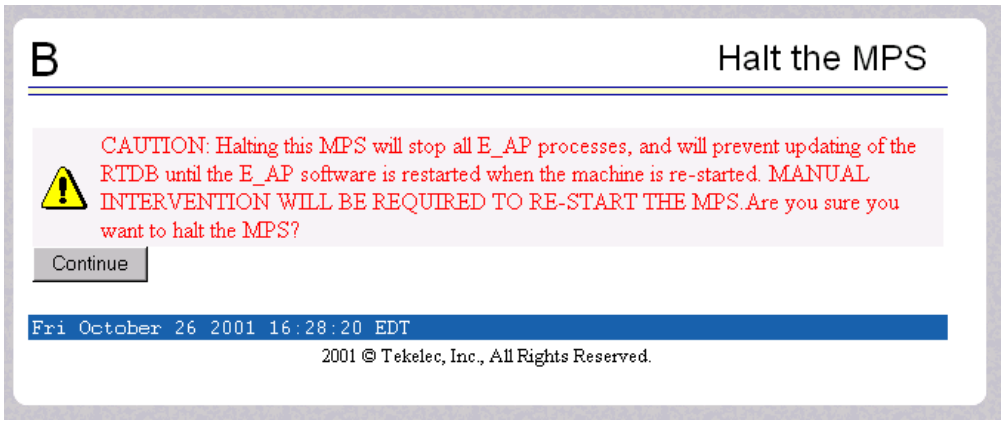
The Platform / Halt the MPS screen allows the user to halt the selected EPAP. All EPAP software processes running on the selected EPAP are shut down normally. Figure 3-89 shows the Halt the MPS screen.

Figure 3-89. Halt the MPS Screen



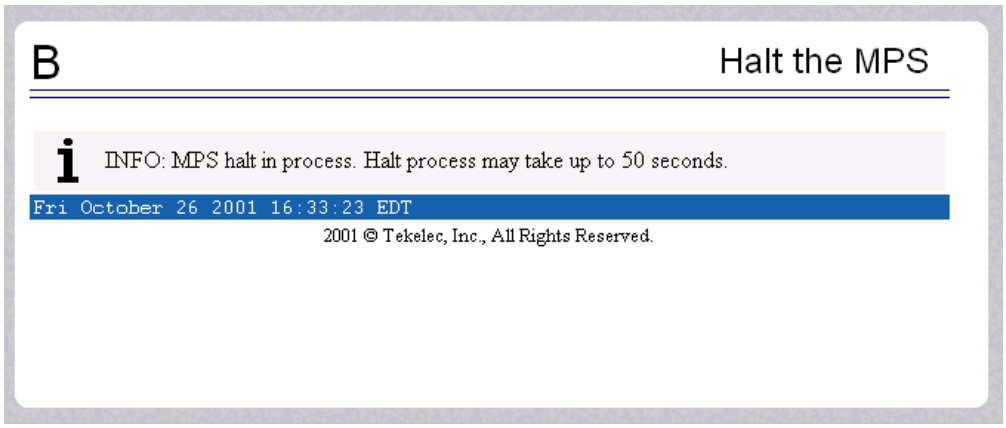
To perform this action, click the halt_MPS button. Next a cautionary message appears, informing the user that this action instructs EPAP to stop all activity and to prevent the RTDB from being updated with new subscriber data. See Figure 3-90.

Figure 3-90. 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 Figure 3-91.

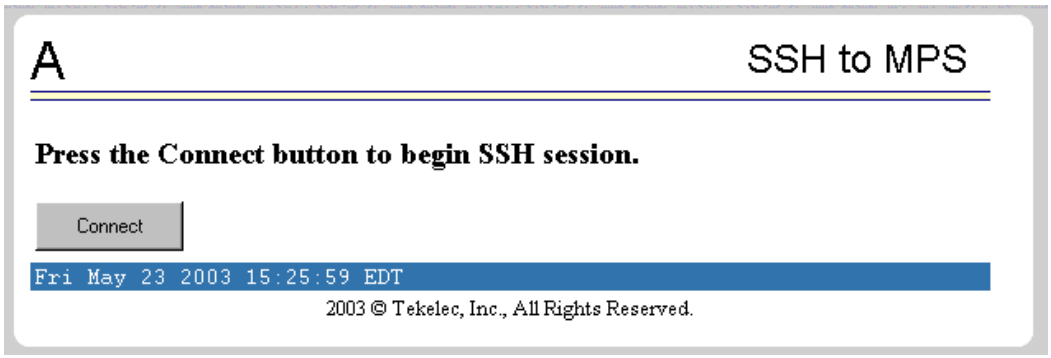
Figure 3-91. Rebooting the MPS in Process



SSH to MPS

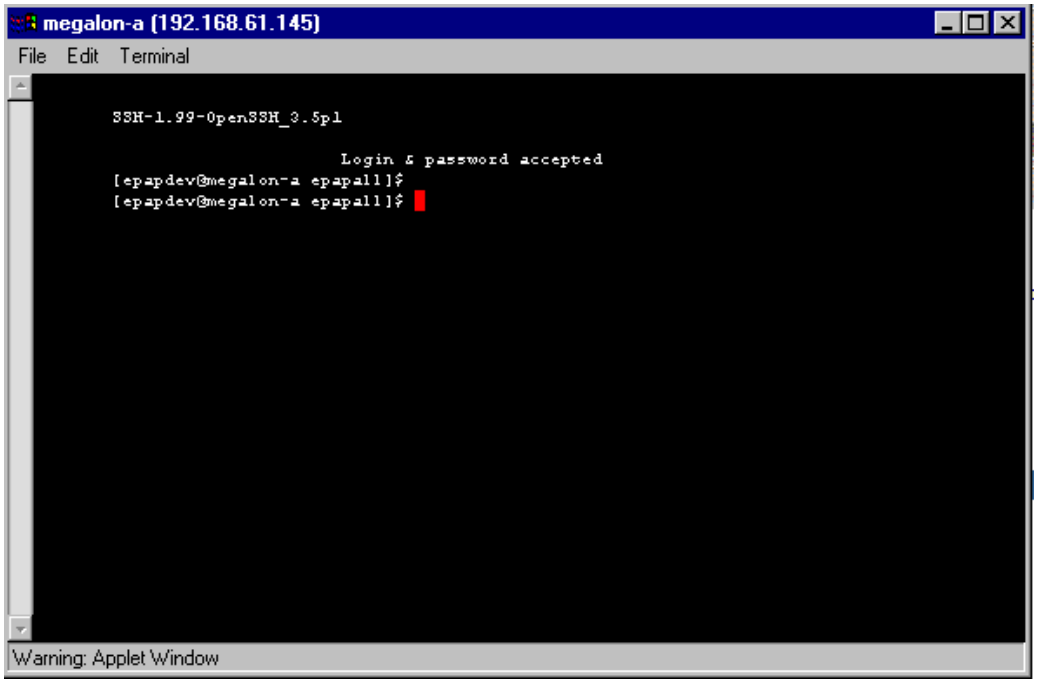
The Platform / SSH to MPS screen allows the user to have a **SSH** window to the user interface user. Clicking on the Connect button, shown in Figure 3-92, opens the SSH User Authentication window. A user name and Password word are required to login.

Figure 3-92. SSH to MPS Screen



After a successful login, the **SSH** window opens and is used to perform **SSH** communications. the screen is shown in Figure 3-93.

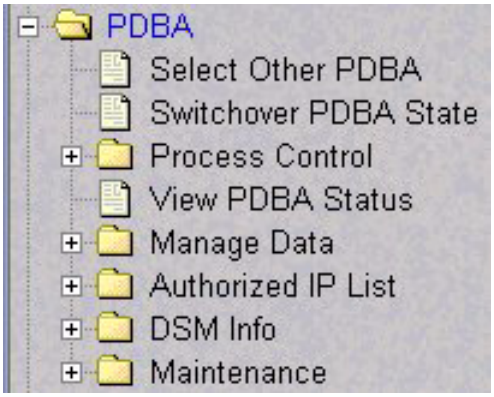
Figure 3-93. Example of a SSH Window



PDBA Menu

The PDBA (Provisioning Database Administration) menu allows the user to maintain and modify the PDBA. The user sees this menu only on EPAP A. See the PDBA menu in Figure 3-94.

Figure 3-94. Provisioning Database Administration Menu



The PDBA menu provides the control, management, and maintenance of the Provisioning Database Administration facility. This menu provides the following functions:

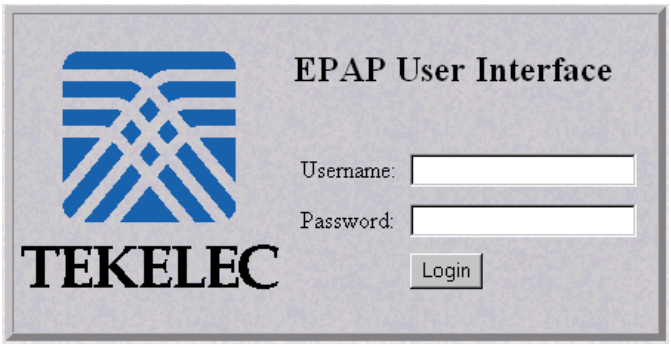
- "Select Other PDBA" on page 3-67
- "Switchover PDBA Status" on page 3-67
- "Process Control" on page 3-68
- "View PDBA Status" on page 3-70
- "Manage Data" on page 3-73
- "Authorized IP List" on page 3-105
- "DSM Info" on page 3-111
- "PDBA / Maintenance" on page 3-113

Select Other PDBA

The PDBA / Select Other PDBA is an action performed from the PDBA menu screen (see Figure 3-94). It provides access to the remote PDBA GUI.

Access the user interface on the remote PDBA. When the action is successful, you see the logon screen of the remote PDBA pair, on which you can log in to the remote EPAP. See Figure 3-95.

Figure 3-95. EPAP UI Login Screen

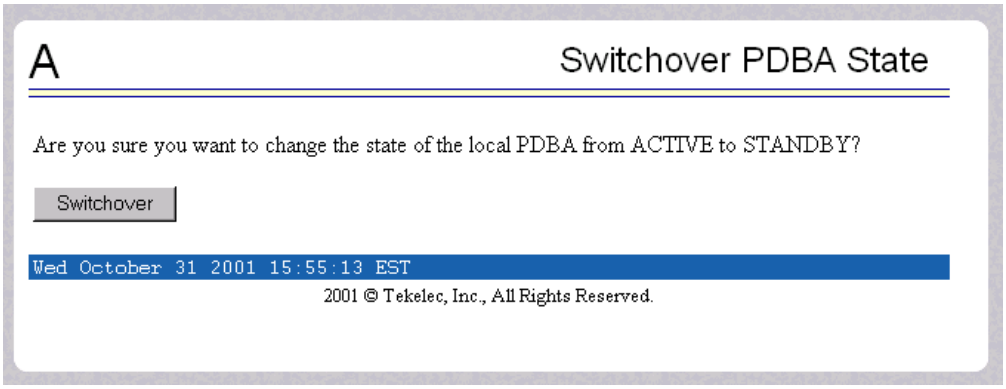


From this screen, you sign on and perform the PDBA actions that you want from the remote PDBA.

Switchover PDBA Status

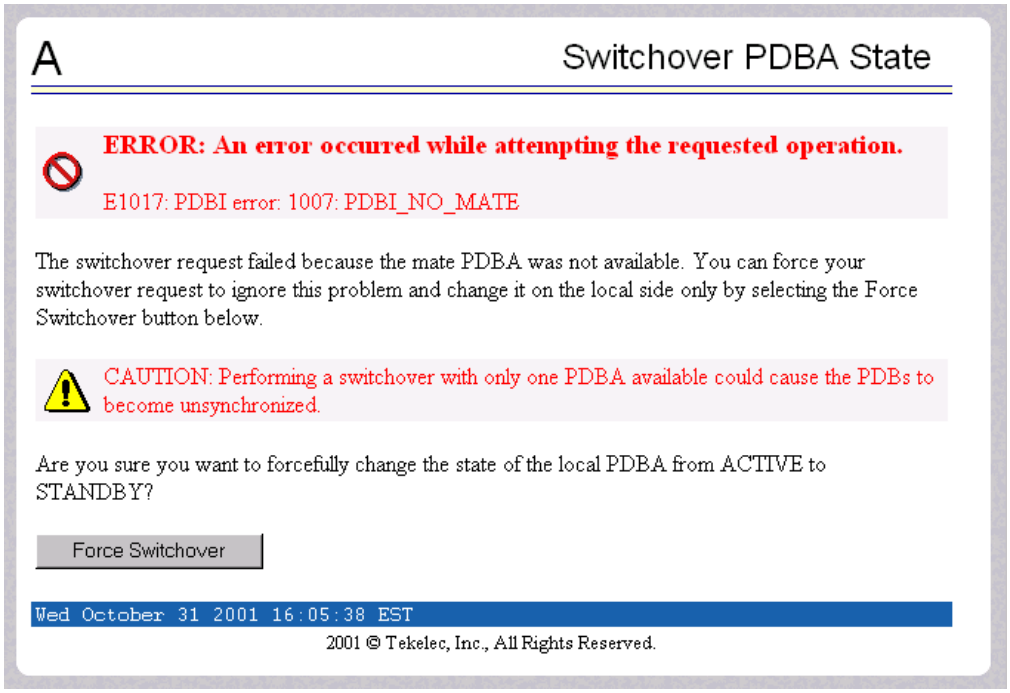
The PDBA / Switchover PDBA Status screen lets you switch the active and standby PDBAs. (This action toggles the states from one state to the other.) When you choose the Select Other PDBA menu item, a screen requires you to confirm the switchover from the Active to the Standby PDBA, or the reverse. See the Switchover PDBA Status screen in Figure 3-96.

Figure 3-96. Switchover PDBA Status Screen



Notice that if only one PDBA is available, you are warned that the action can cause synchronization problems. See the error displayed in the Switchover PDBA Status screen in Figure 3-97.

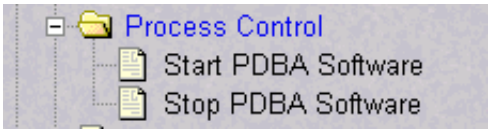
Figure 3-97. Error in Switching a PDBA State



Process Control

The PDBA / Process Control menu lets you to start and stop the PDBA application, shown in Figure 3-98.

Figure 3-98. Process Control Menu



The PDBA / Process Control menu provides these actions:

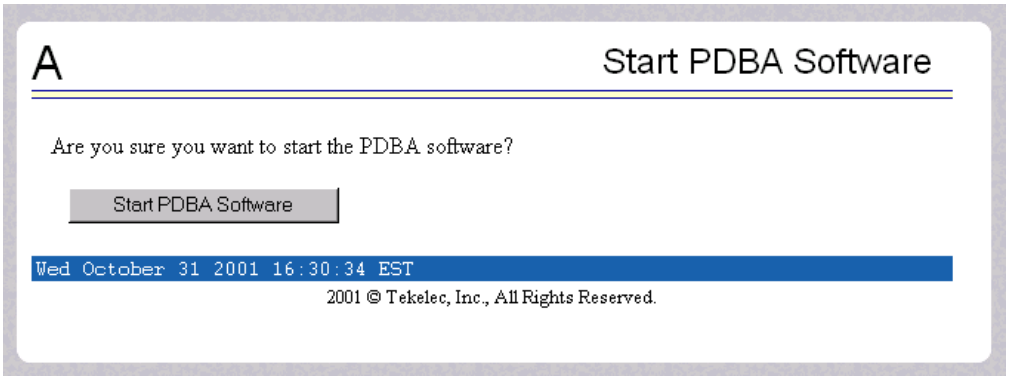
- "Start PDBA Software" on page 3-68
- "Stop PDBA Software" on page 3-69

Start PDBA Software

The PDBA / Process Control / Start PDBA Software screen begins the execution of the PDBA software. When you click the Start PDBA Software button, the EPAP attempts to start the software. Starting the PDBA software from this menu item

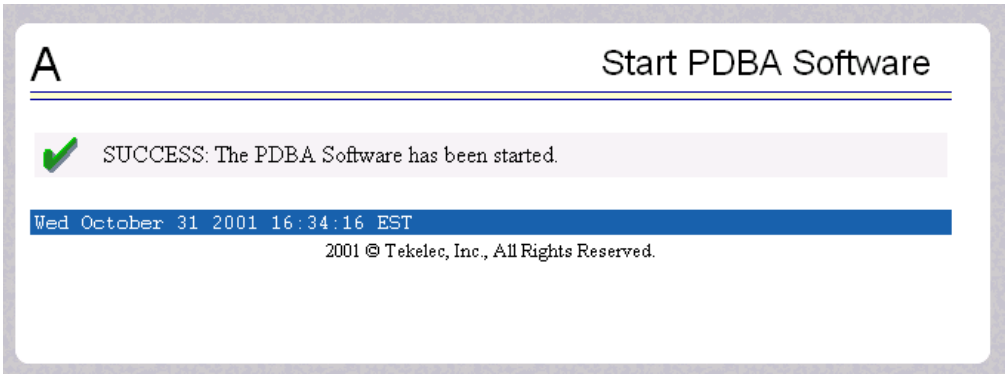
also clears the indicator that keeps the software from being automatically started on a reboot (refer to "Stop PDBA Software" on page 3-69). See Figure 3-99 for the Start PDBA Software screen.

Figure 3-99. Start PDBA Software Screen



When you choose the Start PDBA Software screen, another screen requires to confirm your choice to start the PDBA software. Click the Start PDBA Software button, and see the confirmation shown in Figure 3-100.

Figure 3-100. Success in Starting PDBA Software

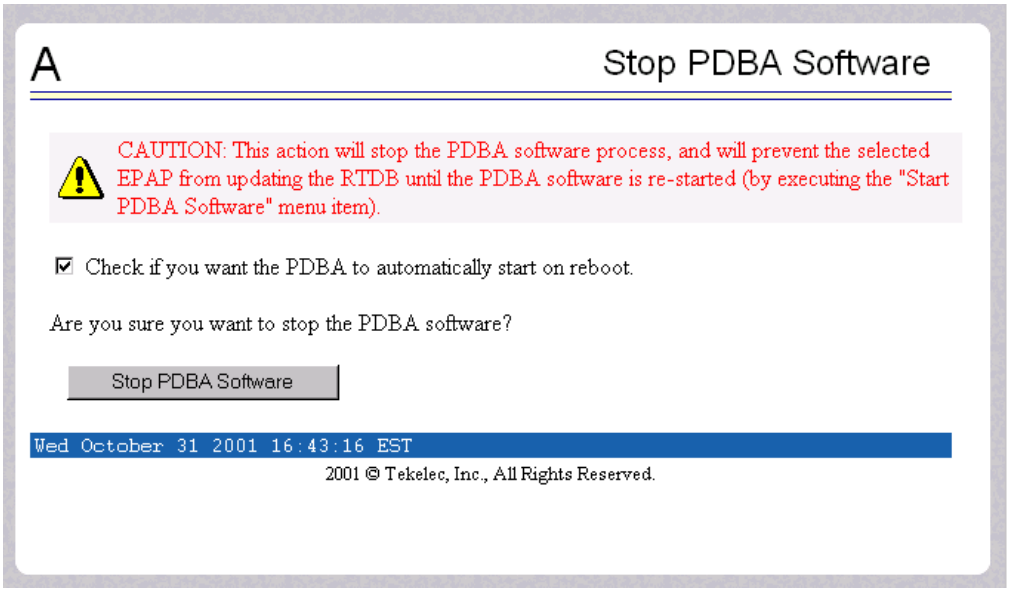


Stop PDBA Software

The PDBA / Process Control / Stop PDBA Software screen stops the PDBA software when you click the Stop PDBA Software button.

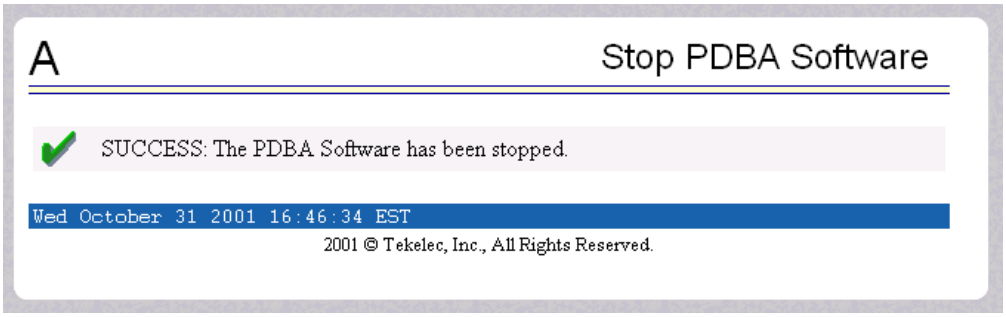
The screen also has a checkbox that lets you specify whether PDBA is to be automatically restarted when the machine boots. If you clear this checkbox, the only way to restart the software is via the Start PDBA menu. See Figure 3-101 for the Stop PDBA Software screen.

Figure 3-101. Stop PDBA Software Screen



When you choose the Stop PDBA Software screen, another screen shows the successful stopping of the PDBA, shown in Figure 3-102.

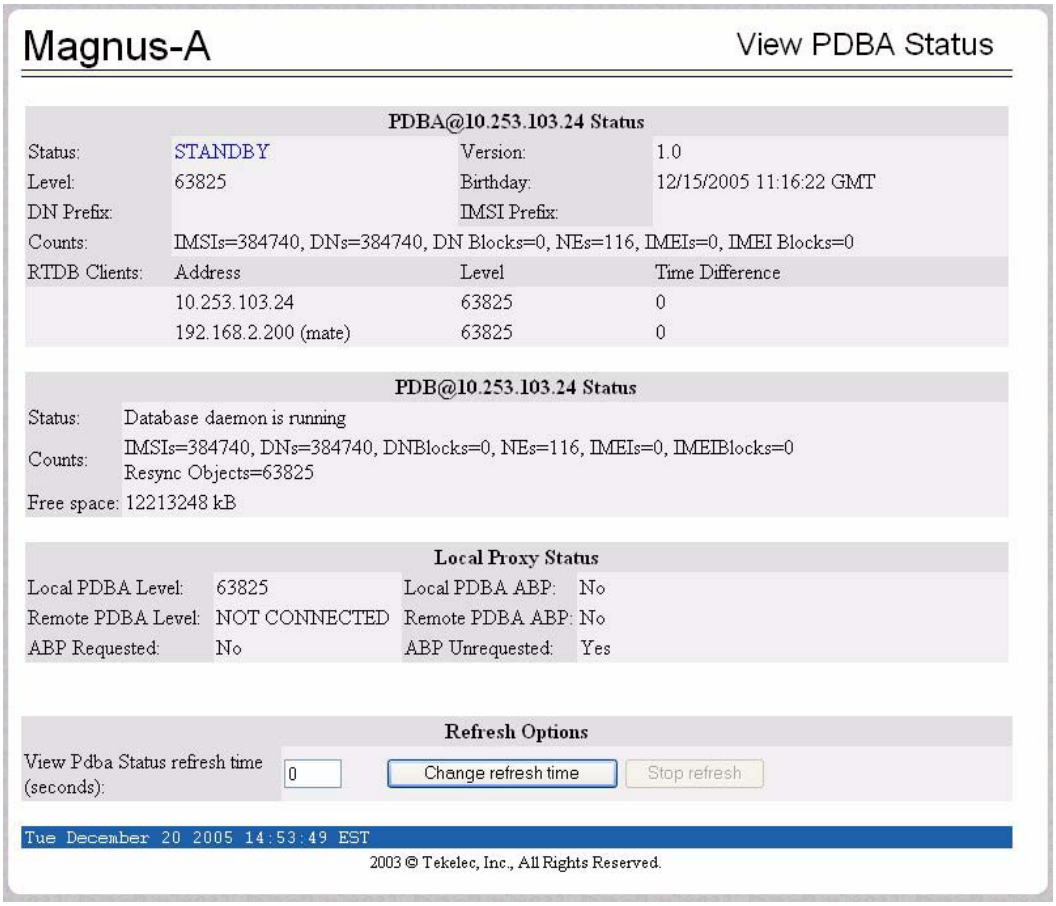
Figure 3-102. Success in Stopping PDBA Software



View PDBA Status

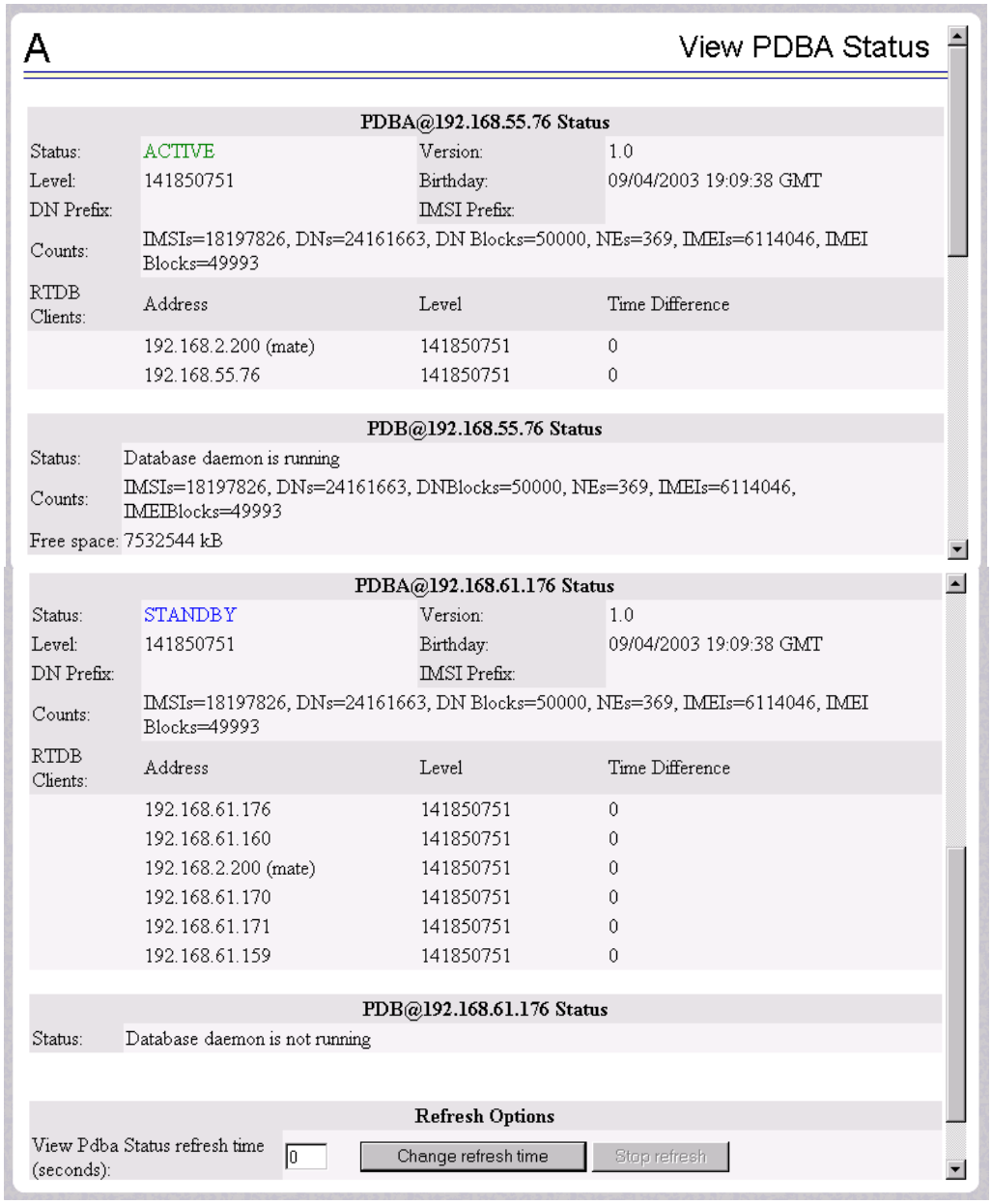
The PDBA / View PDBA Status screen is used to display the current status of the selected PDBA. The PDBA Status refresh time can be viewed and changed with this screen. See two examples of the PDBA the View PDBA Status screen in Figure 3-103 and Figure 3-104..

Figure 3-103. View PDBA Status Screen



NOTE: The Local Proxy Status items only appear if the PDBA Proxy feature is enabled.

Figure 3-104. View PDBA Status Screen

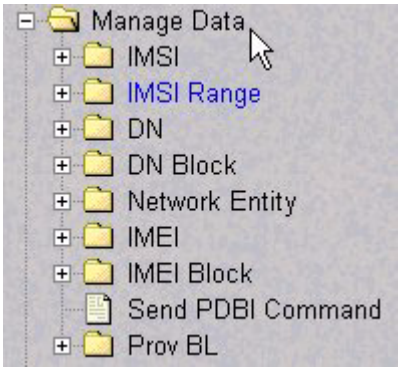


NOTE: The IMSI count returned from the RTDB and the IMSI count returned from the PDB may not match when there is both G-Flex and EIR data. Any IMSI created for EIR that does not have a G-Flex IMSI association is not included in the IMSI counts of the PDB. The PDB reports only G-Flex IMSIs. The RTDB reports the total of G-Flex and EIR IMSIs as one count.

Manage Data

The PDBA / Manage Data menu lets you add, update, delete, and view subscriptions in the Provisioning Database (PDB). See Figure 3-105.

Figure 3-105. Manage Data Menu



NOTE: Use this menu only for the emergency provisioning of individual subscriptions. This menu is not intended for provisioning large numbers of subscriptions. For normal provisioning activities, the user must create a separate provisioning application that communicates with the PDBA program.

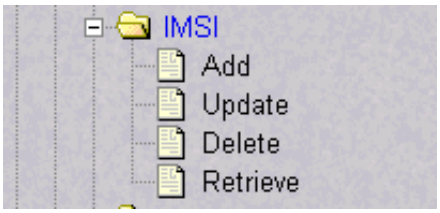
The PDBA / Manage Data menu provides these actions:

- "IMSI" on page 3-74
- "IMSI Range" on page 3-78
- "DN" on page 3-81
- "DN Block" on page 3-85
- "Network Entity" on page 3-89
- "Individual IMEI" on page 3-93
- "Block IMEI" on page 3-97
- "Send Raw PDBI Command" on page 3-101
- "EPAP Provisioning Blacklist Menu" on page 3-103

IMSI

The PDBA / Manage Data / IMSI menu is used to add, update, delete, and view subscription in the Provisioning Database (PDB). See Figure 3-106 for the IMSI menu.

Figure 3-106. IMSI Menu



The PDBA / Manage Data / IMSI menu provides these actions:

- "Add an IMSI" on page 3-74
- "Update an IMSI" on page 3-76
- "Delete an IMSI" on page 3-76
- "Retrieve an IMSI" on page 3-77

Add an IMSI

The PDBA / Manage Data / IMSI / Add an IMSI screen prompts you for the fields needed to add an IMSI to the Provisioning Database (PDB). If there is a conflicting subscription in the PDB, you are prompted to confirm before overwriting the existing subscription. See Figure 3-107 for an example of the Add IMSI screen.

Figure 3-107. Add an IMSI Screen

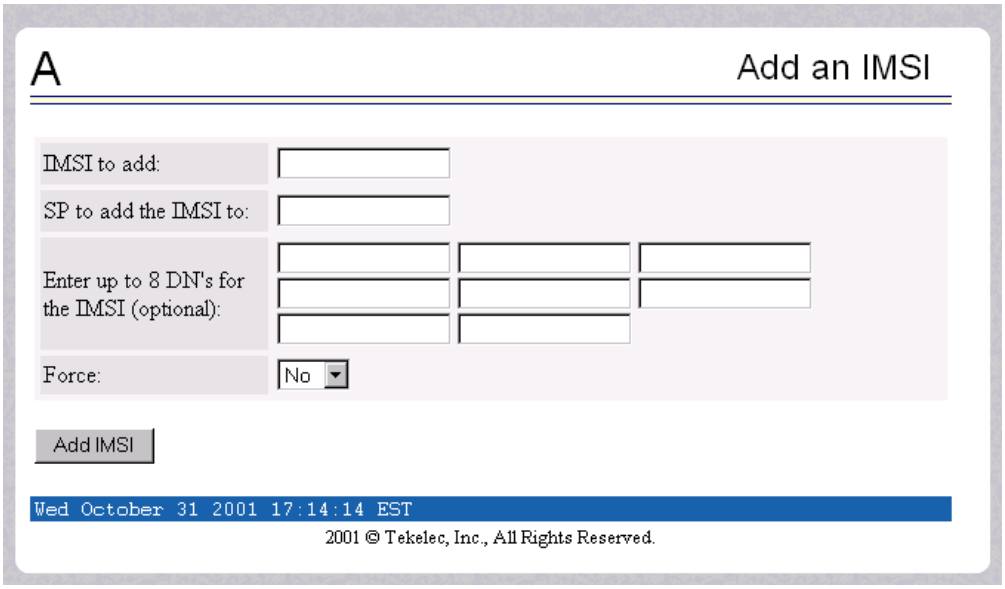
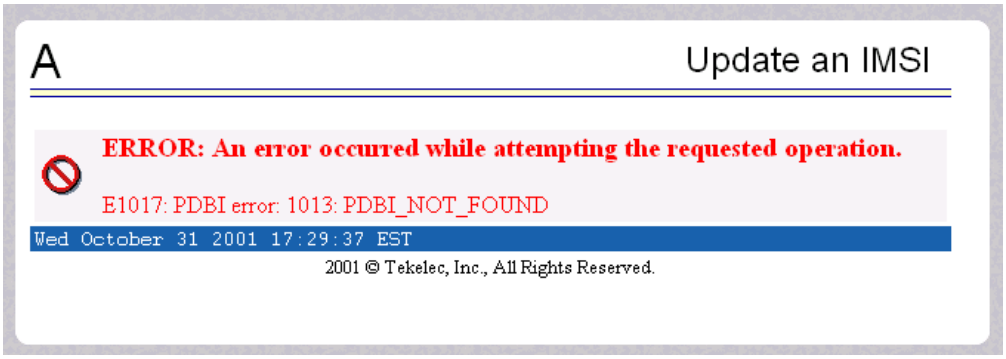


Figure 3-108 illustrates the error of no existing IMSI to update. It shows error E1017, resulting from not finding the specified IMSI number.

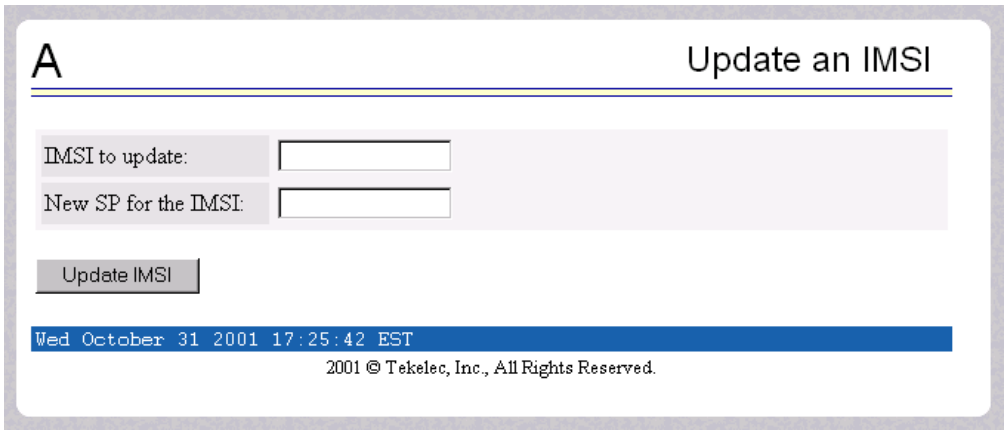
Figure 3-108. Error in Adding an IMSI



Update an IMSI

The PDBA / Manage Data / IMSI / Update IMSI screen prompts the user for the fields necessary to change the SP for an IMSI in the Provisioning Database (PDB). See Figure 3-109 for an example of the Update IMSI screen.

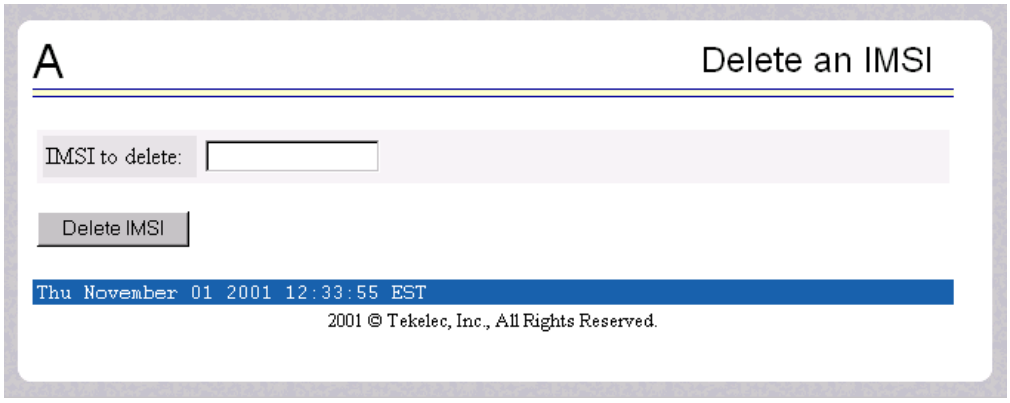
Figure 3-109. Update an IMSI Screen



Delete an IMSI

The PDBA / Manage Data / IMSI / Delete an IMSI screen prompts the user for the fields necessary to remove a subscription from the Provisioning Database (PDB). See Figure 3-110 for an example of the Delete an IMSI screen.

Figure 3-110. Delete IMSI Screen

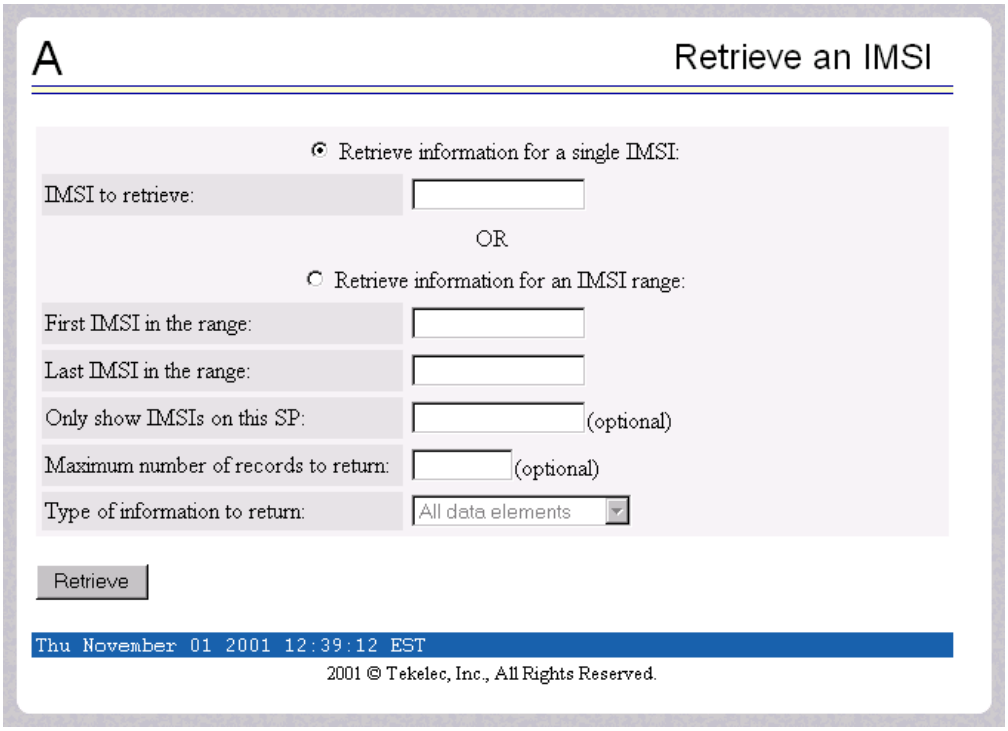


Retrieve an IMSI

The PDBA / Manage Data / IMSI / Retrieve an IMSI screen prompts you for the fields necessary to retrieve subscriptions from the Provisioning Database (PDB). If you specify the 'last IMSI', all subscriptions from the 'first IMSI' and 'last IMSI' are shown.

Figure 3-111 shows a sample output form the Retrieve IMSI menu action. The choices for the drop down menu for the Display field are: All data elements, Network entries only, and Record counts only. See Figure 3-111 for an example of the Retrieve an IMSI screen.

Figure 3-111. Retrieve IMSI Screen



IMSI Range

NOTE: The screens available under the IMSI Range Menu are only operational to SOG customers.

The PDBA / Manage Data /IMSI Range menu is used to add, update, delete, and view subscription in the Provisioning Database (PDB). See Figure 3-112 for the IMSI Range menu.

Figure 3-112. IMSI Range Menu

The PDBA / Manage Data / IMSI Range menu provides these actions:

- "Add an IMSI Range" on page 3-79
- "Update an IMSI Range" on page 3-79
- "Delete an IMSI Range" on page 3-80
- "Retrieve an IMSI Range" on page 3-80

Add an IMSI Range

The PDBA / Manage Data / IMSI Range / Add an IMSI Range screen prompts you for the fields needed to add an IMSI range to the Provisioning Database (PDB). See Figure 3-113 for an example of the Add IMSI Range screen.

NOTE: This screen is only operational to SOG customers.

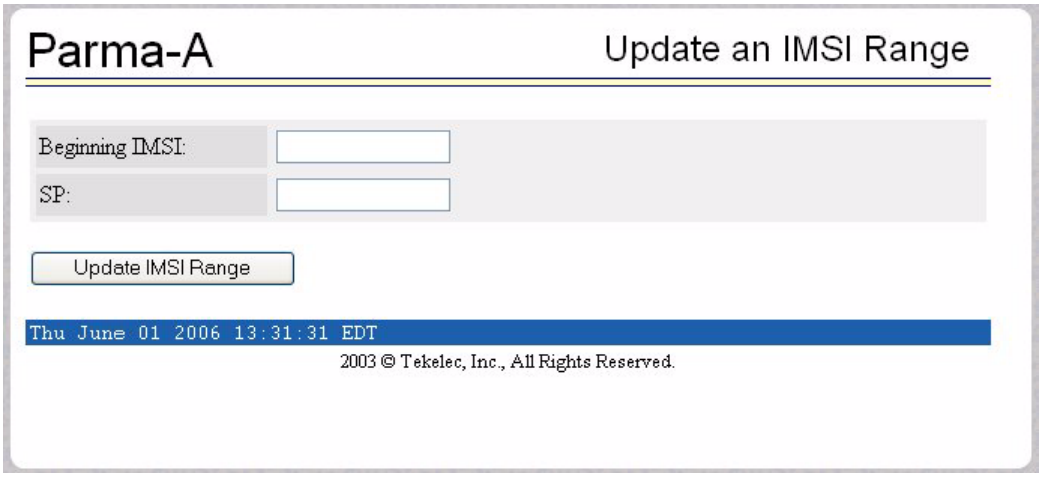
Figure 3-113. Add an IMSI Range Screen

Update an IMSI Range

The PDBA / Manage Data / IMSI Range / Update an IMSI Range screen prompts the user for the fields necessary to change the SP for an IMSI Range in the Provisioning Database (PDB). See Figure 3-114 for an example of the Update an IMSI Range screen.

NOTE: This screen is only operational to SOG customers.

Figure 3-114. Update an IMSI Range Screen



Delete an IMSI Range

The PDBA / Manage Data / IMSI Range / Delete an IMSI Range screen prompts the user for the fields necessary to remove a subscription range from the Provisioning Database (PDB). See Figure 3-115 for an example of the Delete an IMSI Range screen.

NOTE: This screen is only operational to SOG customers.

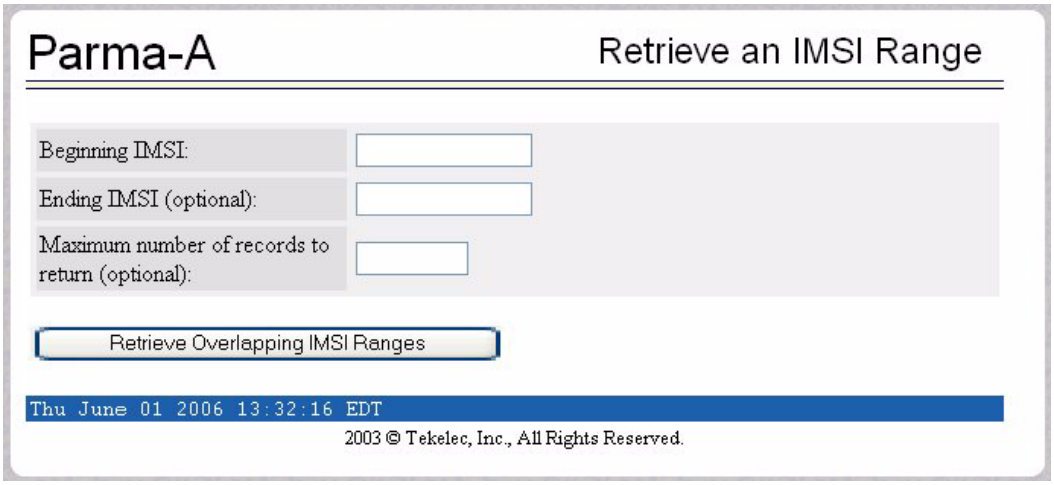
Figure 3-115. Delete IMSI Range Screen

Retrieve an IMSI Range

The PDBA / Manage Data / IMSI Range / Retrieve an IMSI Range screen prompts you for the fields necessary to retrieve subscriptions from the Provisioning Database (PDB). All subscriptions overlapping the *Beginning IMSI* to the *Ending IMSI* are shown.The *Ending IMSI* is not required. Figure 3-116 shows an example of the Retrieve an IMSI Range screen.

NOTE: This screen is only operational to SOG customers.

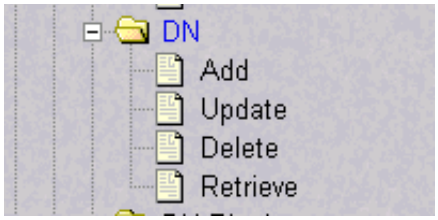
Figure 3-116. Retrieve an IMSI Range Screen



DN

The PDBA / Manage Data / DN menu lets you add, update, delete, and view dialed numbers (DNs) in the Provisioning Database (PDB). A 'dialed number' can refer to any mobile or wireline subscriber number and can include MSISDN, MDN, MIN, or the wireline Dialed Number. See Figure 3-117 for the PDBA / Manage Data / DN screen.

Figure 3-117. Manage Data Screen / DN Menu



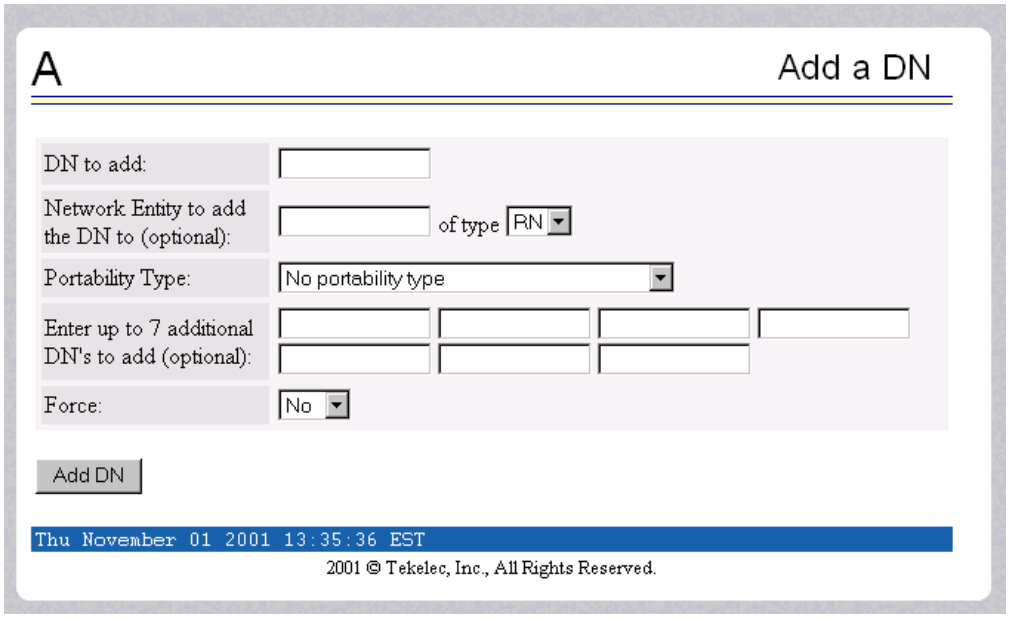
The PDBA / Manage Data / DN menu provides these actions:

- "Add a DN" on page 3-82
- "Update a DN" on page 3-83
- "Delete a DN" on page 3-83
- "Retrieve a DN" on page 3-84

Add a DN

The PDBA / Manage Data / DN / Add a DN screen prompts you for the fields needed to add a DN to the Provisioning Database (PDB). If there is a conflicting subscription in the PDB, you are prompted to confirm before overwriting the existing subscription. See Figure 3-118 for an example of the Add a DN screen.

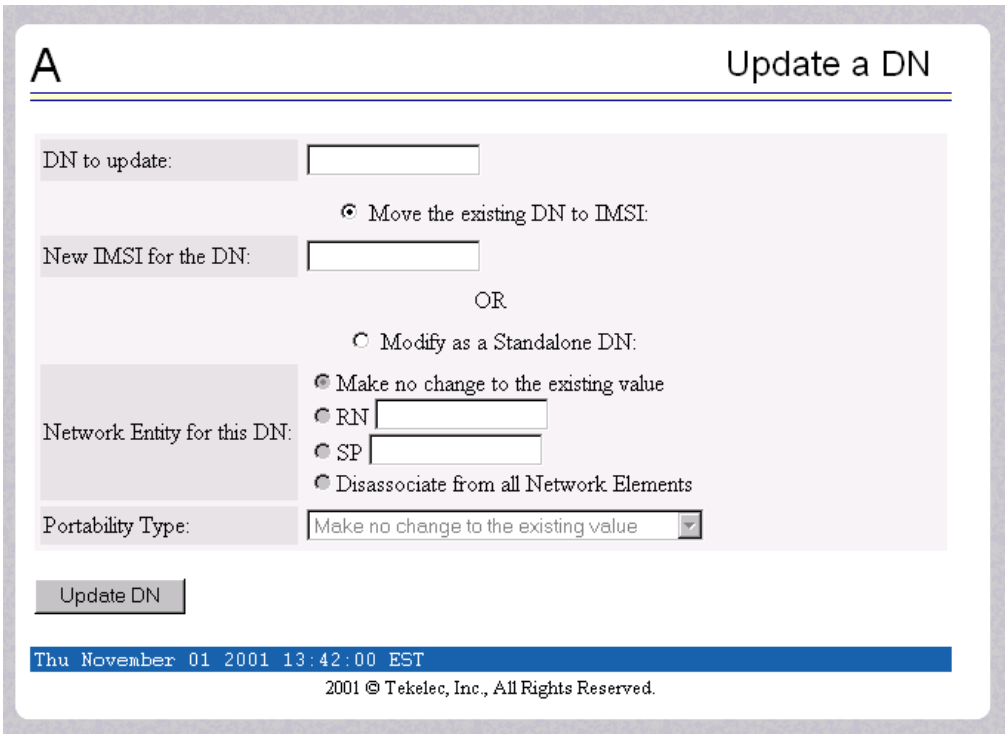
Figure 3-118. Add a DN Screen



Update a DN

The PDBA / Manage Data / DN / Update a DN screen prompts you for the fields necessary to change the SP or RN for an DN in the Provisioning Database (PDB). See Figure 3-119 for an example of the Update a DN menu.

Figure 3-119. Update a DN Screen



Delete a DN

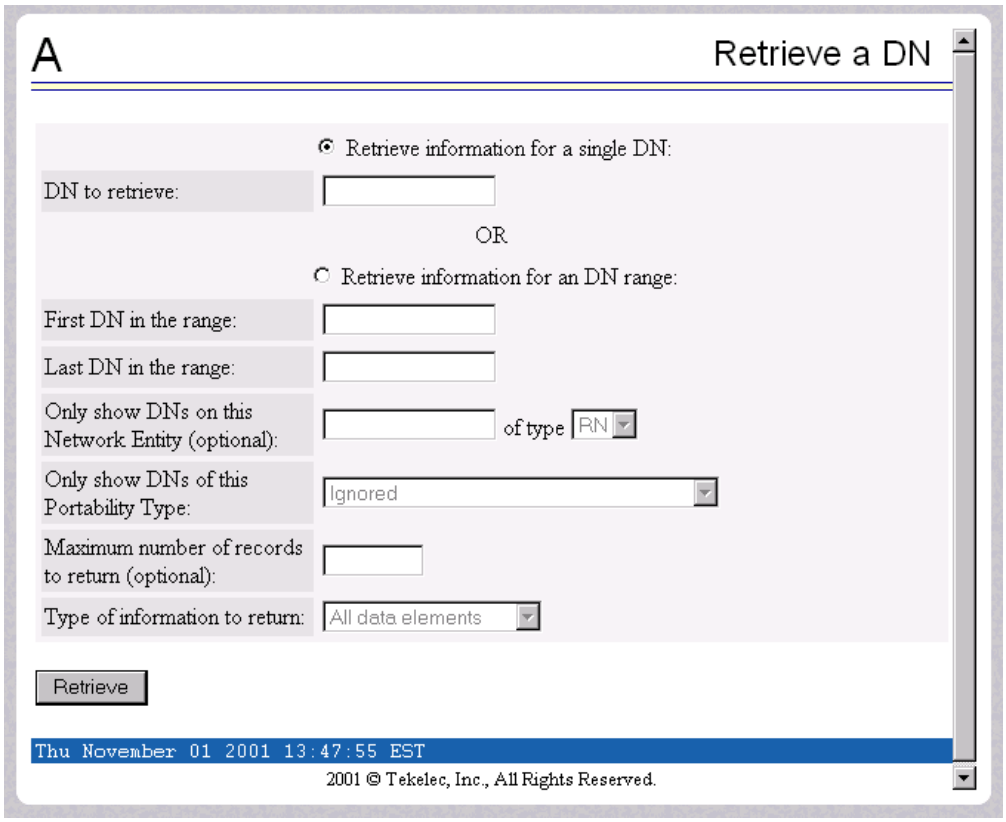
The PDBA / Manage Data / DN / Delete a DN screen prompts the user for the fields necessary to remove a DN from the Provisioning Database (PDB). See Figure 3-120 for an example of the Delete a DN screen.

Figure 3-120. Delete a DN Screen

Retrieve a DN

The PDBA / Manage Data / DN / Retrieve a DN screen prompts you for the fields necessary to retrieve subscriptions from the Provisioning Database (PDB) by DN. See Figure 3-121 for an example of the Retrieve a DN screen.

Figure 3-121. Retrieve a DN Screen

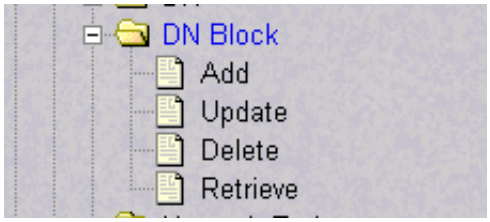


DN Block

The PDBA / Manage Data / DN Block menu lets you add, update, delete, and view DN Blocks in the Provisioning Database (PDB). A 'dialed number' can refer to any mobile or wireline subscriber number, and can include MSISDN, MDN, MIN, or the wireline Dialed Number. A DN Block is a grouping of DN numbers that is treated as a continuous sequence of DNs.

See Figure 3-122 for the PDBA / Manage Data / DN Block menu.

Figure 3-122. PDBA / Manage Data Screen / DN Block Menu



The PDBA / Manage Data / DN Block menu provides these actions:

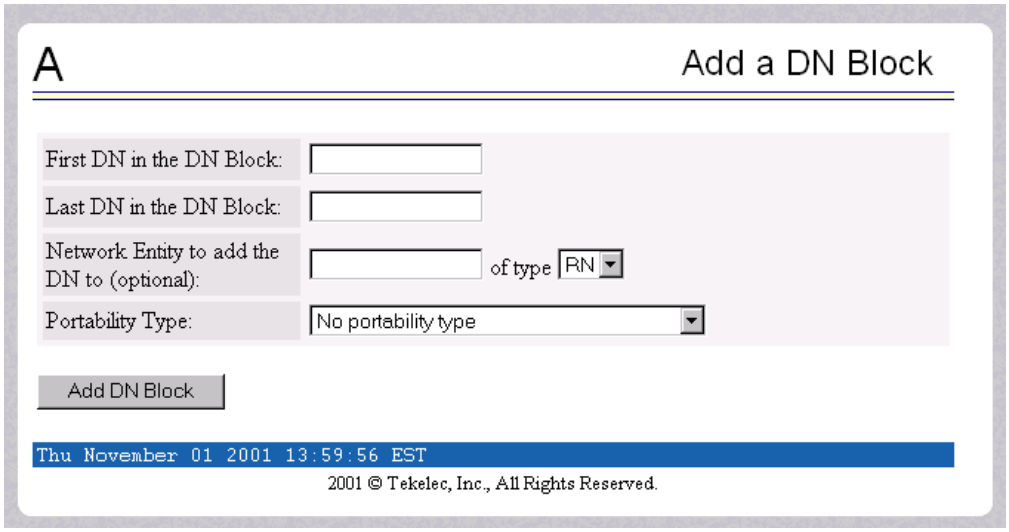
- "Add a DN Block" on page 3-86
- "Update a DN Block" on page 3-87
- "Delete a DN Block" on page 3-87
- "Retrieve DN Blocks" on page 3-88

Add a DN Block

The PDBA / Manage Data / DN Block / Add a DN Block screen prompts you for the fields needed to add a DN block to the Provisioning Database (PDB). If there is a conflicting subscription in the PDB, you are prompted to confirm before overwriting the existing subscription.

See Figure 3-123 for an example of the Add a DN Block screen.

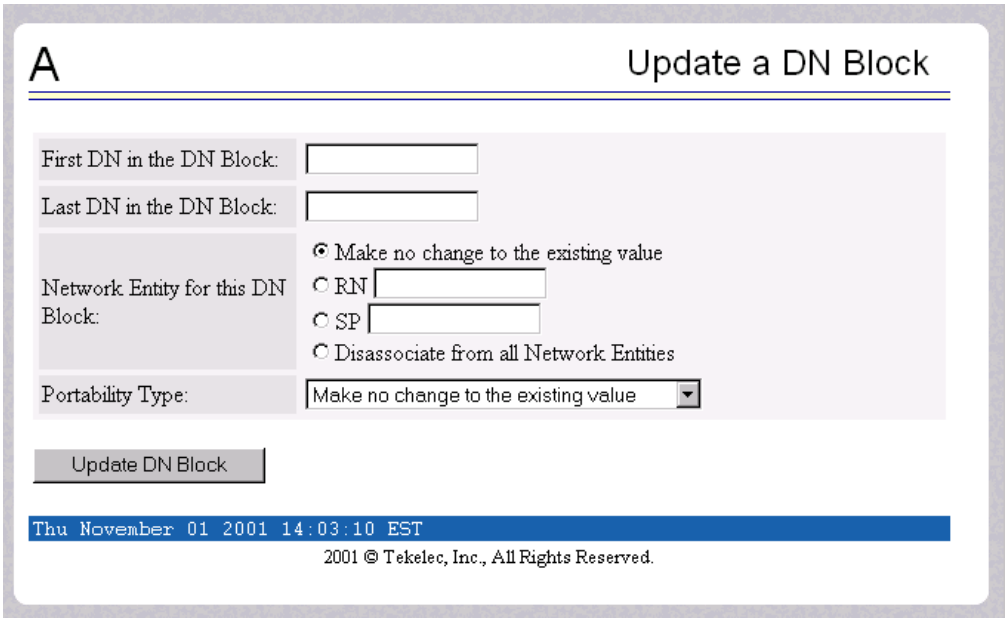
Figure 3-123. Add a DN Block Screen



Update a DN Block

The PDBA / Manage Data / DN Block / Update a DN Block screen prompts you for the fields necessary to change the SP or RN for an DN block in the Provisioning Database (PDB). See Figure 3-124 for an example of the Update a DN Block screen.

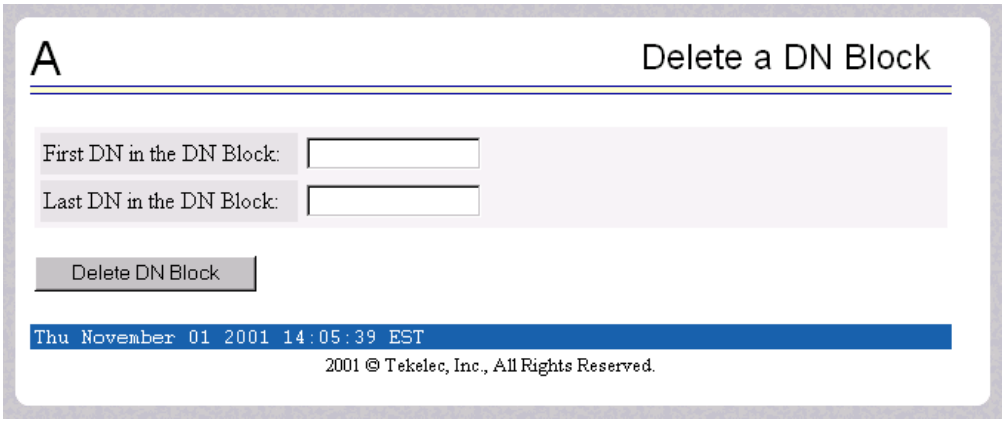
Figure 3-124. Update a DN Block Screen



Delete a DN Block

The PDBA / Manage Data / DN Block / Delete a DN Block screen prompts the user for the fields necessary to remove a DN block from the Provisioning Database (PDB). See Figure 3-125 for an example of the Delete a DN Block screen.

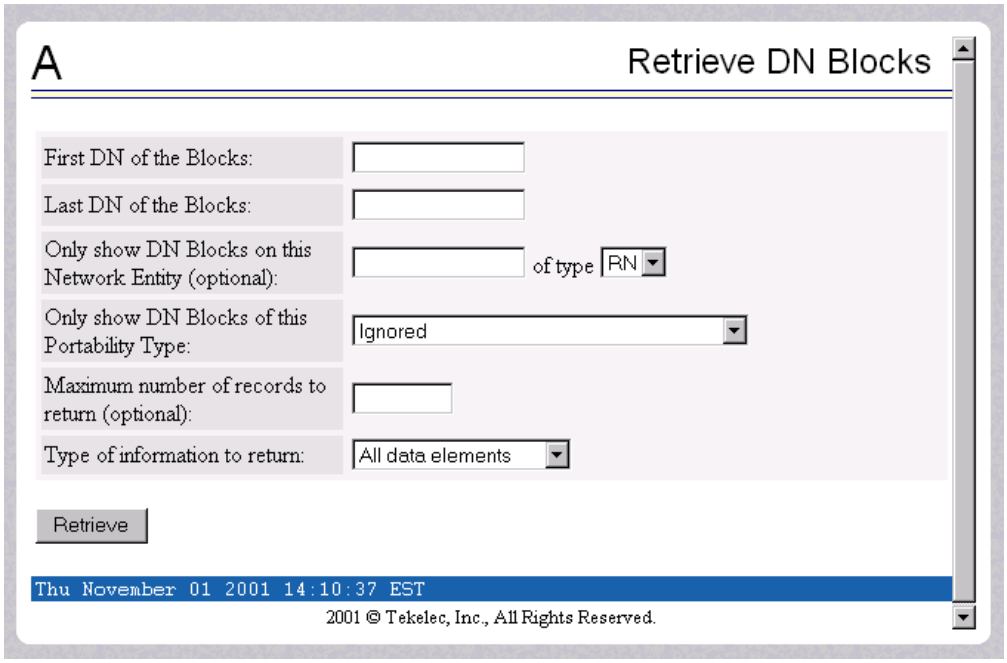
Figure 3-125. Delete a DN Block Screen



Retrieve DN Blocks

The PDBA / Manage Data / DN Block / Retrieve DN Blocks screen prompts you for the fields necessary to retrieve subscriptions from the Provisioning Database (PDB) by DN. You must specify a block of DNs. See Figure 3-126 for an example of the Retrieve DN Blocks screen.

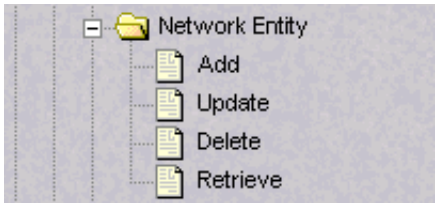
Figure 3-126. Retrieve DN Blocks Screen



Network Entity

The PDBA / Manage Data / Network Entity menu lets you add, update, delete, and retrieve network entities in the Provisioning Database (PDB). See Figure 3-127 for the PDBA / Manage Data / Network Entity menu.

Figure 3-127. PDBA / Manage Data / Network Entity Menu



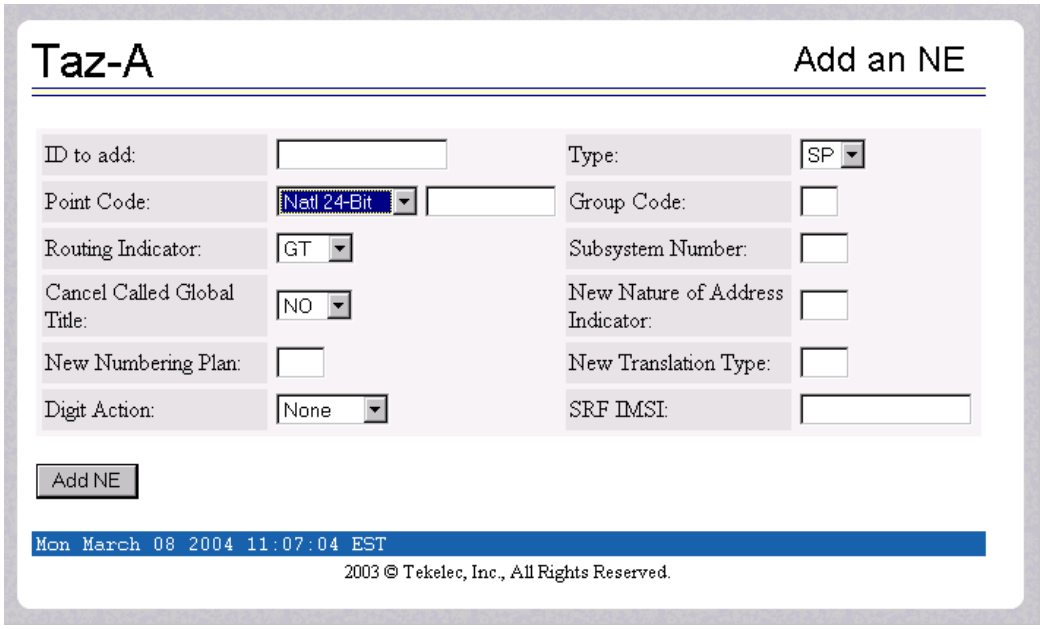
The PDBA / Manage Data / Network Entity menu provides these actions:

- "Add Network Entity" on page 3-90
- "Update Network Entity" on page 3-91
- "Delete Network Entity" on page 3-91
- "Retrieve Network Entity" on page 3-92

Add Network Entity

The PDBA / Manage Data / Network Entity / Add Network Entity menu selection prompts for the fields needed to add a network entity to the Provisioning Database (PDB). See Figure 3-128 for an example of the Add an NE screen.

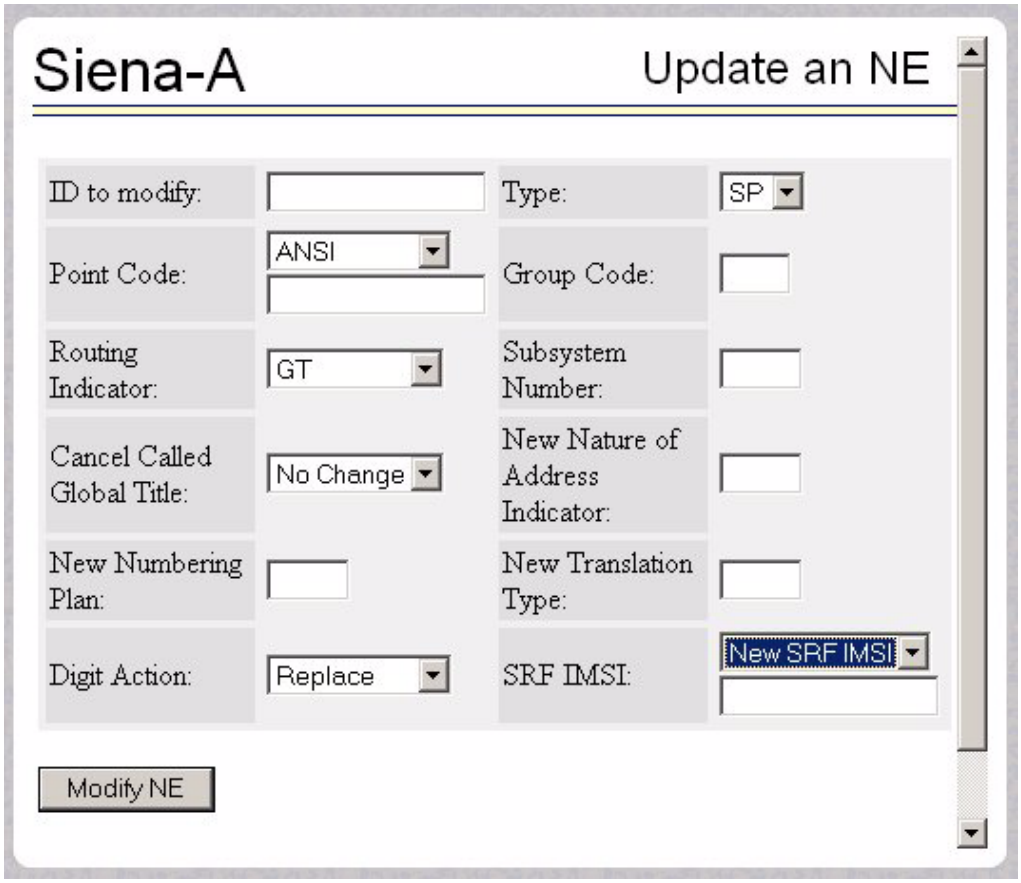
Figure 3-128. Add an NE Screen



Update Network Entity

The PDBA / Manage Data / Network Entity / Update Network Entity screen prompts for the fields necessary to change a Network Entity in the Provisioning Database (PDB). See Figure 3-129 for an example of the Update an NE screen.

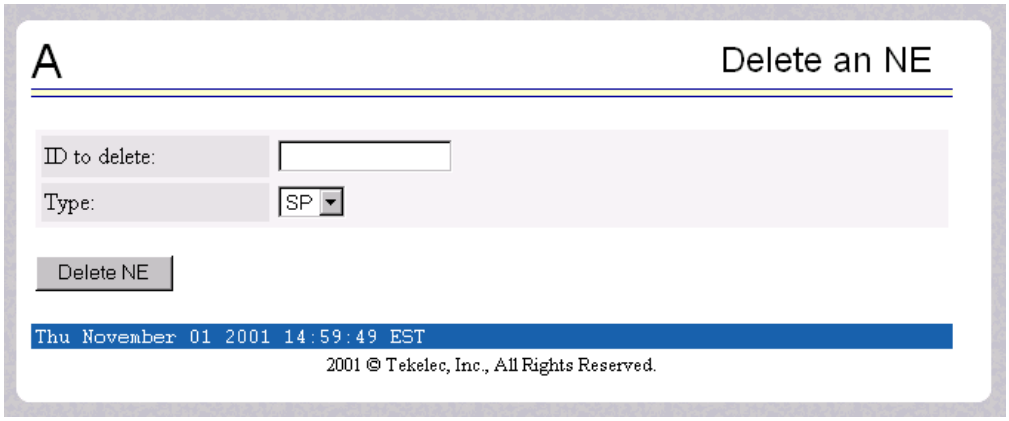
Figure 3-129. Update an NE Screen



Delete Network Entity

The PDBA / Manage Data / Network Entity / Delete Network Entity screen prompts the user for the fields necessary to remove a Network Entity from the Provisioning Database (PDB). See Figure 3-130 for an example of the Delete an NE screen.

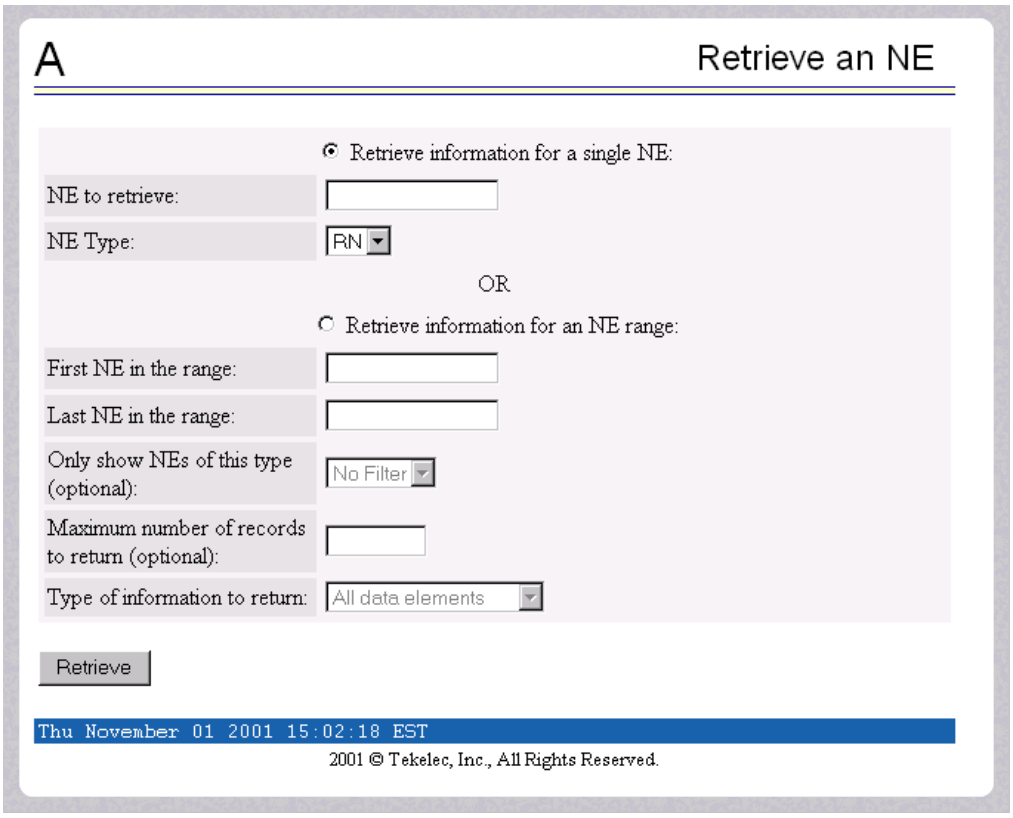
Figure 3-130. Delete an NE Screen



Retrieve Network Entity

The PDBA / Manage Data / Network Entity / Retrieve Network Entity screen prompts you for the fields necessary to retrieve a Network Entity from the Provisioning Database (PDB). See Figure 3-131 for an example of the Retrieve an NE screen.

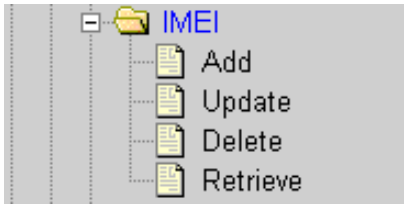
Figure 3-131. Retrieve an NE Screen



Individual IMEI

The PDBA / Manage Data / IMEI menu is used to add, update, delete, and view individual IMEI entries in the Provisioning Database (PDB). See Figure 3-132 for the IMEI menu.

Figure 3-132. IMEI Menu



The PDBA / Manage Data / IMEI menu provides these actions:

- "Add an IMEI" on page 3-93
- "Update an IMEI" on page 3-94
- "Delete an IMEI" on page 3-95
- "Retrieve an IMEI" on page 3-96

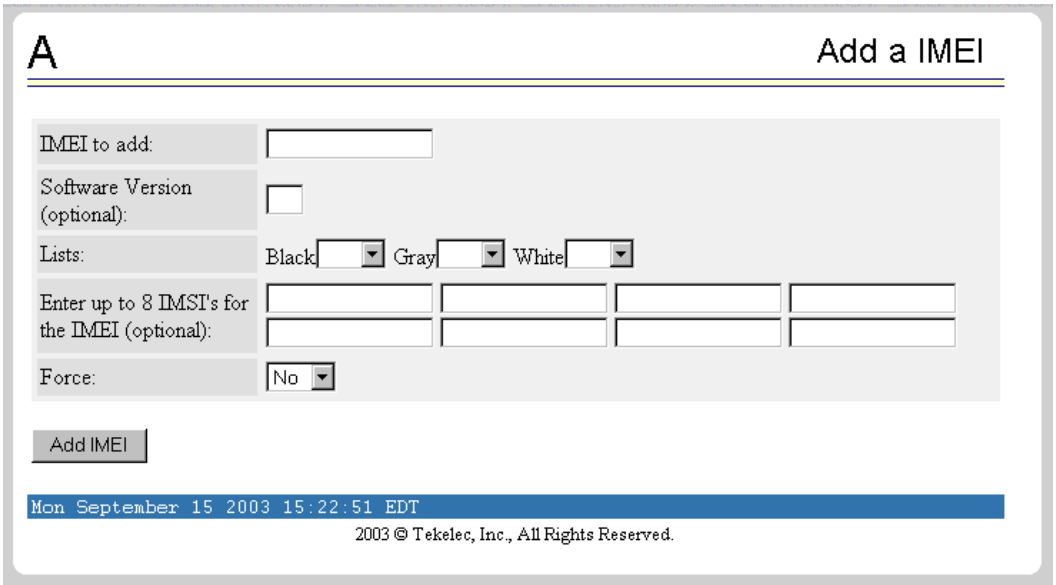
Add an IMEI

The PDBA / Manage Data / IMEI / Add an IMEI screen is used to create new IMEI entries in the Provisioning Database (PDB). The following functions are performed from this screen:

- Add a new IMEI, its associated List Types (WL,GL,BL), SVN, and 0 to 8 IMSIs. An IMEI and at least one List Type must be specified.
- Overwrite an existing IMEI. The IMEI and any other parameters and Force must be specified.
- Add a new IMSI to an existing IMEI. Existing IMEI and IMSI must be specified.

The SVN is an optional field. If no value is entered the default is 0. See Figure 3-133 for an example of the Add a IMEI screen.

Figure 3-133. Add an IMEI Screen



Update an IMEI

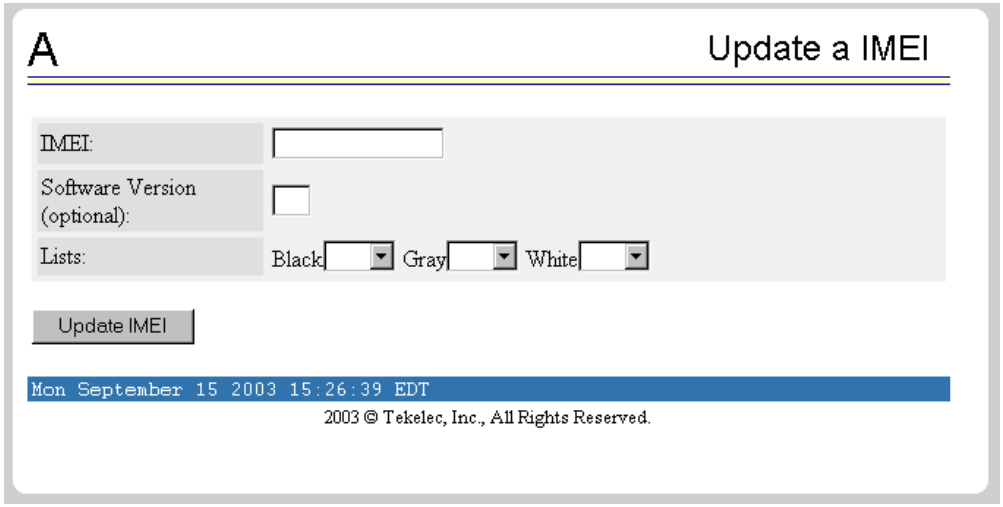
The PDBA / Manage Data / IMEI / Update IMEI screen is used to update/modify individual IMEI entries in the PDB. The following functions are performed from this screen:

- Update an IMEI with its associated List Types (WL,GL,BL). An IMEI and at least one List Type must be specified. At least one List Type must be set to yes. Unless specified, the List types will not change.
- Overwrite an existing SVN. An IMEI and SVN must be specified.

IMSIs cannot be updated with this screen. ENT_EIR and DLT_EIR are used to define IMSIs. To change the List Types, use the yes/no options for the various lists.

See Figure 3-134 for an example of the Update a IMEI screen.

Figure 3-134. Update an IMEI Screen



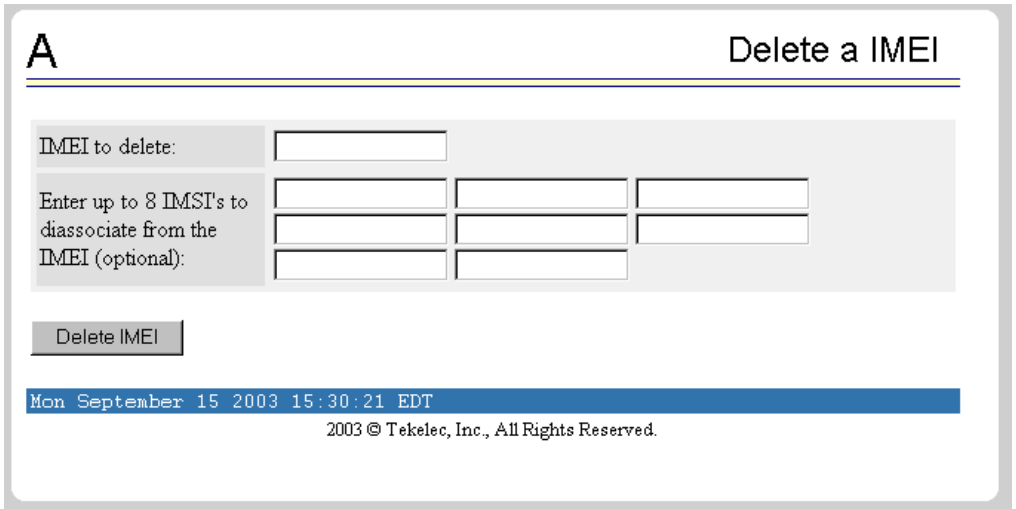
Delete an IMEI

The PDBA / Manage Data / IMEI / Delete an IMEI screen is used to remove IMEI entries from the Provisioning Database (PDB). The following functions are performed from this screen:

- Delete an IMEI and its associated list types, SVN, and any associated IMSIs. The IMEI must be specified.
- Delete an IMSI from a specific IMEI. The IMSI and IMEI must be specified.
- Delete an IMSI from all IMEIs. The IMSI must be specified.

See Figure 3-135 for an example of the Delete a IMEI screen.

Figure 3-135. Delete an IMEI Screen



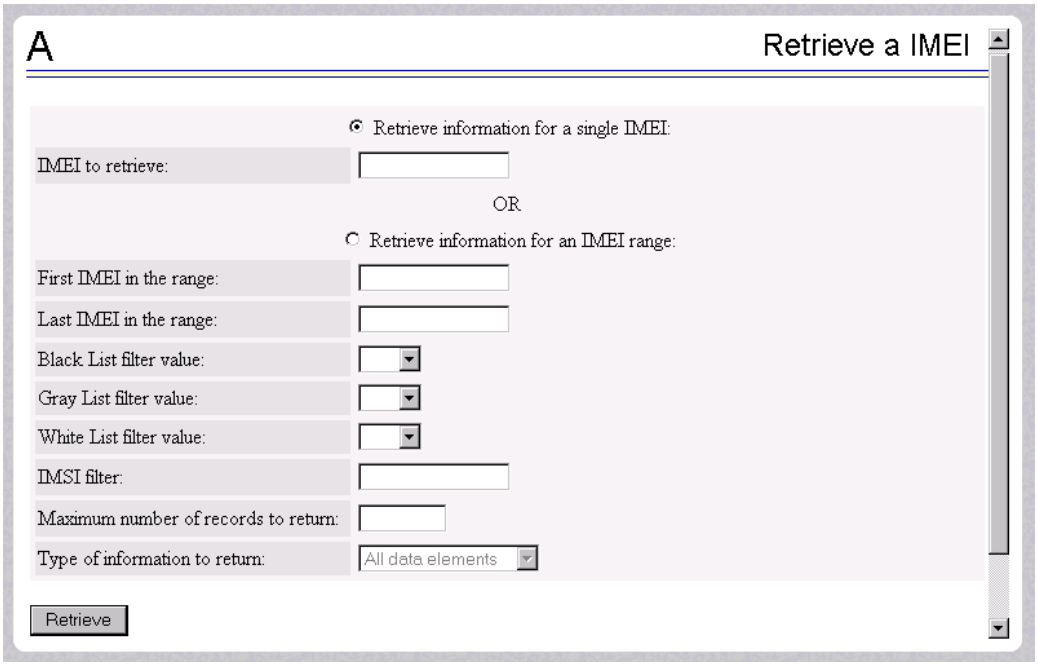
Retrieve an IMEI

The PDBA / Manage Data / IMEI / Retrieve is used to retrieve IMEI data from the Provisioning Database (PDB). The following functions are performed from this screen:

- Retrieve an IMEI and its associated List Types (WL,GL,BL), SVN, and 0 to 8 IMSIs. The IMEI must be specified.
- Retrieve a range (1 through 10,000) of IMEIs that match either of the following using filters:
  - Have a specific List Type set to YES.
  - Have an IMSI that matches the requested IMSI.
- Retrieve the beginning and ending IMEI. At least one optional filter type must be specified.

See Figure 3-136 for an example of the Retrieve a IMEI screen.

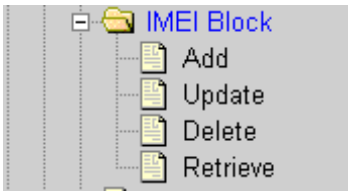
Figure 3-136. Retrieve an IMEI Screen



Block IMEI

The PDBA / Manage Data / IMEI Block menu is used to add, update, delete, and view individual IMEI entries in the Provisioning Database (PDB). See Figure 3-137 for the IMEI Block menu.

Figure 3-137. IMEI Block Menu



The PDBA / Manage Data / IMEI Block menu provides these actions:

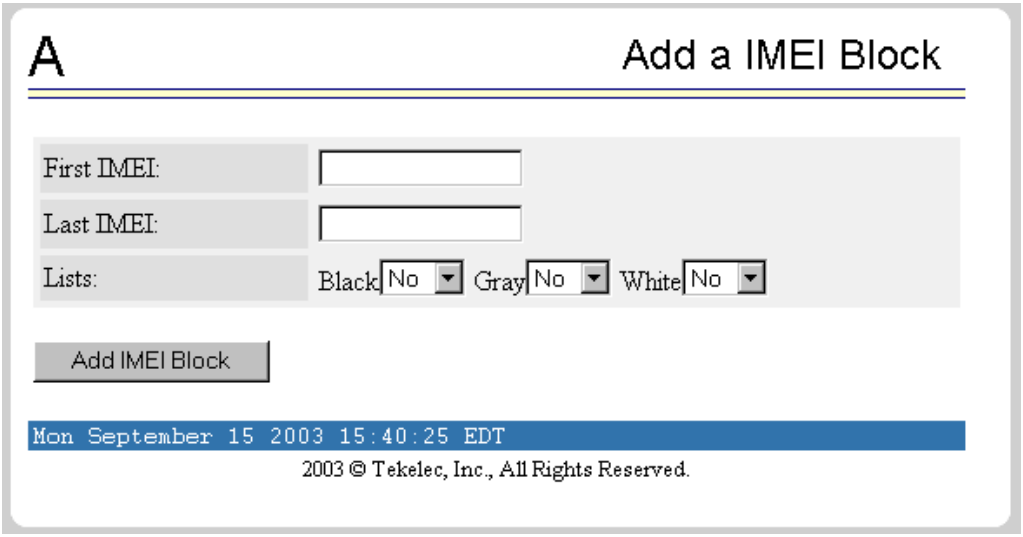
- "Add an IMEI Block" on page 3-97
- "Update an IMEI Block" on page 3-98
- "Delete an IMEI Block" on page 3-99
- "Retrieve an IMEI Block" on page 3-99

Add an IMEI Block

The PDBA / Manage Data / IMEI / Add an IMEI Block screen is used to create new IMEI entries in the Provisioning Database (PDB). This screen is used to add a new IMEI block with its associated List Types (WL,GL,BL). The First IMEI, Last IMEI, and at least one List Type must be specified.

See Figure 3-138 for an example of the Add an IMEI screen.

Figure 3-138. Add an IMEI Block Screen

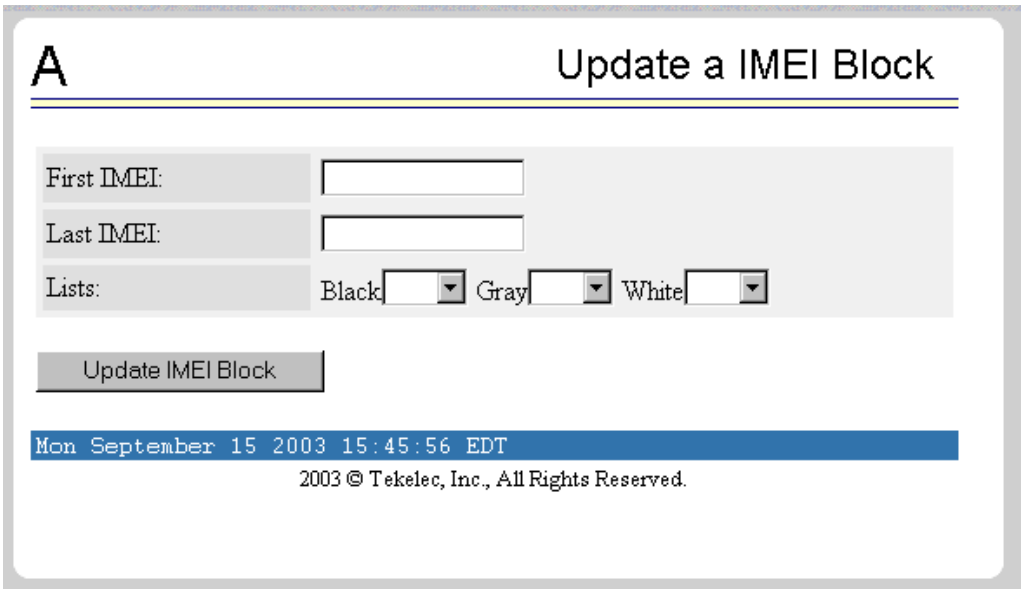


Update an IMEI Block

The PDBA / Manage Data / IMEI / Update IMEI Block screen is used to update/modify IMEI entries in the PDB. This screen is used to update an IMEI block with its associated List Types (WL,GL,BL). The First IMEI, Last IMEI, and at least one List Type must be specified. At least one List Type must be set to yes. Unless specified, the List types will not change.

See Figure 3-139 for an example of the Update an IMEI Block screen.

Figure 3-139. Update an IMEI Block Screen

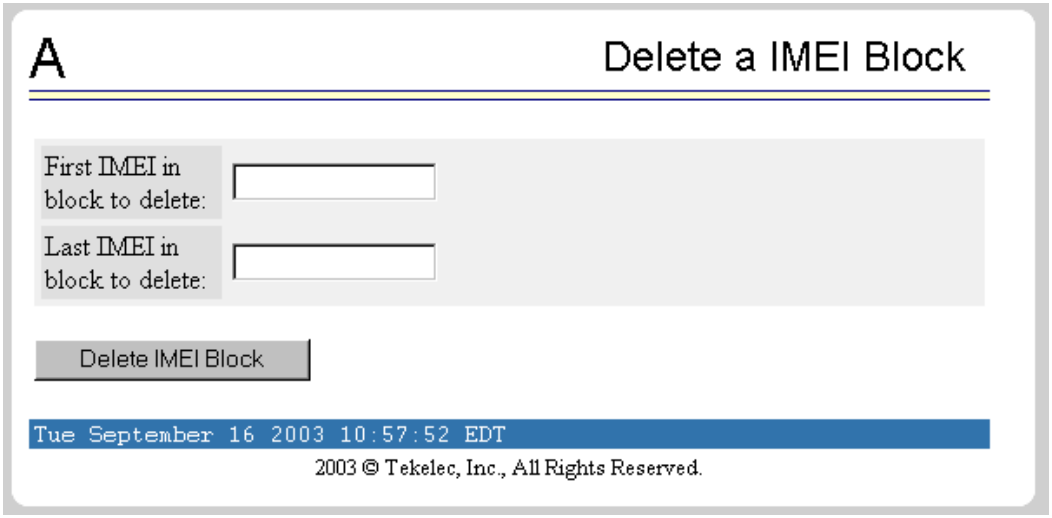


Delete an IMEI Block

The PDBA / Manage Data / IMEI / Delete an IMEI Block screen is used to remove IMEI entries from the Provisioning Database (PDB). This screen is used to delete an IMEI block and its associated list types, SVN, and any associated IMSIs. The First IMEI in the block and Last IMEI in the block must be specified.

See Figure 3-140 for an example of the Delete an IMEI Block screen.

Figure 3-140. Delete an IMEI Block Screen



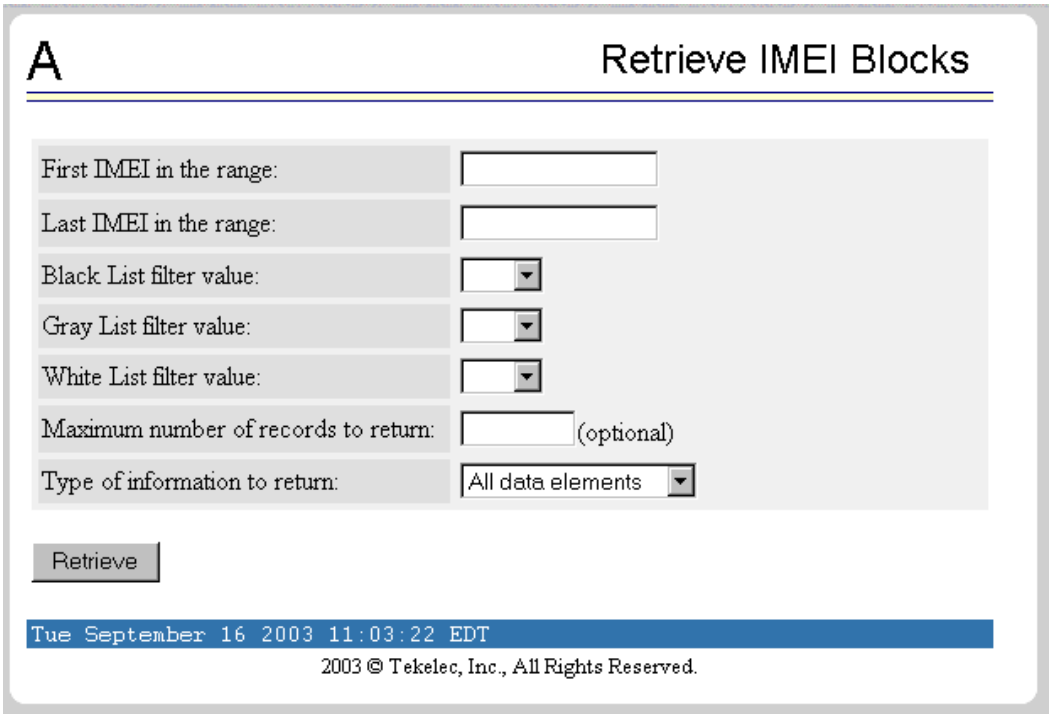
Retrieve an IMEI Block

The PDBA / Manage Data / IMEI / Retrieve is used to retrieve IMEI Block data from the Provisioning Database (PDB). The following functions are performed from this screen:

- Retrieve an IMEI Block and its associated List Types (WL,GL,BL), SVN, and 0 to 8 IMSIs. First IMEI in the range must be specified.
- Retrieve a range of IMEIs that match either of the following using filters:
  - Have a specific List Type set to YES.
  - Have an IMSI that matches the requested IMSI

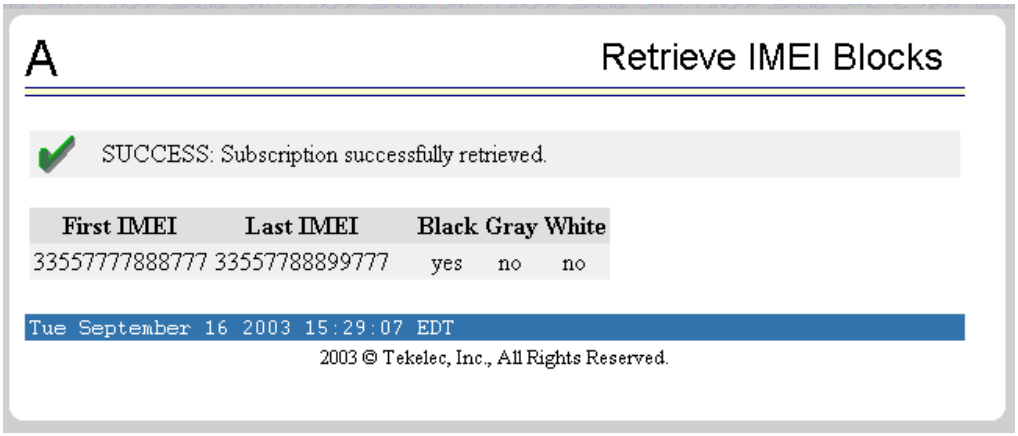
See Figure 3-141 for an example of the Retrieve an IMEI Block screen.

Figure 3-141. Retrieve an IMEI Block Screen



See Figure 3-142 for an example of the output of a Retrieve an IMEI Block screen.

Figure 3-142. Retrieve an IMEI Block Output Screen

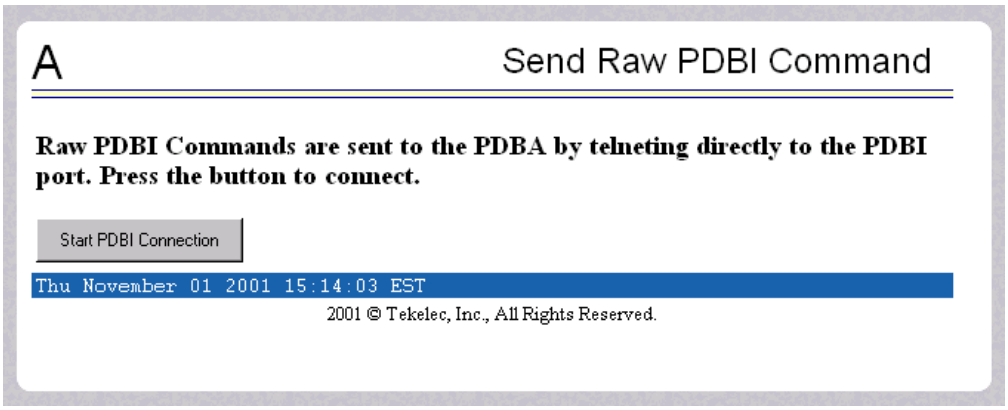


Send Raw PDBI Command

The PDBA / Manage Data / Send Raw PDBI Command screen lets you type PDBI (Provisioning Database Interface) commands that are not explicitly covered by the menu set. (The Send Raw PDBI Command screen appears under the PDBA / Manage Data menu; see Figure 3-105.)

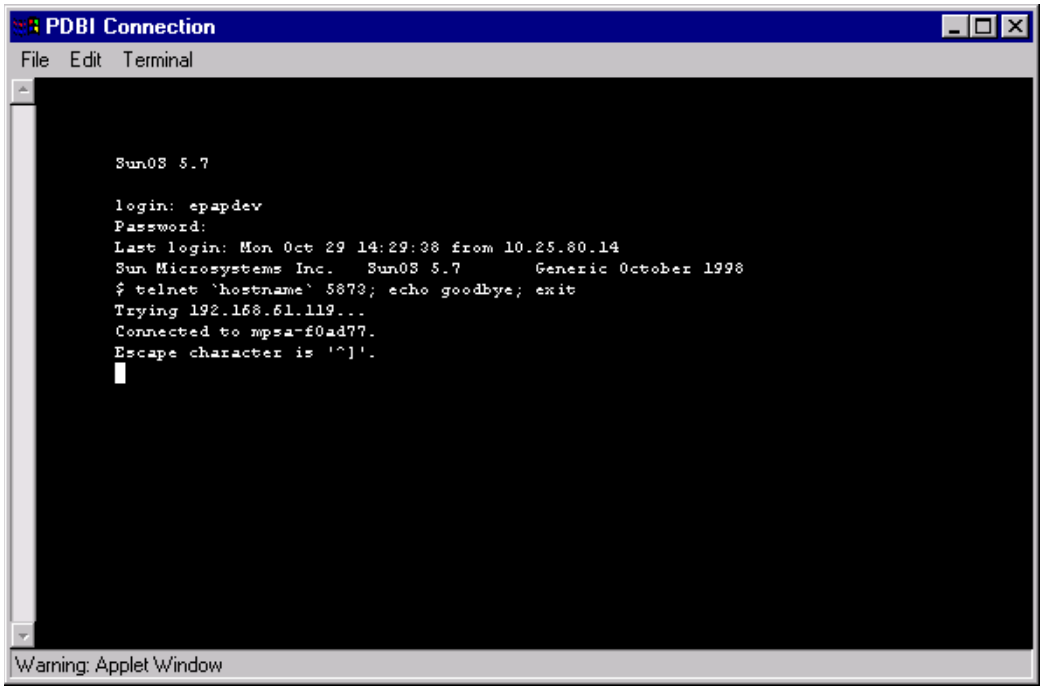
A socket connection to the PDBI is available; however, all other functions, including creating and ending transactions, must be entered by hand. For additional information about the PDBI commands, refer to the *EAGLE Provisioning Database Interface Manual*. See Figure 3-143 for the Send Raw PDBI Command screen.

Figure 3-143. Send Raw PDBI Command Screen



Press the Start PDBI Connection button, and a new window appears with the PDBI connection. Figure 3-144 shows an example of the PDBI Connection window.

Figure 3-144. PDBI Connection Window



You can close the session by:

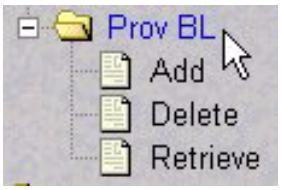
- Closing the window under the File menu, or
- Clicking on the X icon in the upper right of the window, or
- Clicking the Close PDBI Connection button in the EPAP network window.

Refer to the *Provisioning Database Interface Manual* for the rules about syntax, usages, commands, etc.

EPAP Provisioning Blacklist Menu

The PDBA / Manage Data / Prov BL menu is used to add, delete, and view blacklist entries in the Provisioning Database (PDB). See Figure 3-145 for the IMEI menu.

Figure 3-145. Provisioning Blacklist Menu



The PDBA / Manage Data / Prov BL menu provides these actions:

- "Add Provisioning Blacklist" on page 3-103
- "Delete Provisioning Blacklist" on page 3-104
- "Retrieve Provisioning Blacklist" on page 3-105

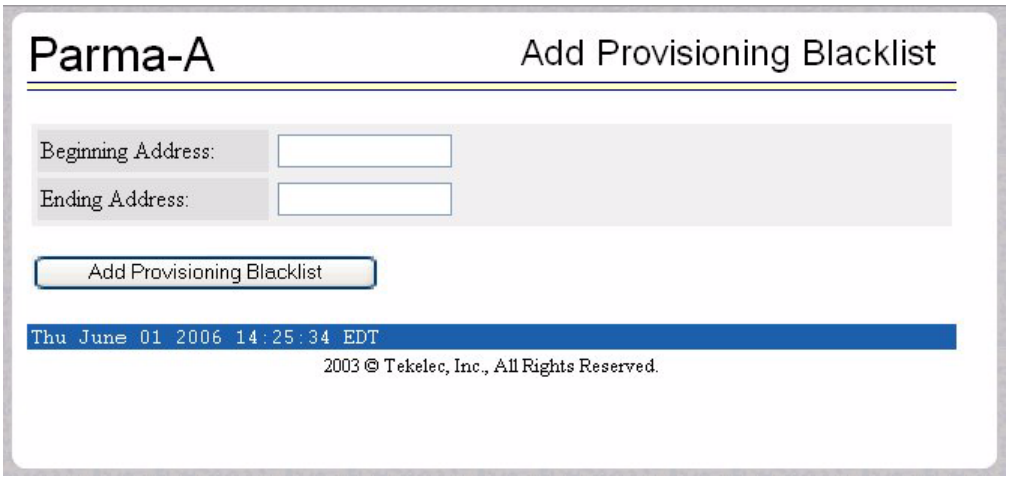
Add Provisioning Blacklist

The PDBA / Manage Data / Prov BL /Add Provisioning Blacklist screen is used to add Blacklist data to prevent certain address ranges from being used as DN, DN Block, and IMSI address strings.The following criteria must be followed when entering the blacklist data:

- The address strings are defined as two digit strings of 5-15 hexadecimal digits, where the ending address is greater than or equal to the beginning address.
- The beginning blacklist value and ending blacklist value must be of the same length.
- The address strings cannot conflict with DN, DN block, or IMSI values in the PDB.

See Figure 3-146 for an example of the Add Provisioning Blacklist screen.

Figure 3-146. Add Provisioning Blacklist Screen

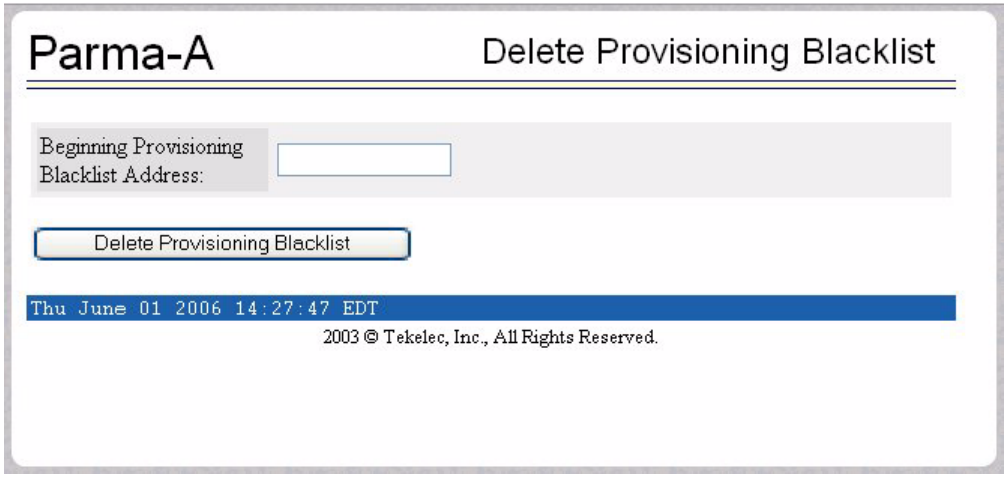


Delete Provisioning Blacklist

The PDBA / Manage Data / Prov BL / Delete Provisioning Blacklist screen is used to delete the EPAP Blacklist range from the Provisioning Database (PDB). The beginning address string is defined as a string of 5-15 hexadecimal digits.

See Figure 3-147 for an example of the Delete Provisioning Blacklist screen.

Figure 3-147. Delete Provisioning Blacklist Screen

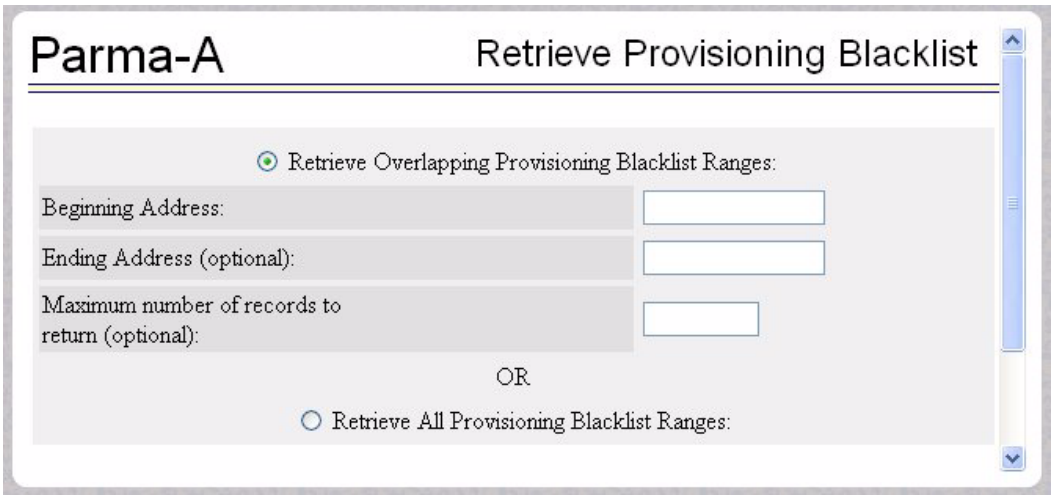


Retrieve Provisioning Blacklist

The PDBA / Manage Data / Prov BL /Retrieve Provisioning Blacklist screen is used to retrieve Blacklist data from the Provisioning Database (PDB). The address strings are defined as two digit strings of 5-15 hexadecimal digits of the same length, where the ending address is greater than or equal to the beginning address.

See Figure 3-148 for an example of the Retrieve Provisioning Blacklist screen.

Figure 3-148. Retrieve Provisioning Blacklist Screen

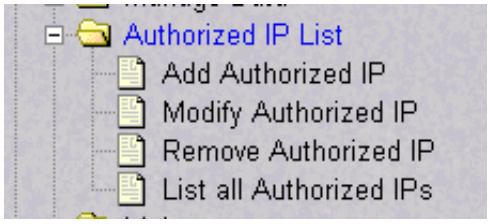


Authorized IP List

The PDBA / Authorized IP List menu lets you add, modify, remove, and list the IP addresses authorized to connect to the PDBA through the Provisioning Database (PDB). This menu also lets you specify whether an SSH (secure shell) tunnel should be created between the that IP address and the EPAP, and if so, specify what username, password and port number to use on the machine represented by the IP address. Figure 3-149 shows the Authorized IP List menu.

For more information about SSH tunneling, refer to the *Provisioning Database Interface Manual*.

Figure 3-149. Authorized IP List



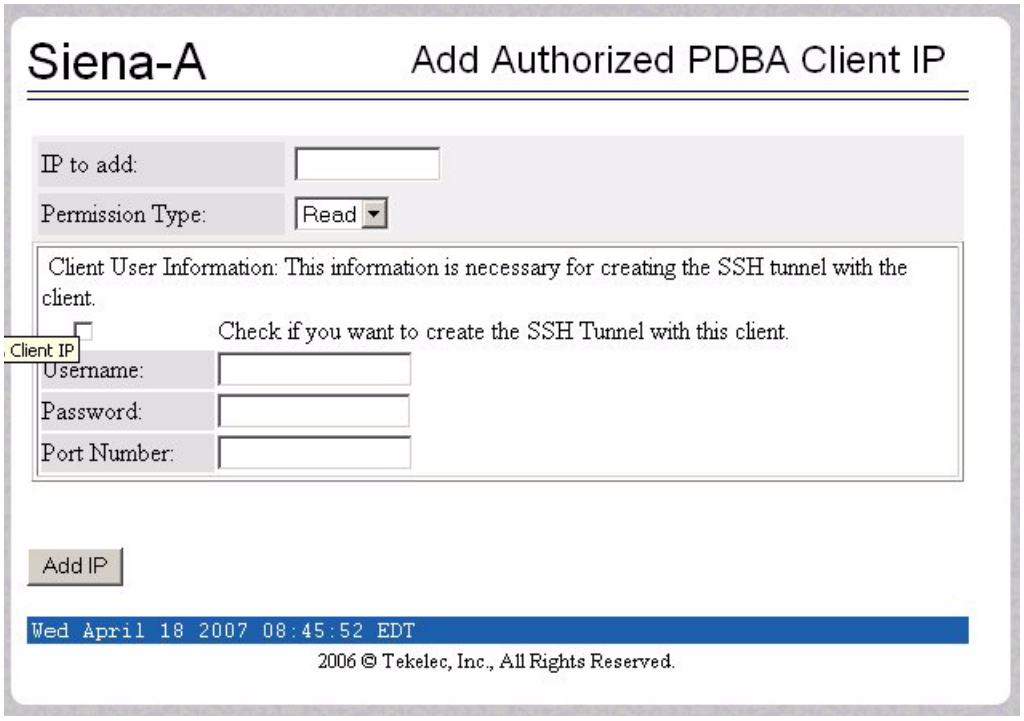
The PDBA / Authorized IP List menu provides these actions:

- "Add Authorized IP" on page 3-106
- "Modify Authorized IP" on page 3-108
- "Remove Authorized IP" on page 3-109
- "List All Authorized IPs" on page 3-111

Add Authorized IP

The PDBA / Authorized IP List / Add Authorized PDBA Client IP screen lets you add to the list of authorized addresses.For each added IP address, you can specify the permission type, Read or Write (read/write), whether an SSH (secure shell) tunnel should be created between the that IP address and the EPAP, and if so, specify what username, password and port number to use on the machine represented by the IP address. See Figure 3-150 for the Add Authorized PDBA Client IP Screen.

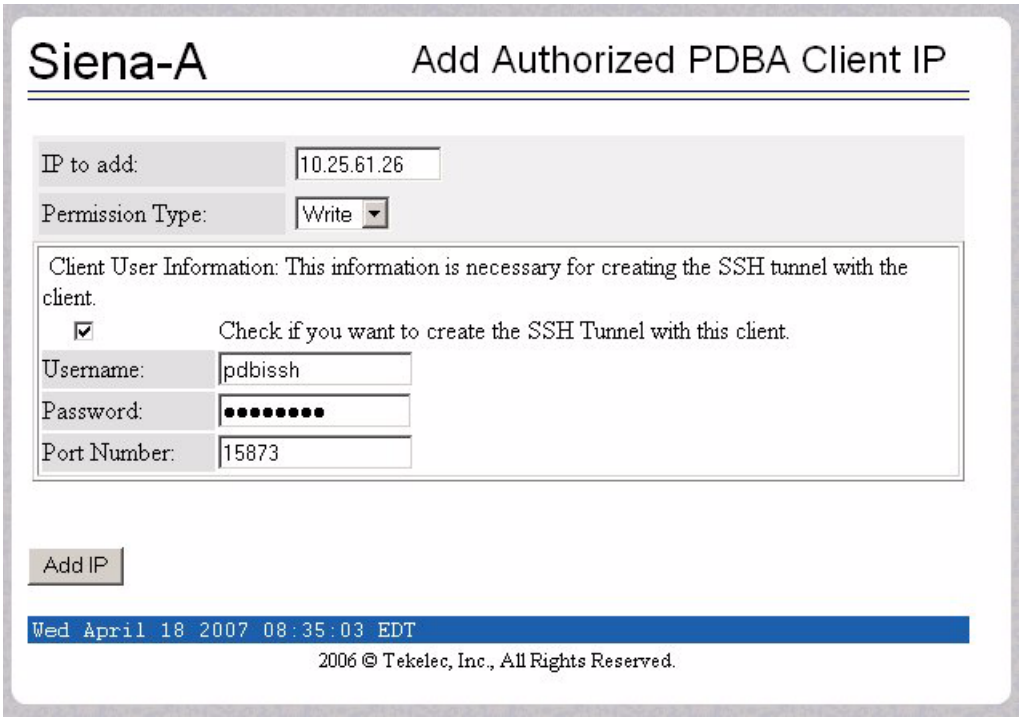
Figure 3-150. Add Authorized PDBA Client IP Screen



To add an authorized PDBA client IP address, enter the desired IP address in the field, select the Read or Write Permission Type, and if you want an SSH tunnel between that IP address and the EPAP, select the Client User Information checkbox , and enter the username, password, and port to be used. Then, click the Add IP button, as Figure 3-151 shows.

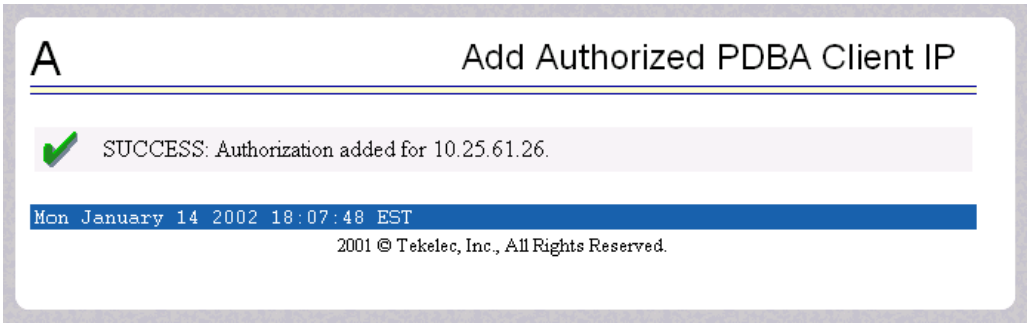
NOTE: Only IP addresses with WRITE permission are allowed to create an SSH tunnel. The EPAP does not store the password of the client machine. The password is used only one time for SSH key exchange.

Figure 3-151. Example of Adding an Authorized PDBA Client IP



When the IP address is accepted, you see the message indicating a successful acceptance of the address in Figure 3-152.

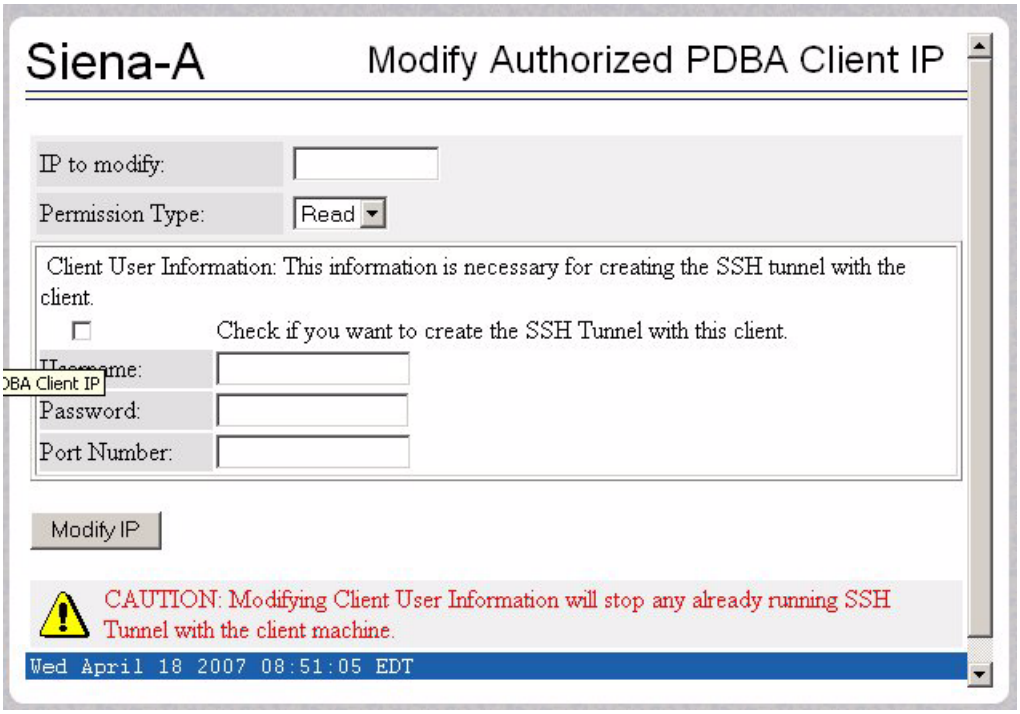
Figure 3-152. Successfully Adding an Authorized PDBA Client IP



Modify Authorized IP

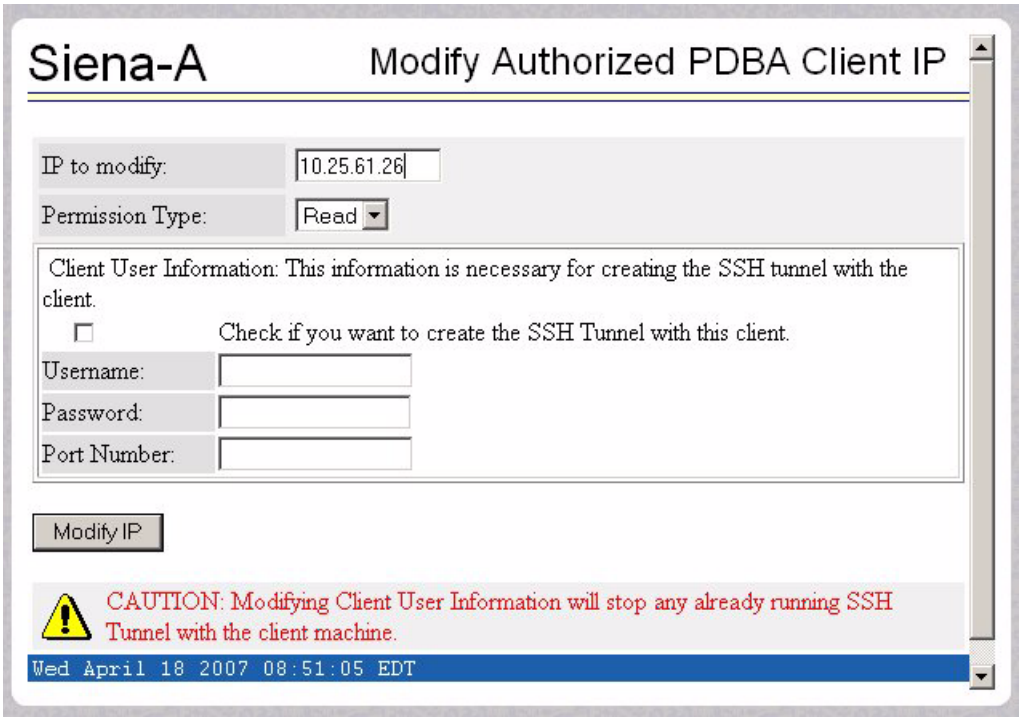
The PDBA / Authorized IP List / Modify Authorized PDBA Client IP screen lets you change the type of permission of an authorized PDBA client IP address, change whether an SSH tunnel should be created, and change the username, password, and port number. See Figure 3-153 for the Modify Authorized PDBA Client IP Screen.

Figure 3-153. Modify Authorized PDBA Client IP Screen



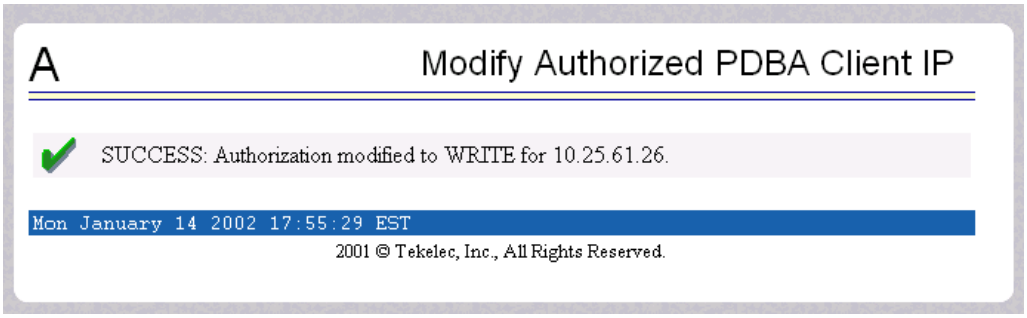
To modify an authorized PDBA client IP address, enter the desired IP address in the field, select the Read or Write Permission Type, select or deselect the Client User Information checkbox, enter the desired username, password, or port number, and click the Modify IP button, shown in Figure 3-154.

Figure 3-154. Example of Modifying an Authorized PDBA Client IP



When the modification of the IP address is accepted, you see the message indicating a successful acceptance of the altered permission type in Figure 3-155.

Figure 3-155. Successfully Modifying an Authorized PDBA Client IP



Remove Authorized IP

The PDBA / Authorized IP List / Remove Authorized PDBA Client IP screen lets you remove an IP address from the list of authorized addresses. A CAUTION message informs you that removing an IP will stop any SSH tunnel that is currently connected with that IP. See Figure 3-156 for the Remove Authorized PDBA Client IP Screen.

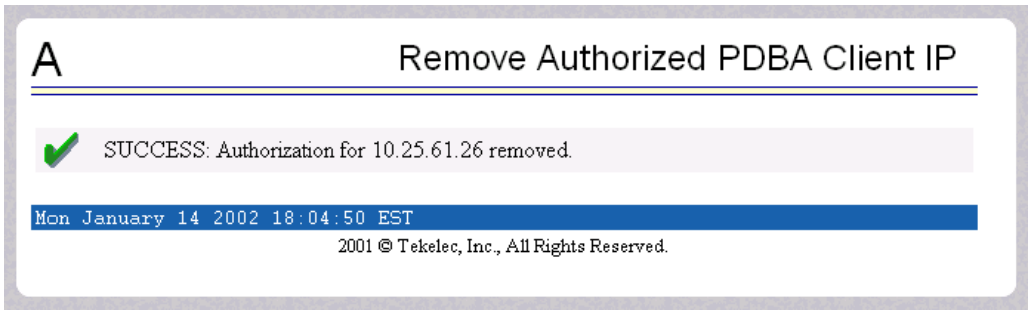
Figure 3-156. Remove Authorized PDBA Client IP Screen

To remove an authorized PDBA client IP address, enter the desired IP address in the field, and click the Remove IP button, shown in Figure 3-157.

Figure 3-157. Example of Removing an Authorized PDBA Client IP

When the removal of the IP address is accepted, you see the message indicating a successful completion of the action in Figure 3-158.

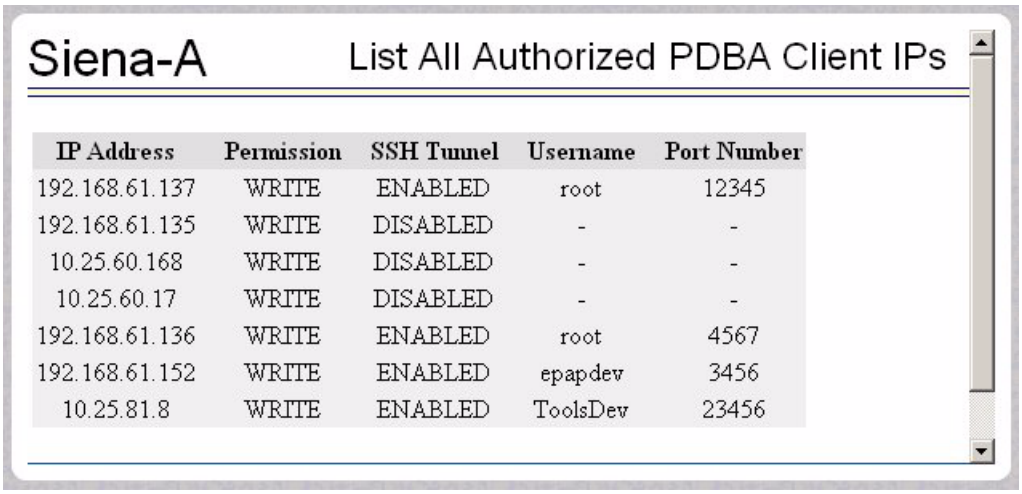
Figure 3-158. Successfully Removing an Authorized PDBA Client IP



List All Authorized IPs

The PDBA / Authorized IP List / List All Authorized PDBA Client IPs screen lets you display all authorized IP addresses. The list displays the permission type, whether the SSH tunnel is enabled or disabled, and the username and port number. See Figure 3-159 for the List All Authorized PDBA Client IPs screen.

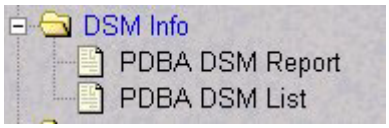
Figure 3-159. List All Authorized PDBA Client IPs Screen



DSM Info

The PDBA / DSM Info menu is used to request information on the DSMs in the network. Figure 3-149 shows the DSM Info menu.

Figure 3-160. DSM Info



The PDBA / DSM Info menu provides these actions:

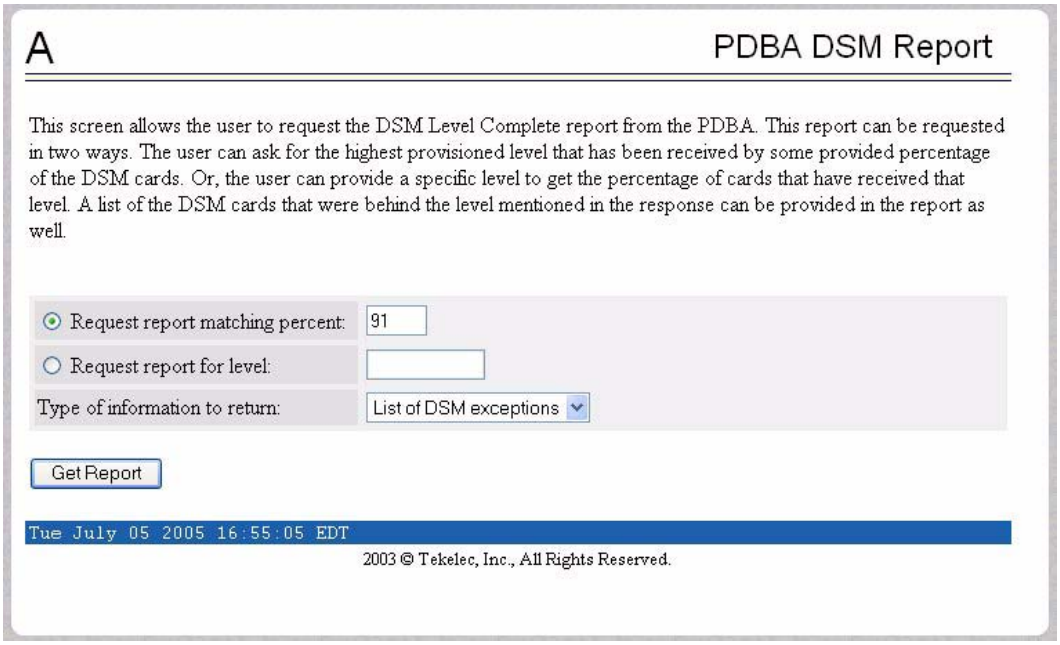
- "PDBA DSM Report" on page 3-111
- "PDBA DSM List" on page 3-112

PDBA DSM Report

The PDBA / DSM Info / PDBA DSM Report screen is used request the DSM Level complete report from the PDBA. This report can be requested in two ways. The user can ask for the highest provisioned level that has been received by some provided percentage of the DSM cards. Or the user can provide a specific level to

get the percentage of cards that have received that level. A list of the DSM cards that were behind the level mentioned in the response can be provided in the report as well. See Figure 3-161 for the PDBA DSM Report screen.

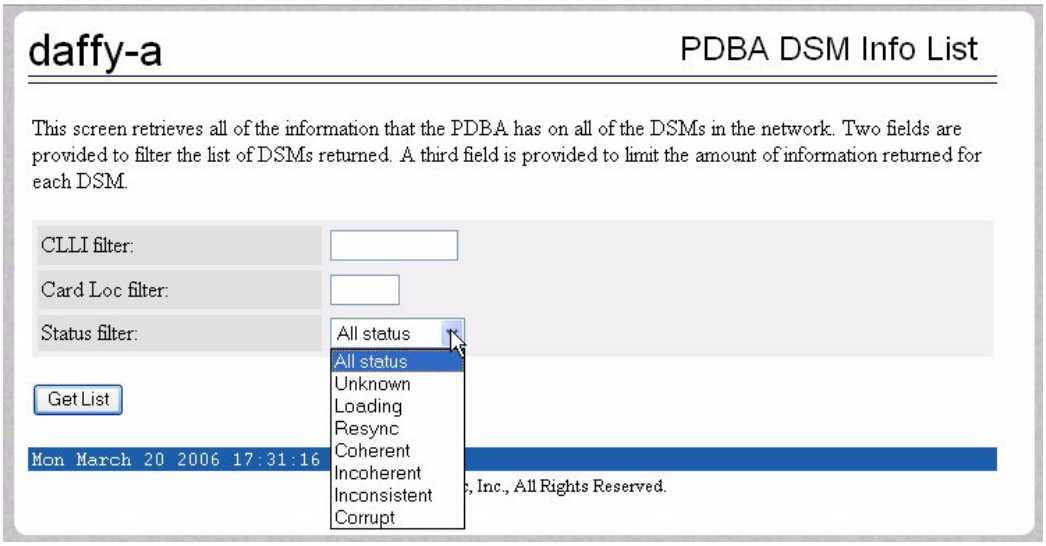
Figure 3-161. PDBA DSM Report Screen



PDBA DSM List

This screen retrieves all of the information that the PDBA has on all of the DSMs in the network. Two fields are provided to filter the list of DSMs returned. A third field is provided to limit the amount of information returned for each DSM. Refer to Figure 3-162 for an example of the PDBA DSM Info List.

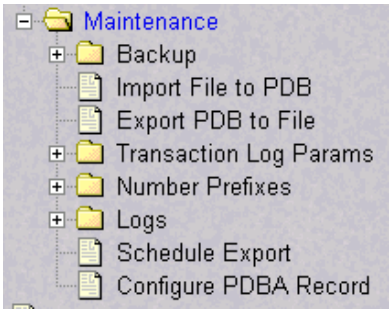
Figure 3-162. PDBA DSM Info List Screen (with Status filter pulldown)



PDBA / Maintenance

The PDBA / Maintenance menu lets you perform various PDB maintenance operations for the Provisioning Database (PDB). See Figure 3-163.

Figure 3-163. PDBA / Maintenance Menu



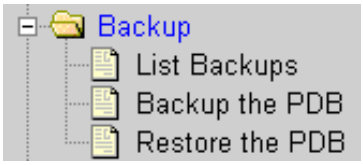
The PDBA / Maintenance menu provides these actions:

- "PDBA / Maintenance / Backup" on page 3-114
- "PDBA / Maintenance / Import File to PDB" on page 3-117
- "PDBA / Maintenance / Export PDB to File" on page 3-119
- "PDBA / Maintenance / Transaction Log Params" on page 3-121
- "PDBA / Maintenance / Number Prefixes" on page 3-123
- "PDBA / Maintenance / Logs" on page 3-126
- "PDBA / Maintenance / Schedule PDB Export" on page 3-127
- "PDBA / Maintenance / Configure PDBA Record Delay" on page 3-131

PDBA / Maintenance / Backup

The PDBA / Maintenance / Backup menu lets you perform backup actions, including listing backups and backup on device, backing up the PDB, and restoring the PDB. See Figure 3-164 for the PDBA / Maintenance / Backup menu.

Figure 3-164. Backup Menu



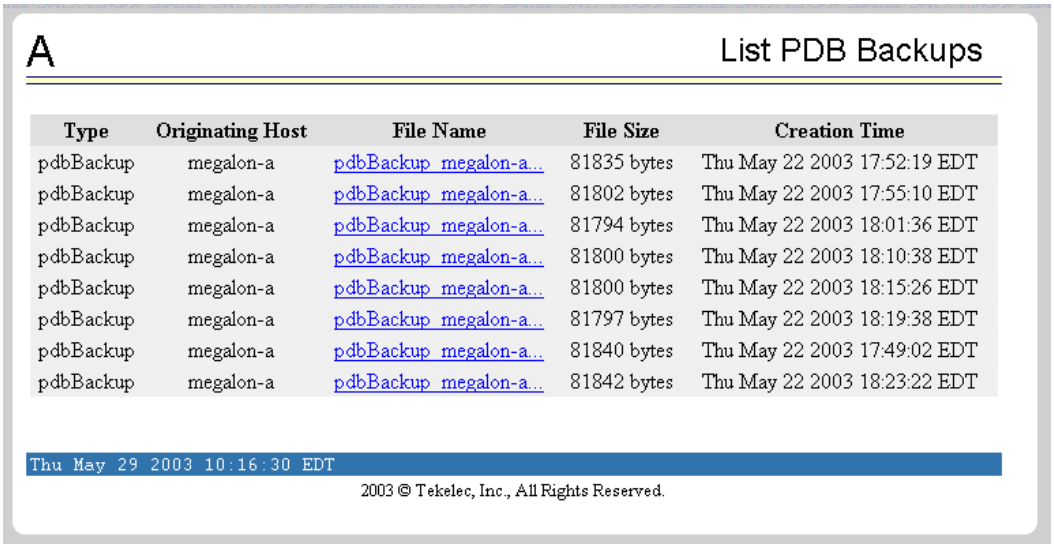
The PDBA / Maintenance / Backup menu provides these actions:

- "List Backups" on page 3-114
- "Backup the PDB" on page 3-114
- "Restore the PDB" on page 3-116

List Backups

The PDBA / Maintenance / Backup / List PDB Backups screen lists the details of the backup. See Figure 3-165 for an example of the List PDB Backups screen.

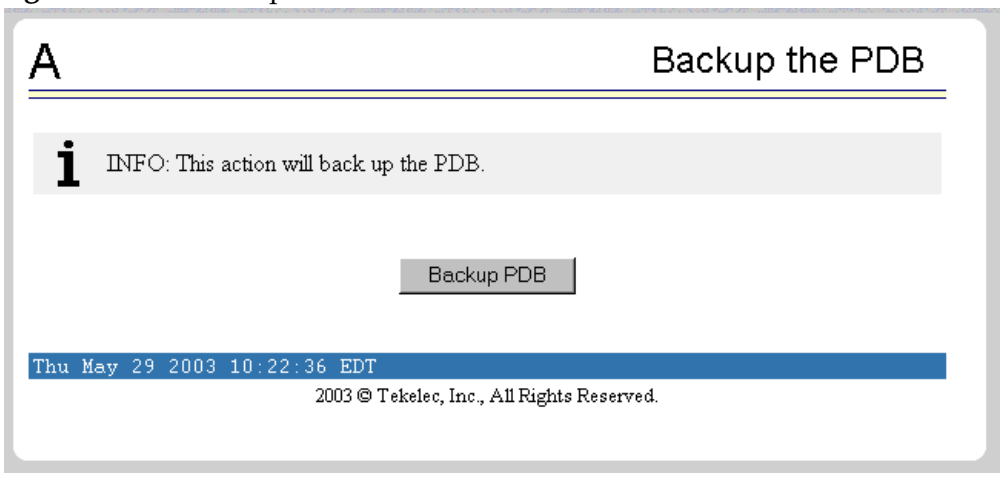
Figure 3-165. List PDB Backups Screen



Backup the PDB

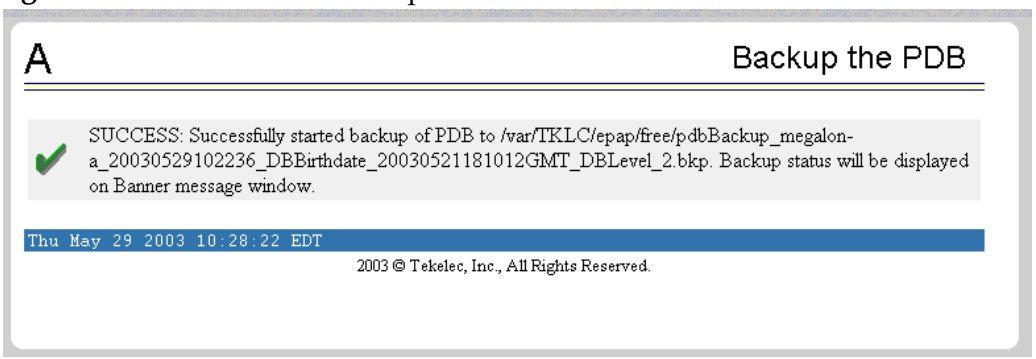
The PDBA / Maintenance / Backup / Backup the PDB screen makes a copy of the database, from which it can restore the PDB, in case of emergency. The screen is shown in Figure 3-166.

Figure 3-166. Backup the PDB Screen



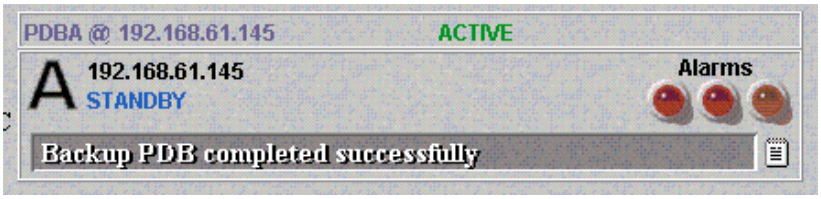
The successful backup of the database results in this screen, shown in Figure 3-167.

Figure 3-167. Successful Backup of the PDB



The completed successful backup results in the Banner Message Window as shown in Figure 3-168.

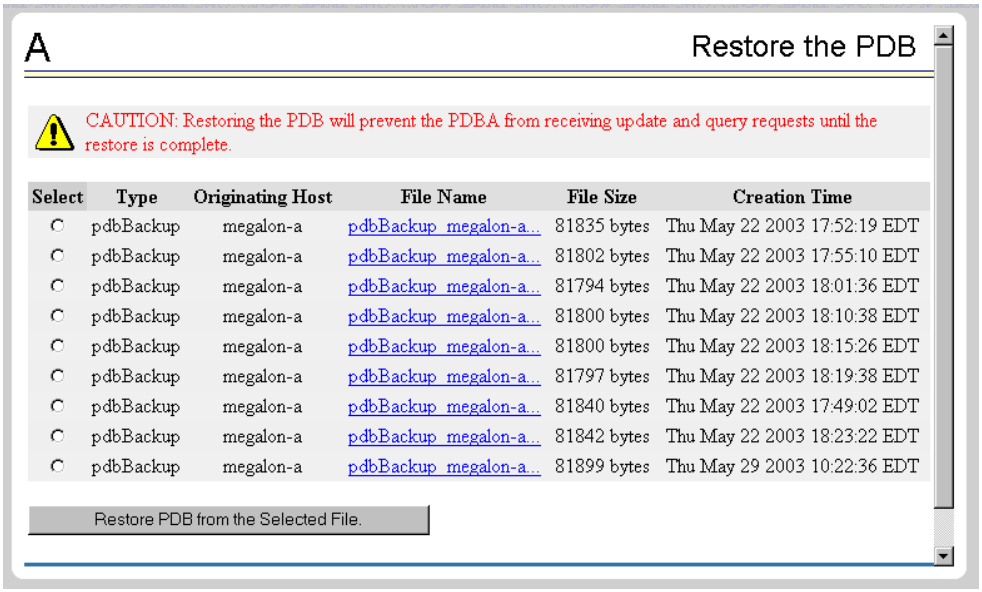
Figure 3-168. PDB Backup Successful Banner Message



Restore the PDB

The PDBA / Maintenance / Backup / Restore the PDB screen lets you restore the PDB (Provisioning Database) from a previous backup. See Figure 3-169 for the Restore the PDB screen.

Figure 3-169. Restore the PDB Screen

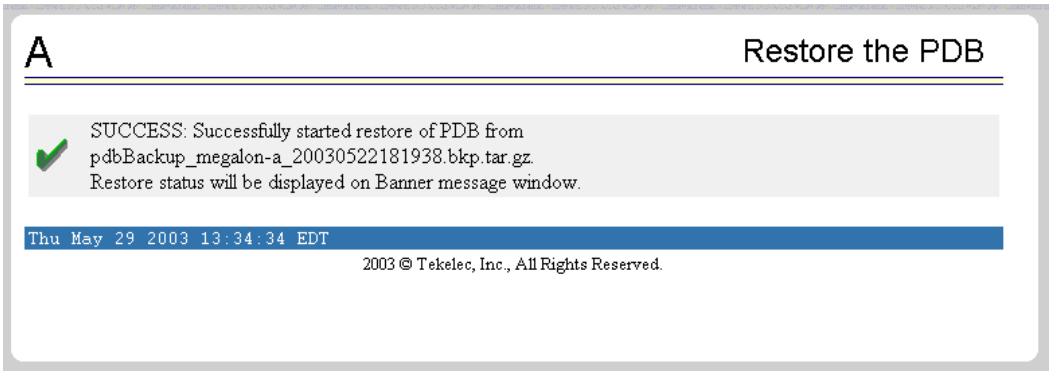


This screen is used in the "Restoring the PDB" procedure in the *EAGLE 5 ISS with T1000 AS MPS Platform Software and Maintenance Manual*.

CAUTION: Do not attempt to use this screen until you have contacted Customer Care Services for assistance. Restoring the PDB is service-affecting.

When the Restore the PDB process has started, the in-process screen will be displayed as shown in Figure 3-170. The status will be displayed in the Banner Message Window.

Figure 3-170. Restore the PDB Started Screen



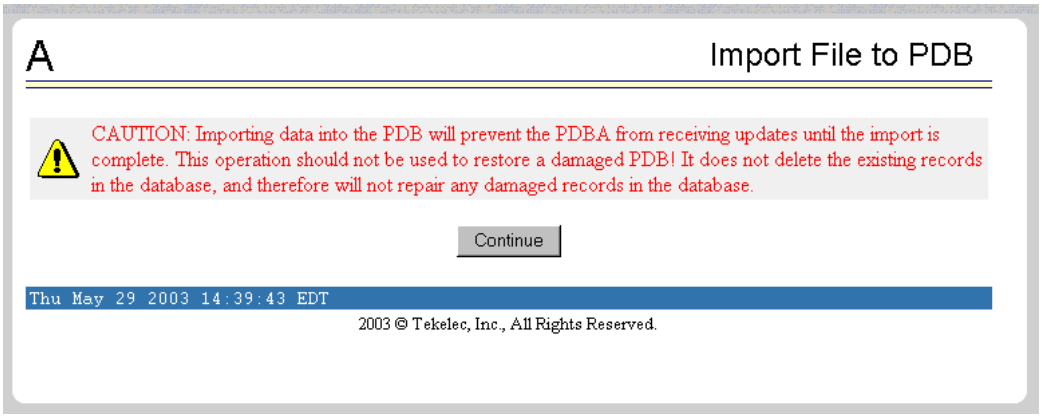
PDBA / Maintenance / Import File to PDB

The PDBA / Maintenance / Import File to PDB screen prompts you to import a file into the PDB. This action inserts new database records into the PDB by reading PDBI commands (refer to *Provisioning Database Interface Manual*) from the input file.

NOTE: Do not use this action to restore a damaged PDB!
This action does not delete the existing records in the database, and consequently does not repair any damaged records in the database.
To repair a damaged database, contact Customer Care Services for information and assistance; see "Customer Assistance" on page 1-4 for more information.

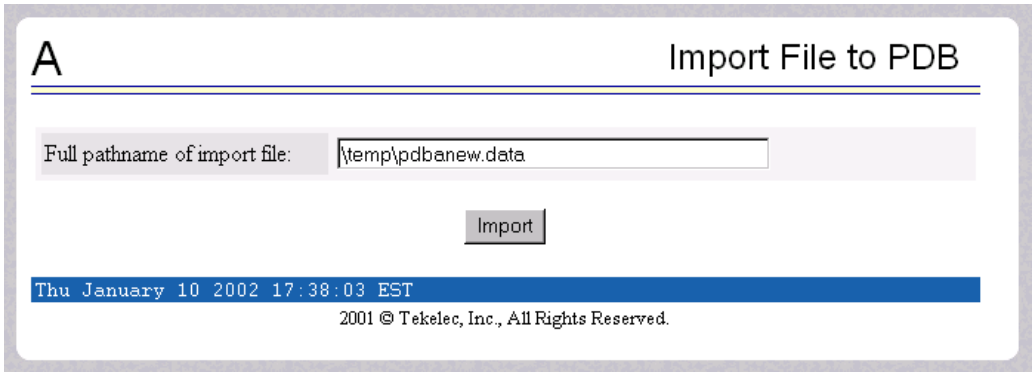
Although the input file is normally generated by the customer's provisioning application, the "PDBA / Maintenance / Export PDB to File" on page 3-119 action also generates a file suitable for importing with this command. See Figure 3-171 for the PDBA / Maintenance / Import File to PDB menu.

Figure 3-171. Import File to PDB Screen



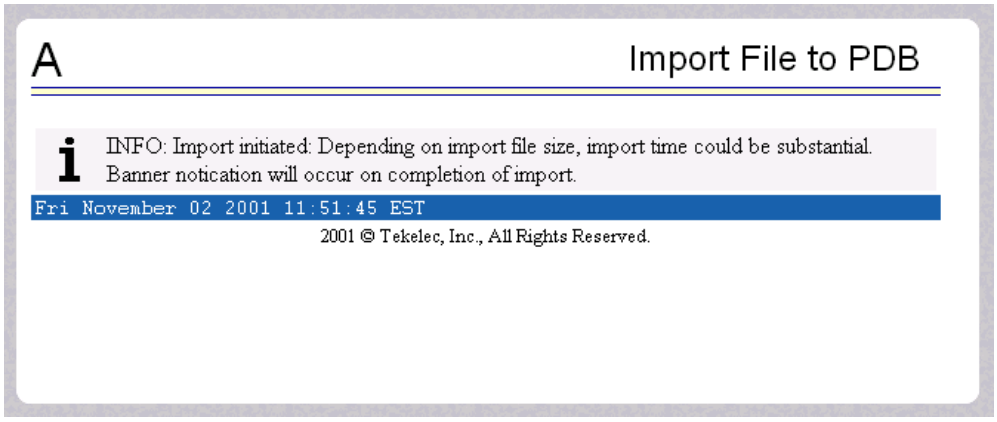
When you decide to import a file to the PDB, click the Continue button, and see the screen in Figure 3-172 that names the file to import.

Figure 3-172. Naming the File to Import to PDB



Specify the path and name of the file to import, and click the Import button. See the screen in Figure 3-173 that shows the file import has started.

Figure 3-173. Confirming Start of Import File to PDB



For additional information about Importing Files to the PDB, refer to the *Provisioning Database Interface Manual*, "Import/Export Files."

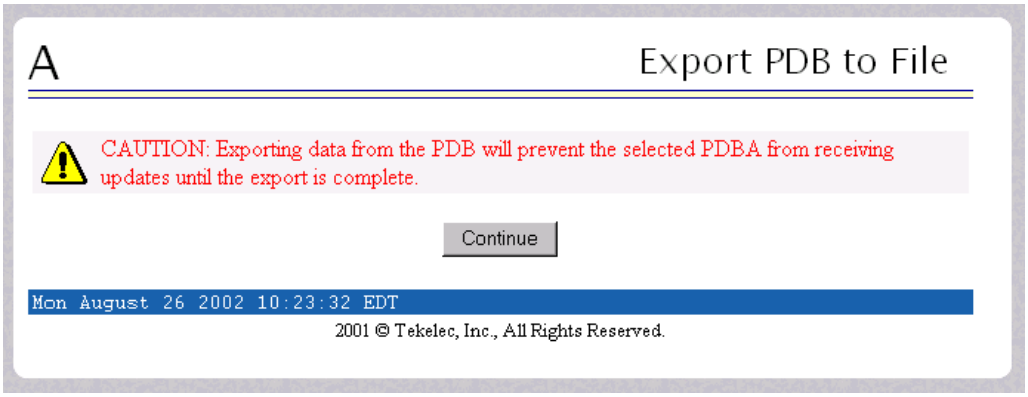
PDBA / Maintenance / Export PDB to File

This screen is used to export data to a specified location. The PDBA / Maintenance / Export PDB to File screen menu prompts for a file to export the PDB. This action writes the commands required to re-create each IMSI, IMEI, DN, DN Block, SP and RN to the specified file in a PDBI or CSV format. For additional information about PDBI format, refer to the *Provisioning Database Interface Manual*, "PDBI Format."

NOTE: Do not use this action as a substitute for "Backup the PDB". Do not use a file generated by this action to restore a damaged database! Use this action only a starting point for creating a file suitable for "PDBA / Maintenance / Import File to PDB" on page 3-117.

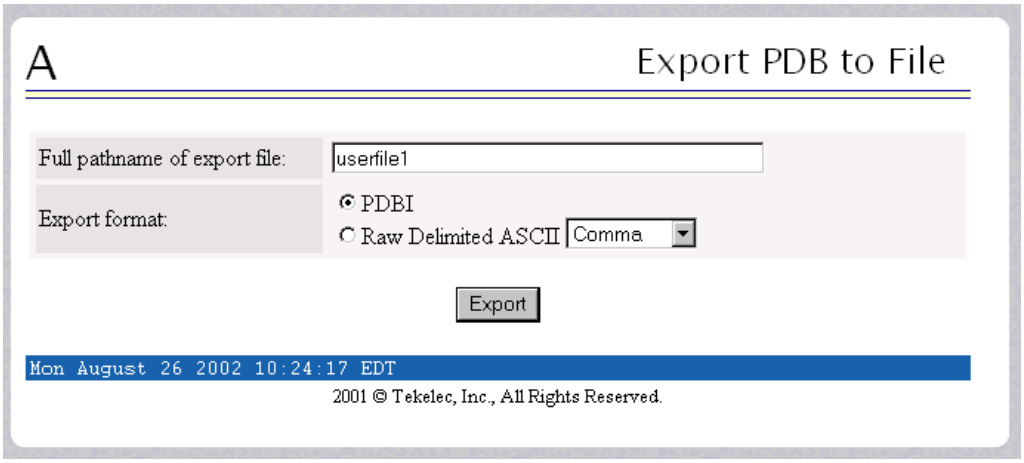
To export the PDB to a user file, enter a user filename of your choice. The EPAP automatically uses the default path **`/usr/external/logs/<user file name>`**. Figure 3-174 and Figure 3-175 show the screens to perform the PDBA / Maintenance / Export PDB to File screen.

Figure 3-174. Export PDB to File Screen



When you want to export a PDB to File, click the Continue button, and see the screen in Figure 3-175 that names the file to export.

Figure 3-175. Naming the File to Export to PDB



In the input field called 'Full pathname of export file', specify the filename of your choice for the PDB you want to export to file; the example uses the name '**`userfile1`**'. Select an export format, either the PDBI or raw delimited ASCII format; if the ASCII, select a delimiter from the drop-down menu. When you have made your selections, click the Export button.

The path to your copy of the exported file will be the EPAP default path **`/usr/external/logs/<user file name>`**.

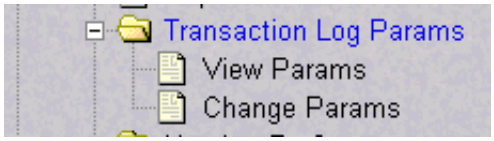
For more information about the PDBI and ASCII formats, refer to the *Provisioning Database Interface Manual,* "PDBI Format" and "Raw Delimited ASCII Format."

For additional information about Importing Files to the PDB, refer to the *Provisioning Database Interface Manual,* "Import/Export Files."

PDBA / Maintenance / Transaction Log Params

The PDBA / Maintenance / Transport Log Params menu lets you view and change the parameters of the transaction log for a file to which it can export the PDB. See Figure 3-176 for the Transport Log Params menu.

Figure 3-176. Transport Log Params Menu



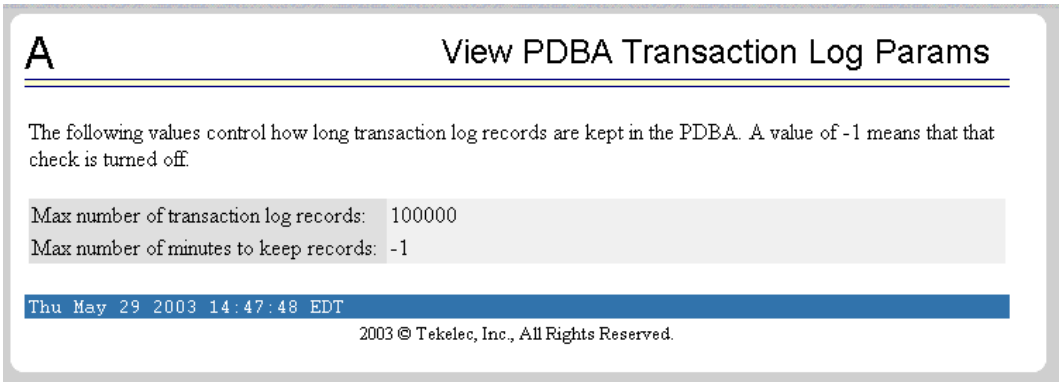
The PDBA / Maintenance / Transport Log Params menu provides these actions:

- "View Params" on page 3-121
- "Change Params" on page 3-122

View Params

The PDBA / Maintenance / Transport Log Params / View Params screen lets you display the current values of the PDBA Transaction Log parameters. These parameters control how frequently the PDBA transaction log is cleaned up. See Figure 3-177 for the View PDBA Transaction Log Params screen.

Figure 3-177. View Params Screen



See "Change Params" on page 3-122 for details about the parameters.

Change Params

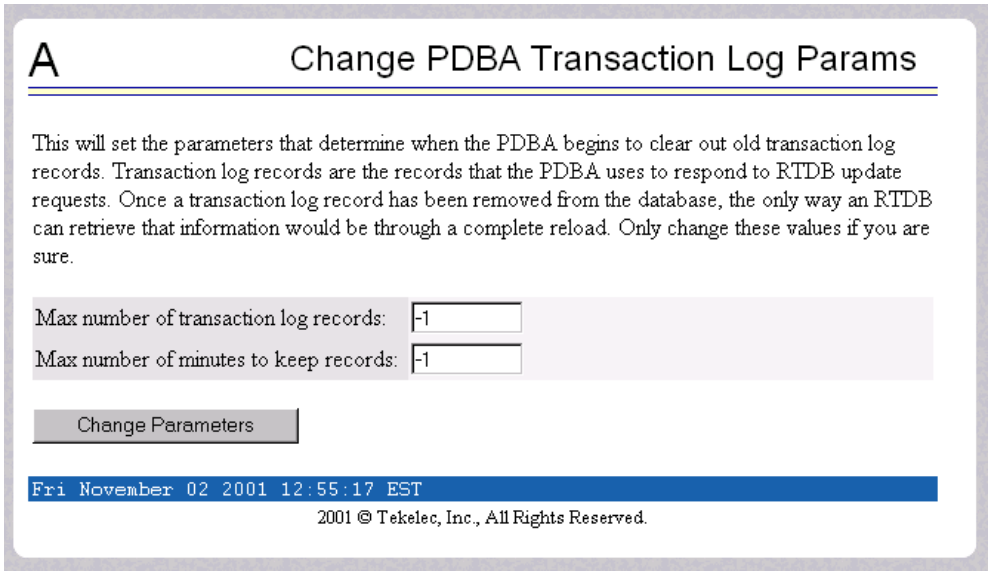
The PDBA / Maintenance / Transport Log Params / Change Params screen lets you change the frequency that old transaction log records are removed.

As described in the Change PDBA Transaction Log Params screen, you can change parameters that control when the PDBA removes old transaction log records. (Transaction log records are the records of PDBA responses to RTDB update requests.) You can specify the maximum number of records to keep or the length of time (expressed in minutes) to keep records. When either limit is reached, the oldest records are automatically deleted.

When a transaction log record has been removed from the database, the RTDB can retrieve that information only through a complete reload. Therefore, change these values only if you are certain.

See Figure 3-178 for the Change PDBA Transaction Log Params screen.

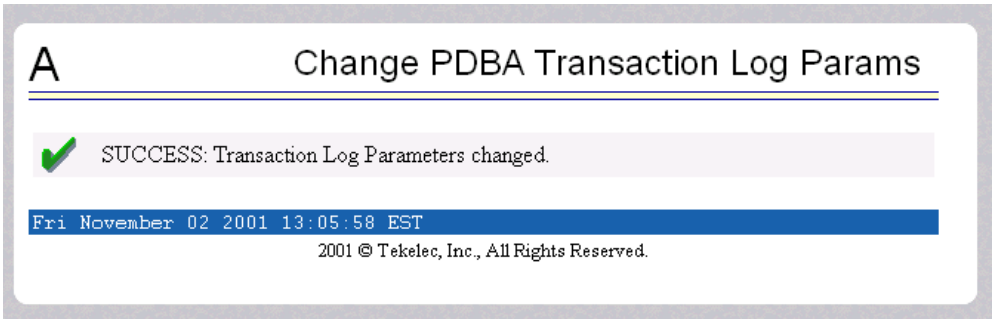
Figure 3-178. Change PDBA Transaction Log Params Screen



You should enter the maximum number of transactions log record and the maximum number of minutes to keep record. The maximum number is specified as '-1'.

When you change either the number of records or number of minutes to keep in the Transaction Log, click the Change Parameters button, and see the screen in Figure 3-179 that confirms the change of parameters.

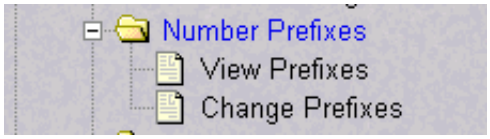
Figure 3-179. Confirming Change of PDBA Transaction Log Params



PDBA / Maintenance / Number Prefixes

The PDBA / Maintenance / Number Prefixes menu lets you view and change the parameters of the PDBA prefixes. See Figure 3-180 for the PDBA / Maintenance / Number Prefixes menu.

Figure 3-180. PDBA / Maintenance / Number Prefixes Menu



The handling of number prefixes is a convention followed by EPAP, PDBI, and the G-Flex, G-Port, and INP systems. For more information about "Number Prefixes," refer to the *Provisioning Database Interface Manual.*

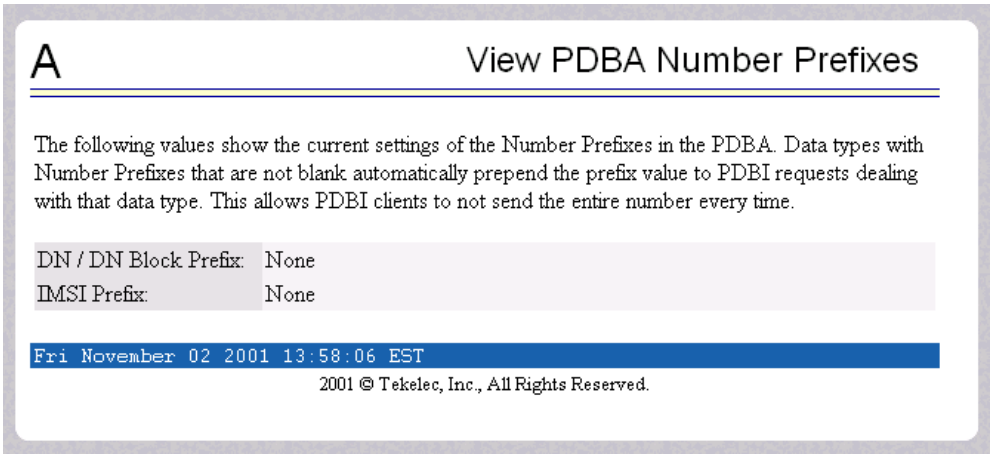
The PDBA / Maintenance / Number Prefixes menu provides these actions:

- "View Prefixes" on page 3-124
- "Change Prefixes" on page 3-124

View Prefixes

The PDBA / Maintenance / Number Prefixes / View PDBA Number Prefixes screen lets you display the current values for the PDBA number prefixes. See the Change PDBA Number Prefixes screen (Figure 3-182) for a detailed description of those parameters. See Figure 3-181 for the View PDBA Number Prefixes screen.

Figure 3-181. View PDBA Number Prefixes Screen

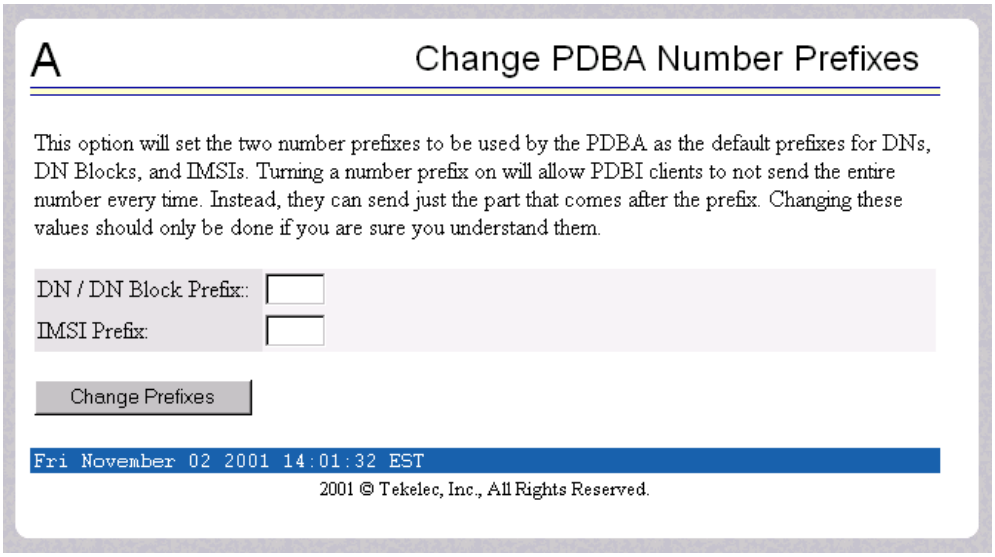


Change Prefixes

The PDBA / Maintenance / Number Prefixes / Change PDBA Number Prefixes screen lets you set the two number prefixes used by the PDBA as default prefixes for DNs, DN blocks, and/or IMSIs. Turning on a number prefix allows PDBI clients to avoid sending an entire number on every transmission; instead, only the portion following the prefix is sent. For details about the concept of "Number Prefixes," refer to the *Provisioning Database Interface Manual*.

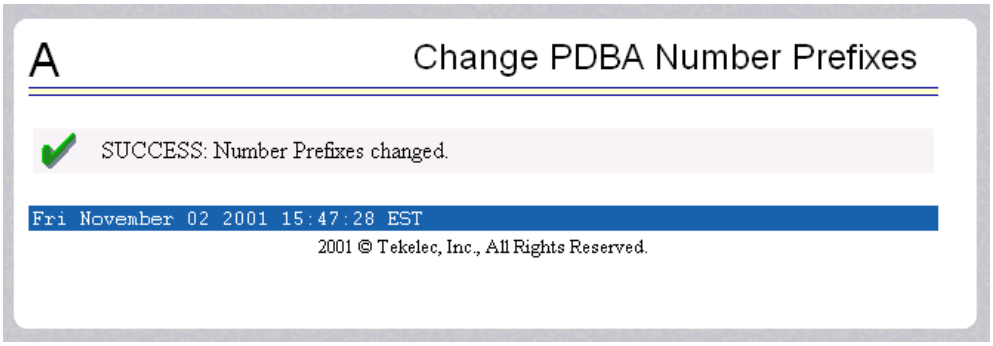
See Figure 3-182 for the Change PDBA Number Prefixes screen.

Figure 3-182. Change PDBA Number Prefixes Screen



You can enter either the DN or DN block prefix and/or the IMSI prefix. When you have entered the values to specify, click the Change Prefixes button, and see the screen in Figure 3-183 that confirms the change of parameters.

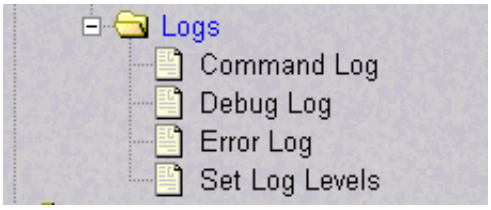
Figure 3-183. Confirmed Change of PDBA Number Prefixes



PDBA / Maintenance / Logs

The PDBA / Maintenance / Logs menu allows the user to view the PDB error, command, and debug logs, as well as set log threshold values. See Figure 3-184 for the PDBA / Maintenance / Logs menu.

Figure 3-184. PDBA / Maintenance / Logs Menu



NOTE: The contents of these logs are intended for the use of Customer Care Services in diagnosing system operation and problems. If you require assistance with your system involving the use of the Logs menu, contact Customer Care Services. See "Customer Assistance" on page 1-4 for more information.

The PDBA / Maintenance / Logs menu provides these actions:

- "View Command Log" on page 3-126
- "View Debug Log" on page 3-126
- "View Error Log" on page 3-126
- "Set Log Levels" on page 3-127

View Command Log

The PDBA / Maintenance / Logs / View Command Log menu selection lets you view the current PDBA Command Log. To be able to see historic PDBA command logs, use the View Any File action. Refer to "View Any File" on page 3-52.

View Debug Log

The PDBA / Maintenance / Logs / View PDBA Debug Log menu selection lets you view the current PDBA Debug Log. To be able to see historic PDBA Debug logs, you must use the View Any File action. Refer to "View Any File" on page 3-52.

View Error Log

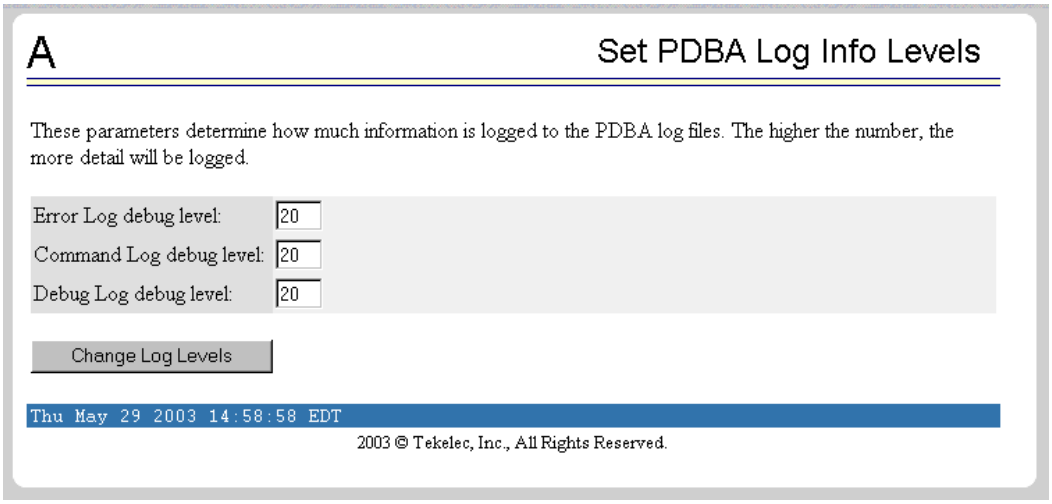
The PDBA / Maintenance / Logs / View PDBA Error Log menu selection lets you view the current PDBA Error Log. To be able to see historic PDBA Error logs, you must use the View Any File action. Refer to "View Any File" on page 3-52.

Set Log Levels

The PDBA / Maintenance / Logs / Set PDBA Log Info Levels screen prompts you for the level of detail to be written to the error, debug, and command logs. Setting a higher debug level results in logs being recorded with more detail, while a lower level contains less detail. Setting the debug level to a value of 0 turns logging off.

See Figure 3-185 for the Set PDBA Log Info Levels screen.

Figure 3-185. Set PDBA Log Info Levels Screen



NOTE: The levels for error, command and debug logs should be set only under the guidance of Customer Care Services. See "Customer Assistance" on page 1-4 for more information.

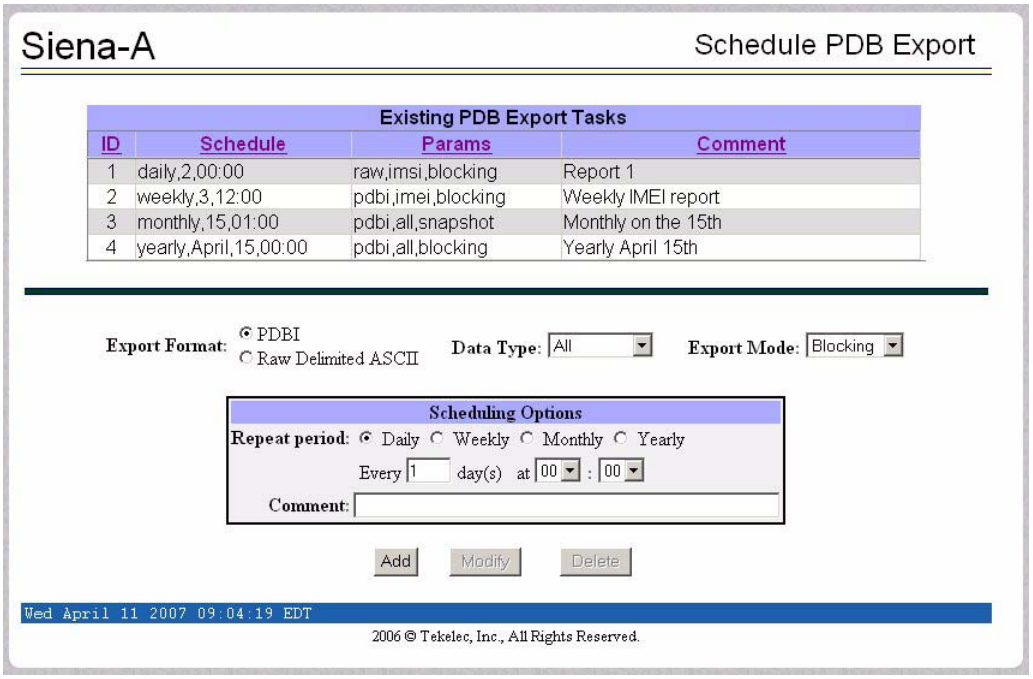
PDBA / Maintenance / Schedule PDB Export

This screen is used for the the Automatic/Schedule Export Mode. This screen is used to automatically export PDB data to a file that is then available to a client SFTP. This screen allows the user to export a single object type rather than the complete database. By default, all object types are exported. Through this screen the customer has a choice of what data to be exported as well as the day and time of day the data is exported.

The export can be scheduled at a specific time for each of the following repeat periods: every N number of days (N can be up to 365), on specified days of the week, on a specified day of the month, or on a specified day of the year. The Schedule Export screen is used to display any existing PDB export tasks and to create a task by specifying the data type, the export format (PDBI or CSV), the export mode (blocking, snapshot, or real-time) as well as the time and repeat period. In addition, a Comment field is available to describe the task.

See Figure 3-186 for an example of the Schedule PDB Export screen.

Figure 3-186. Schedule PDB Export Screen



Existing PDB Export Tasks

The Existing PDB Export Tasks portion at the top of the screen displays all currently scheduled exports in table format. Clicking on a column heading causes the entries in that column to be sorted, either alphabetically or numerically, depending on whether the column entries start with a letter or a number. Clicking the column again sorts the entries in the opposite order.

Clicking on a row causes the data contained in that task to be displayed in the data entry fields below the table, for viewing, modification, or deletion.

Export Format, Data Type, and Export Mode

For more information about the Export Format, Data Type, and Export Mode choices, refer to the *Provisioning Database Interface Manual*.

Scheduling Options

The Scheduling Options section of the Schedule PDB Export screen allows the user to choose how often to repeat the scheduled export and to specify the exact day and time. The appearance of this section changes depending on which radio button in the Repeat Period is selected:

- The following fields are the same among the various Repeat Period selections (for more information about fields that differ depending on the Repeat Period selected, see "Variable Fields in Scheduling Options" on page 3-129):
  - **Start Time:** Select the values for the hour and minute to start the scheduled export from the two drop-down boxes at the right of the Scheduling Options section. The hour drop-down uses a 24-hour clock. For example, if you want the export to start at 10:30 PM, select 22 from the left drop-down box and select 30 from the right drop-down box.
  - **Comment:** Use this optional field to add comments about this export. The content of this field is stored and displayed on the GUI, but it is not used otherwise.

Variable Fields in Scheduling Options

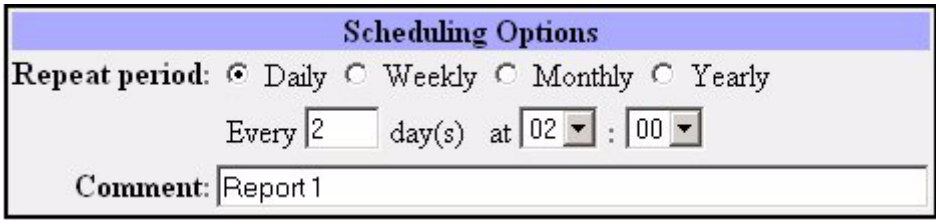
The following sections describe how the Scheduling Options fields change depending on the Repeat Period that is selected.

Daily Repeat Period

To schedule an export to be run every N days, select the Daily radio button, specify a number (N) to indicate that the export should be run every N days, select the time, and optionally enter a comment, as shown in Figure 3-187.

NOTE: Although the maximum value allowed in the day(s) field is 365, if an export is desired to run once a year, it is recommended to use the yearly repeat period so that leap years are properly treated (see "Yearly Repeat Period" on page 3-130).

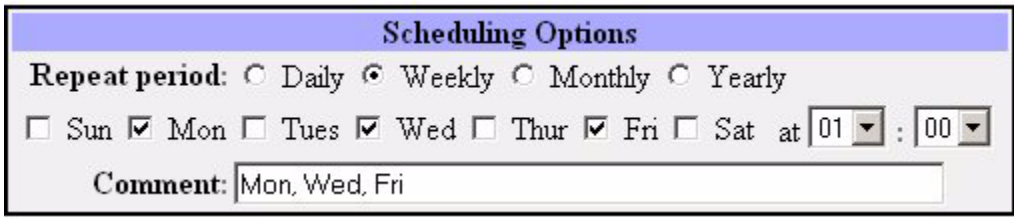
Figure 3-187. Daily Scheduling Options



Weekly Repeat Period

To schedule an export to be run each week, select the Weekly radio button, select one or more days of the week, select the time, and optionally enter a comment, as shown in Figure 3-188.

Figure 3-188. Weekly Scheduling Options

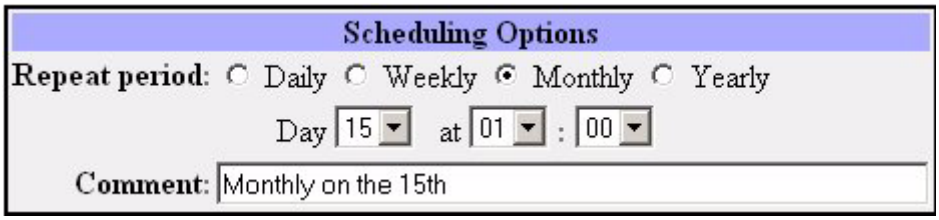


Monthly Repeat Period

To schedule an export to be run one day each month, select the Monthly radio button, select a numeric day of the month, select the time, and optionally enter a comment, as shown in Figure 3-189.

NOTE: For months that do not contain the number of days specified in the Day field, the export will run on the first day of the following month. (For example, if the Day field value is 29, the export will run on March 1 rather in February for any year that is not a leap year.)

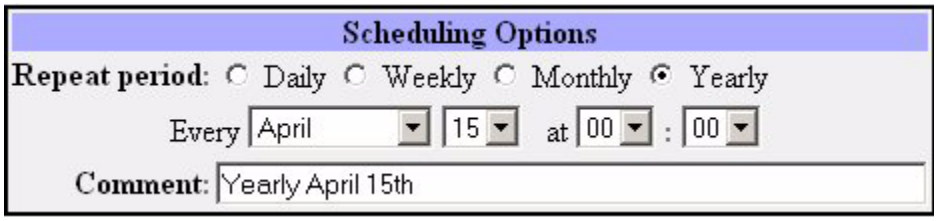
Figure 3-189. Monthly Repeat Options



Yearly Repeat Period

To schedule an export to be run one day each year, select the Yearly radio button, select a numeric day of the year, select the time, and optionally enter a comment, as shown in Figure 3-190.

Figure 3-190. Yearly Repeat Options



Add, Modify, and Delete Buttons

The Add, Modify, and Delete buttons are located at the bottom of the Schedule PDB Export screen.

Add Button. To add a scheduled PDB export, enter all the data to describe the export, and click the Add button.

If the task, as described by the current data in the data entry fields, does not exactly match an existing task, a new task is scheduled. If the task exactly matches an existing task, an error message is displayed.

Modify Button. To modify a scheduled PDB export, click that export task in the Existing PDB Export Tasks table, change any data that describes the export, and click the Modfy button.

The Modify button is selectable only when an entry in the Existing PDB Export Tasks table at the top of the screen has been selected and one or more fields on the screen has been changed.

If the task, as described by the current data in the data entry fields, does not exactly match an existing task, a new task is scheduled. If the task exactly matches an existing task, an error message is displayed.

Delete Button. To delete a scheduled PDB export, click that export in the Existing PDB Export Tasks table, and click the Delete button.

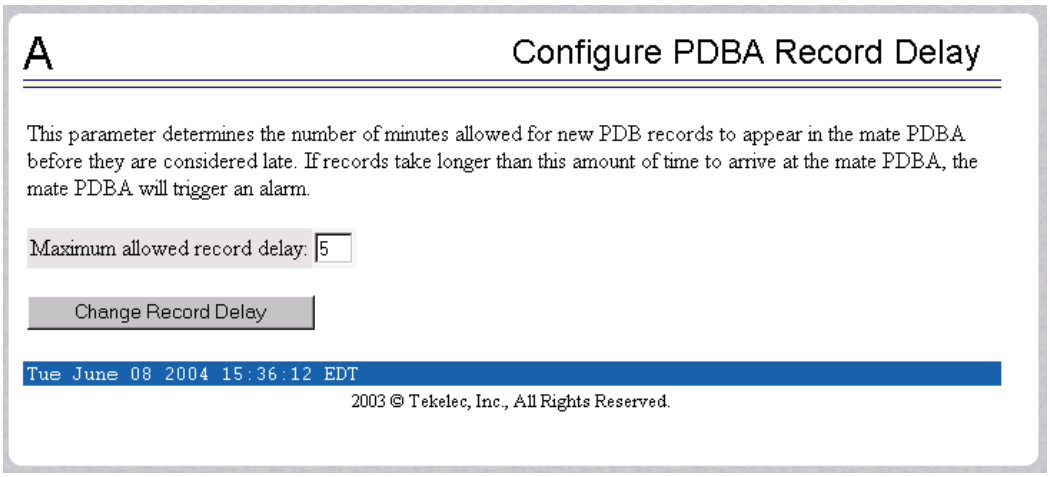
The Delete button is selectable only when an entry in the Existing PDB Export Tasks table at the top of the screen has been selected.

PDBA / Maintenance / Configure PDBA Record Delay

This screen is used to configure the amount of time (in minutes) allowed for new PDB records to appear in the mate PDBA before they are considered late. If records take longer than this amount of time to arrive at the mate PDBA, the mate PDBA will trigger an alarm. This value can be set from 1 to 300. The default value is 15.

See Figure 3-191 for an example of the Configure PDBA Record Delay screen.

Figure 3-191. Configure PDBA Record Delay Screen

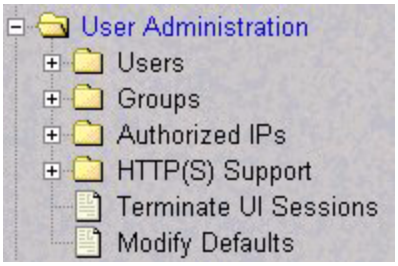


User Administration Menu

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.

See the User Administration menu in Figure 3-192.

Figure 3-192. 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 EPAP 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 EPAP 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 configurable number, with a default of **3** (three). This restriction is turned off if N is set to 0 by the administrator.

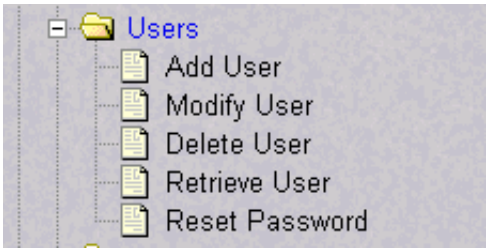
The User Administration menu performs administration functions for users and groups, and handles terminating active sessions and modifying system defaults. See these topics discussed:

- "Users" on page 3-134
- "Groups" on page 3-148
- "Authorized IPs" on page 3-155
- "HTTP(S) Support" on page 3-159
- "Terminate UI Sessions" on page 3-161
- "Modify Defaults" on page 3-162

Users

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 User menu in Figure 3-193.

Figure 3-193. Users 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 EPAP user interface comes pre-defined with user interface users in order to provide a seamless transition to the graphical user interface. This is done by duplicating the Unix user logins and permissions that existed on the original (version 1.0) text-based UI. Refer to Table 3-3 for the current login names.

Table 3-3. EPAP UI Logins

Login Name	Access Granted
epapmaint	Maintenance menu and all submenus
epapdatabase	Database menu and all submenus
epapdebug	Debug menu and all submenus
epapplatform	Platform menu and all submenus
uiadmin	User Administration menu
epapall	All of the above menus
epapconfig	Configuration menu and all submenus (text-based UI)

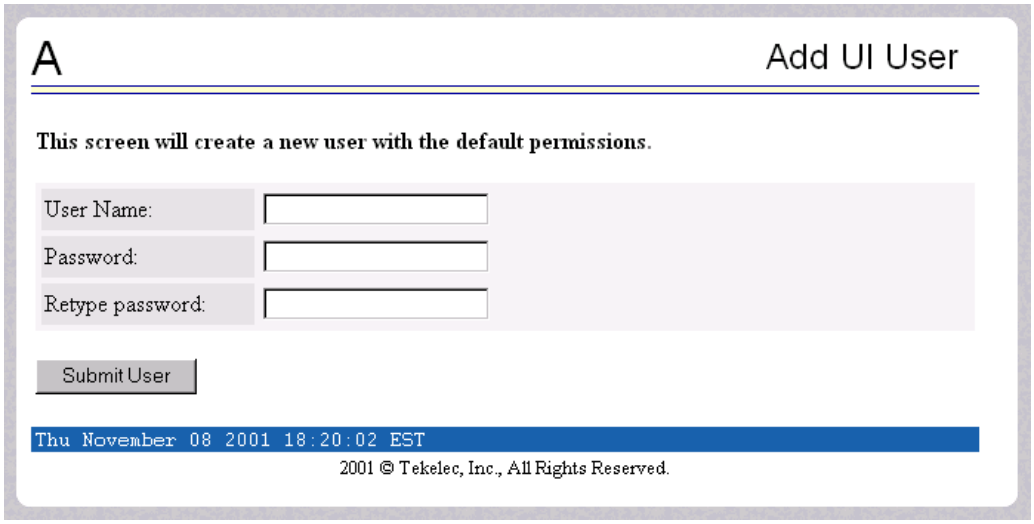
The Users menu performs the following actions:

- "Add User" on page 3-136
- "Modify User" on page 3-137
- "Delete User" on page 3-142
- "Retrieve User" on page 3-143
- "Reset Password" on page 3-146

Add User

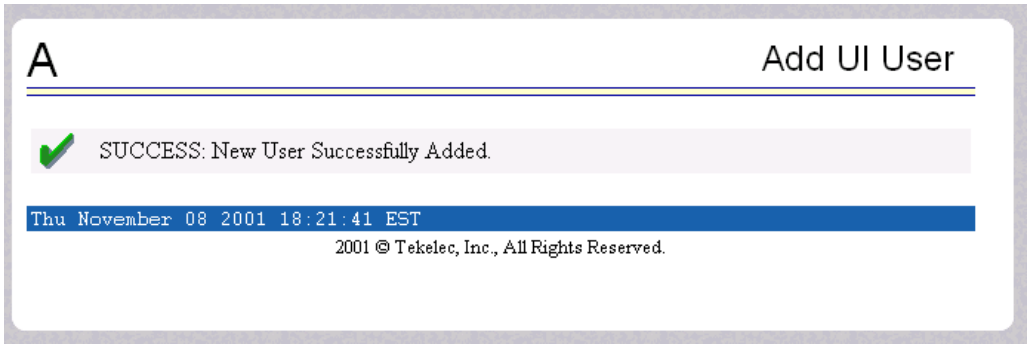
The User Administration / Users / Add UI User screen is used to add a new user interface user name and a default password. Figure 3-194 shows the Add UI User screen.

Figure 3-194. Add UI User Screen



See Figure 3-195 for the screen confirmation of the newly added user.

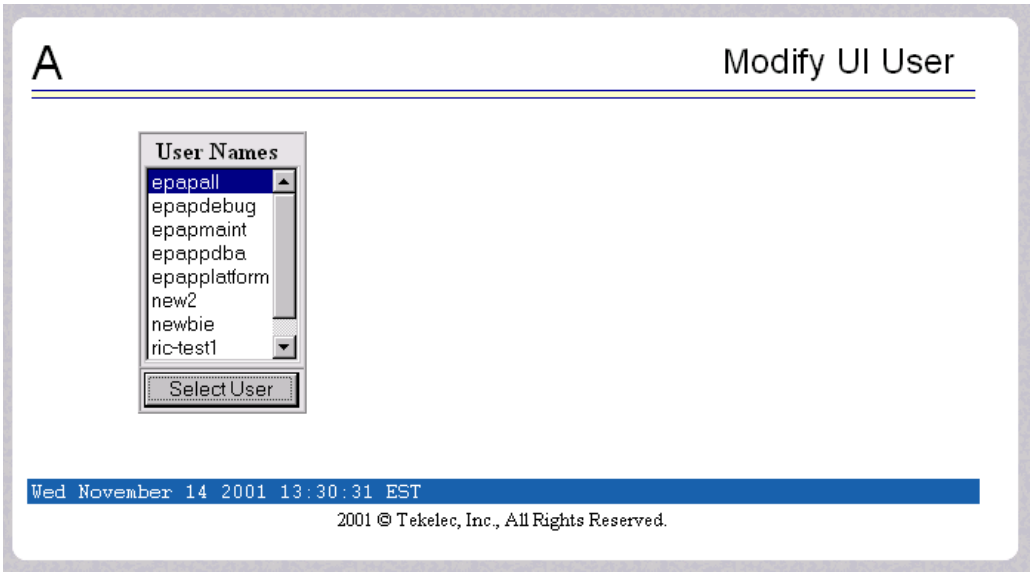
Figure 3-195. Success in Adding UI User



Modify User

The User Administration / Users / Modify UI User screen is used to change a user permission profile. The administrator must first select a user name from the list of current users, as shown in Figure 3-196.

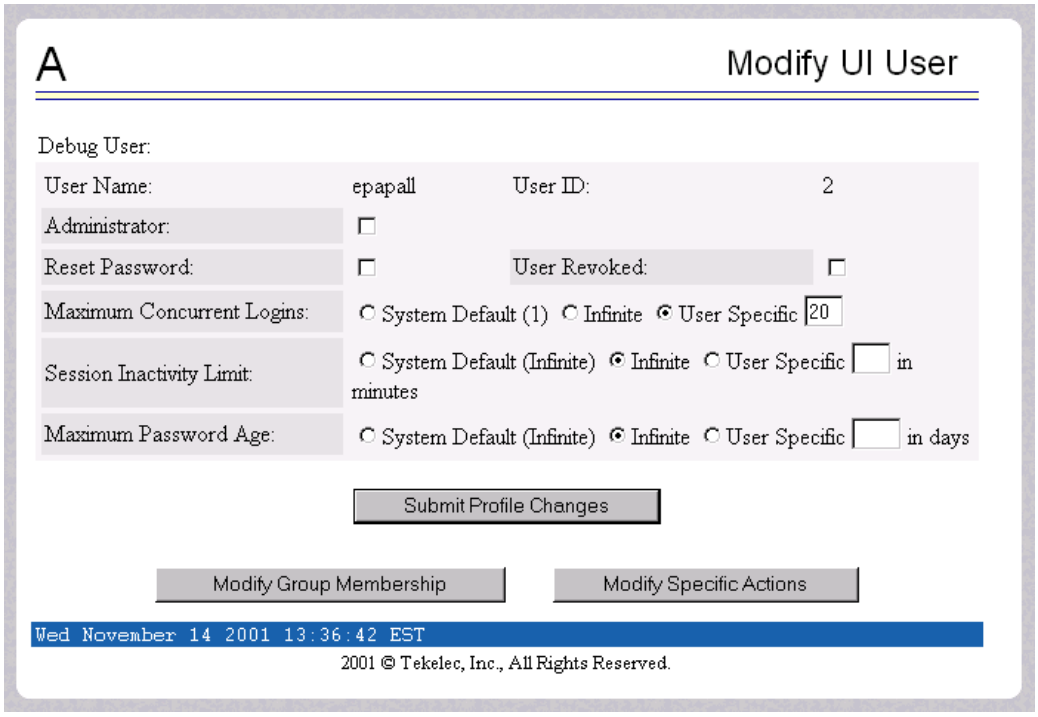
Figure 3-196. Modify UI User Screen



After selecting a User Name in the previous screen, the screen to specify the user permissions appears, as shown in Figure 3-197. In this screen, the permissions allowed to the user can viewed and specified.

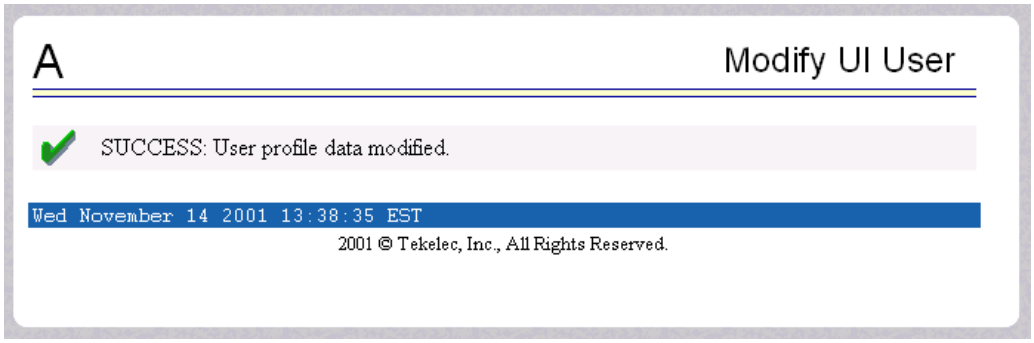
You can directly specify the number of concurrent log-ins, an inactivity time limit, and a password age limit. In addition, you can modify group membership data and specific actions that the user is permitted. See Figure 3-197 to see how to specify user modifications.

Figure 3-197. Specify the Modify UI User Screen



When modifying any of the direct entries, such as concurrent logins or inactivity, and click the Submit Profile Changes, the following screen Figure 3-198 is displayed.

Figure 3-198. Confirming Modify UI User Profile Changes



After clicking the Modify Group Membership in Figure 3-197, the screen displays the group membership choices available for the user. See Figure 3-199.

Figure 3-199. Modify UI User's Group Membership

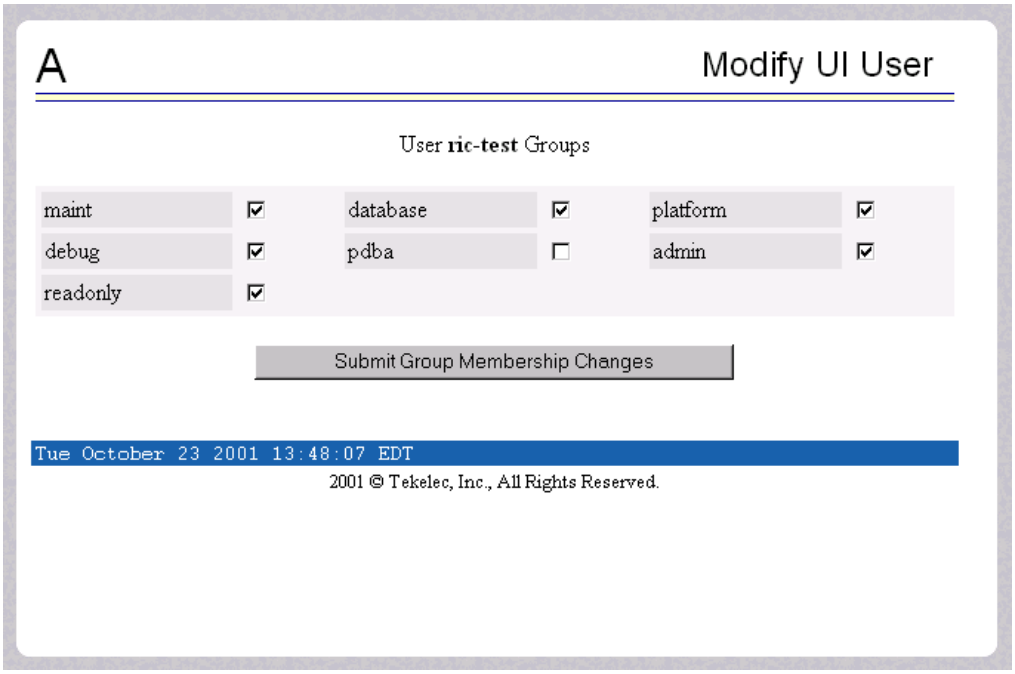
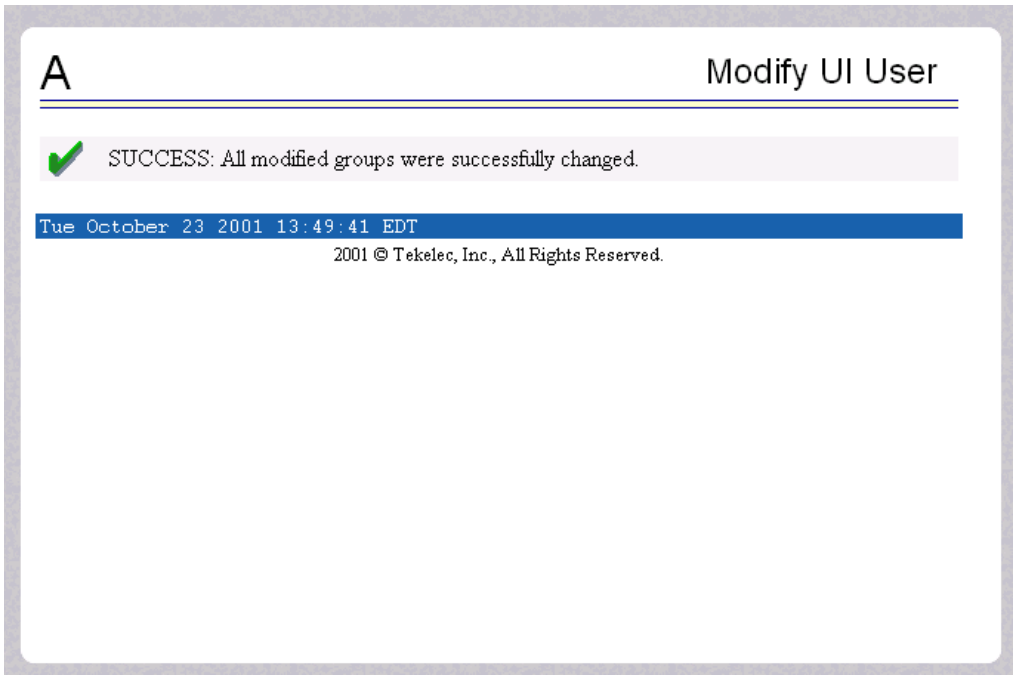


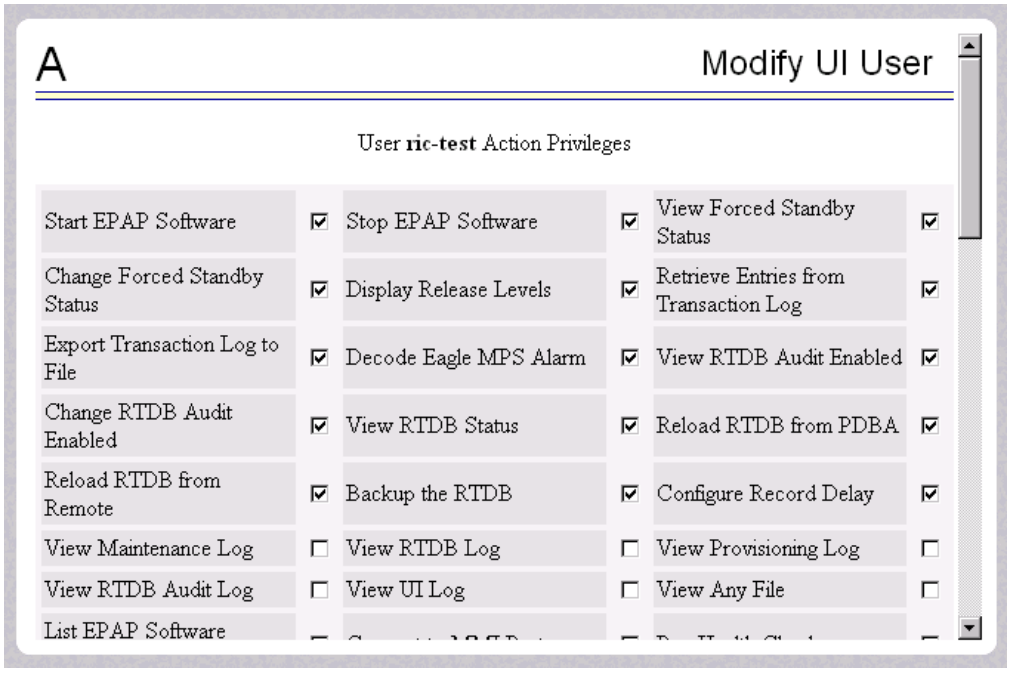
Figure 3-200 illustrates the confirmation screen used to submit changes for group membership.

Figure 3-200. Confirming Modify UI User Group Changes



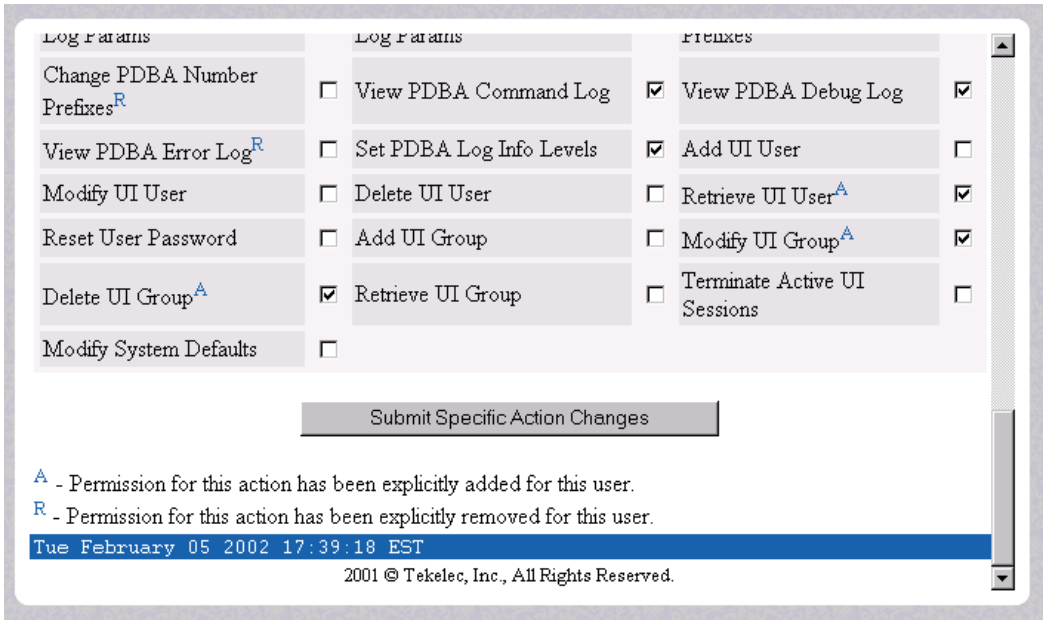
When you click Modify Specific Actions in Figure 3-197, the screen displays Action Privileges you can specify for the user you are modifying. See Figure 3-201.

Figure 3-201. Modify UI User's Specific Actions



This screen contains many selections from which to choose. Figure 3-202 shows the continuation of the screen and the Submit button to press when you are done.

Figure 3-202. Continuing Modify UI User's Specific Actions



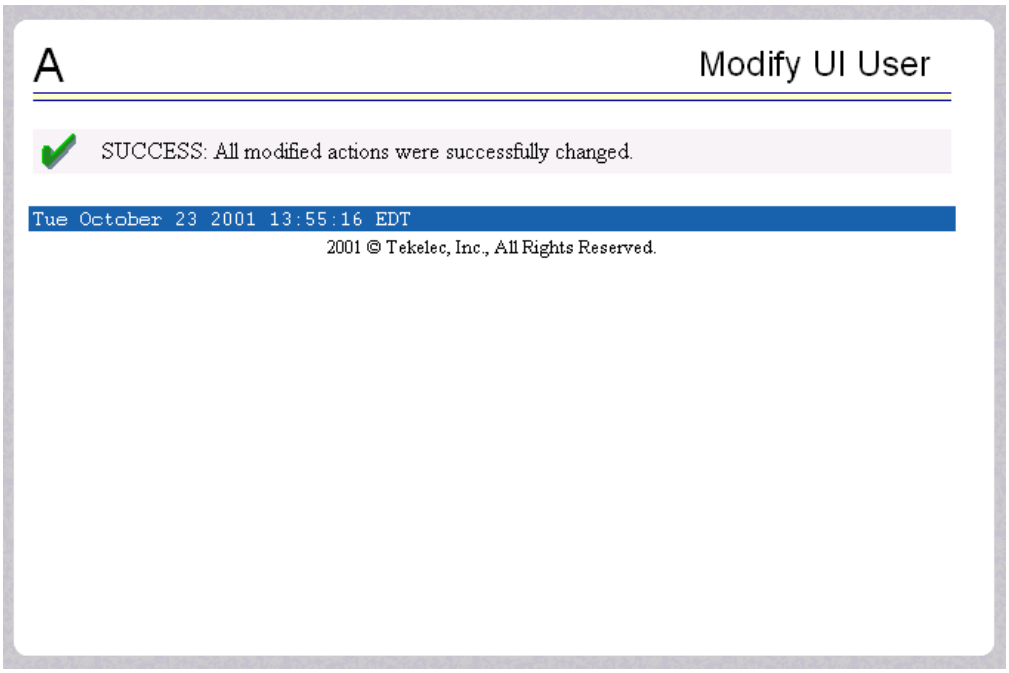
The bottom of the Modify UI User's Special Actions screen contains these explanatory notes:

- 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 3-203 shows the system accepting your change in action privileges for the specified user.

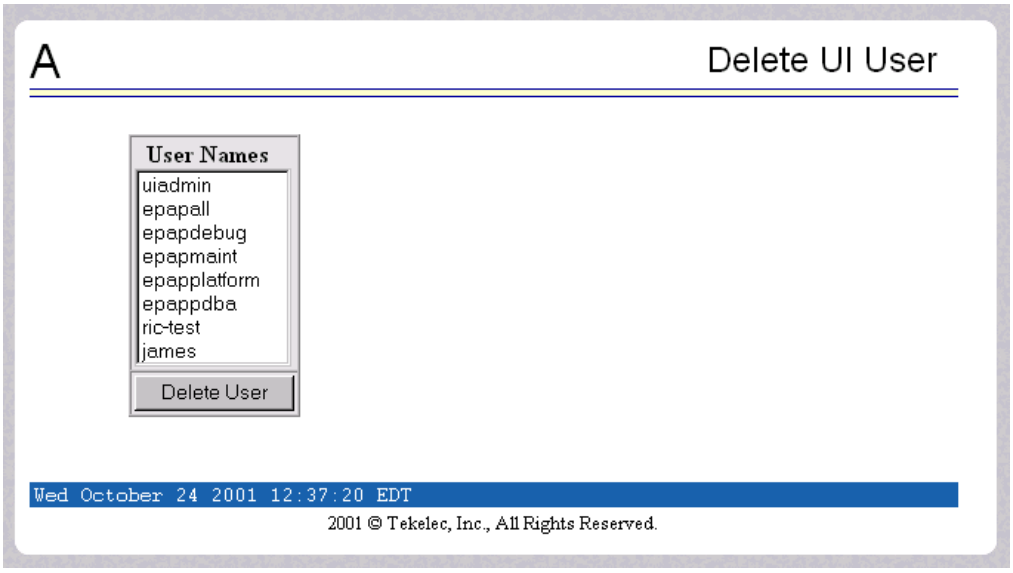
Figure 3-203. Confirming Modify UI User Specific Actions Changes



Delete User

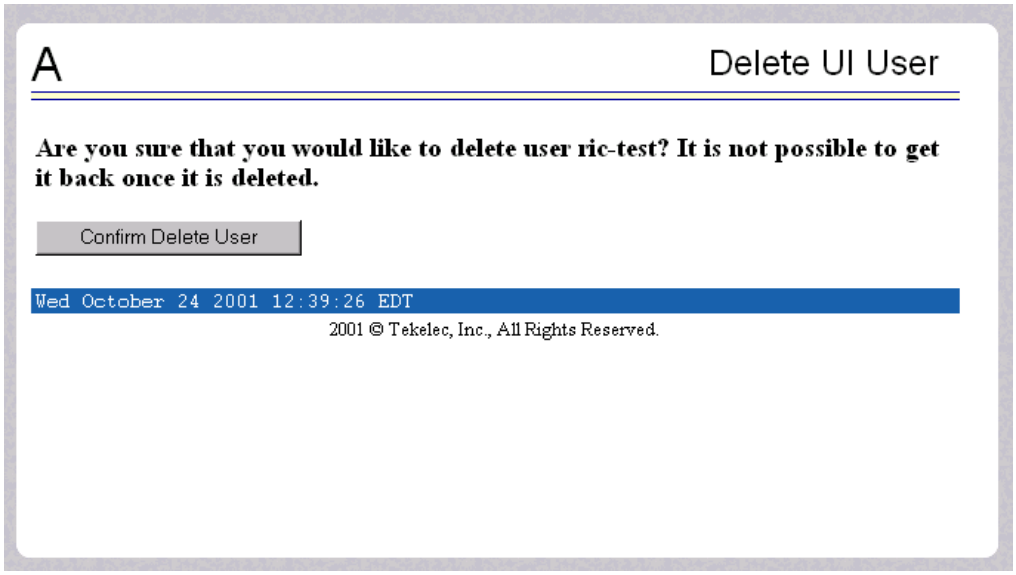
The User Administration / Users / Delete UI User screen lets an administrator remove a user name from the list of user interface names. First you select the user name to be deleted and click the Delete User button, shown in Figure 3-204.

Figure 3-204. Delete UI User Screen



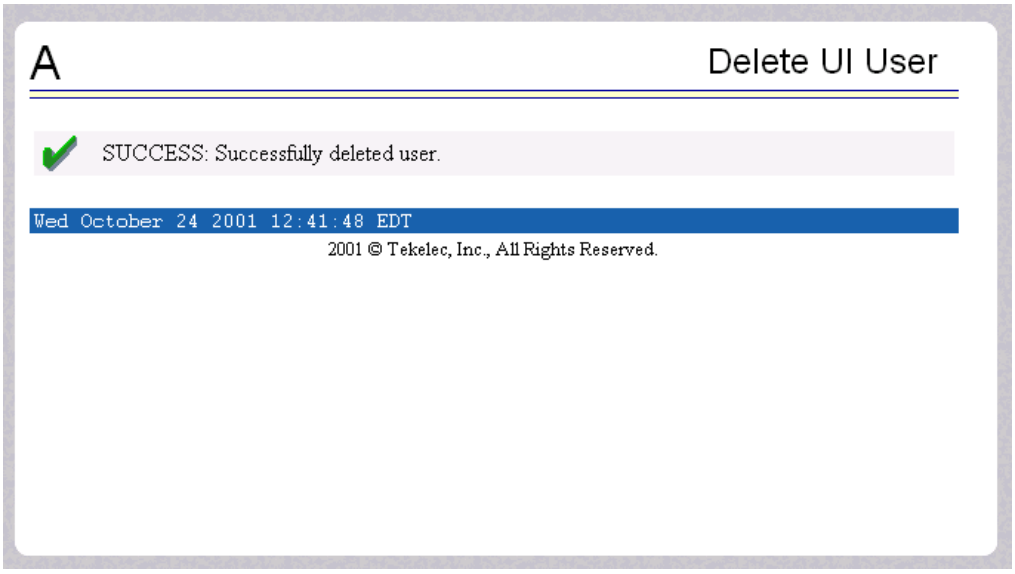
Next a confirmation screen appears, as shown in Figure 3-205.

Figure 3-205. Requesting Confirmation of User Deletion



Finally, the screen shows the user has been successfully removed as shown in Figure 3-206.

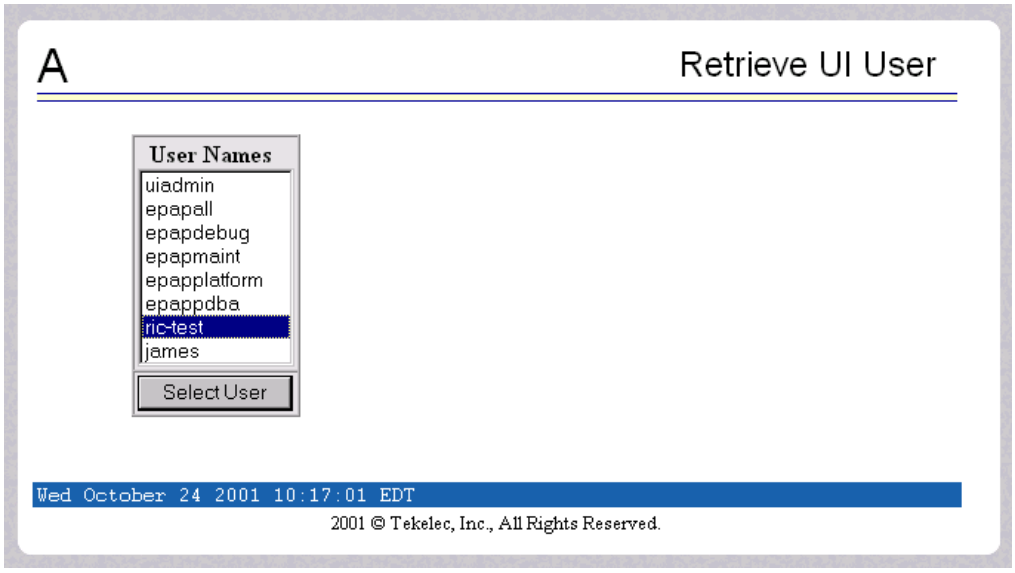
Figure 3-206. Confirming Deletion of the User



Retrieve User

The User Administration / Users / Retrieve UI 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 3-207.

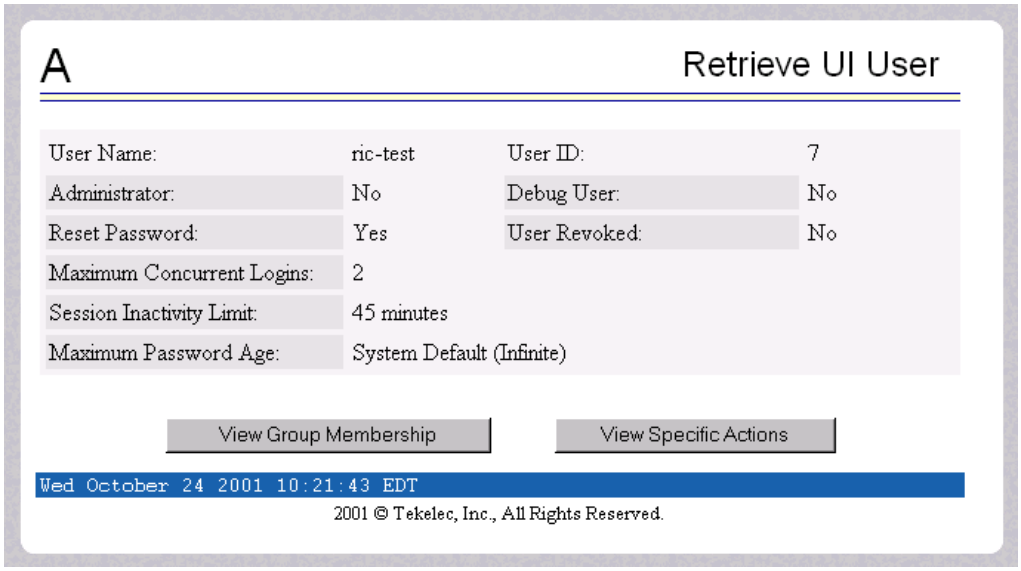
Figure 3-207. Select a User to Retrieve Screen



After you select a User Name in the screen above, the screen to view the user permissions appears, as shown in Figure 3-208. There you can view the permissions allowed to this user.

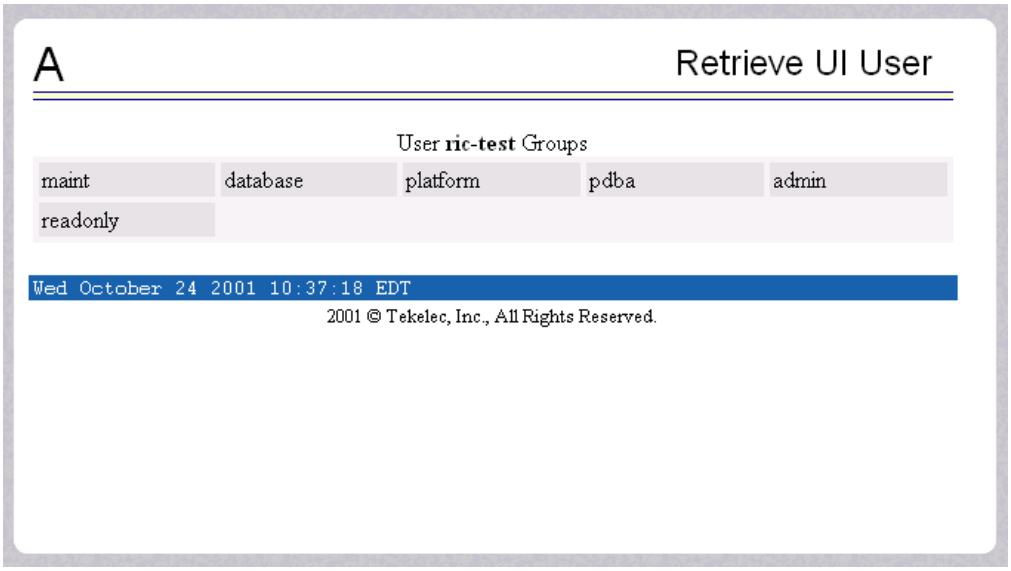
You can directly see certain information such as the maximum allowed number of concurrent log-ins and the inactivity time limit. In addition, you can go on to view the user's group membership data and specific actions (privileges). See Figure 3-208 for the user's permissions and privileges.

Figure 3-208. Retrieval of UI User Information Screen



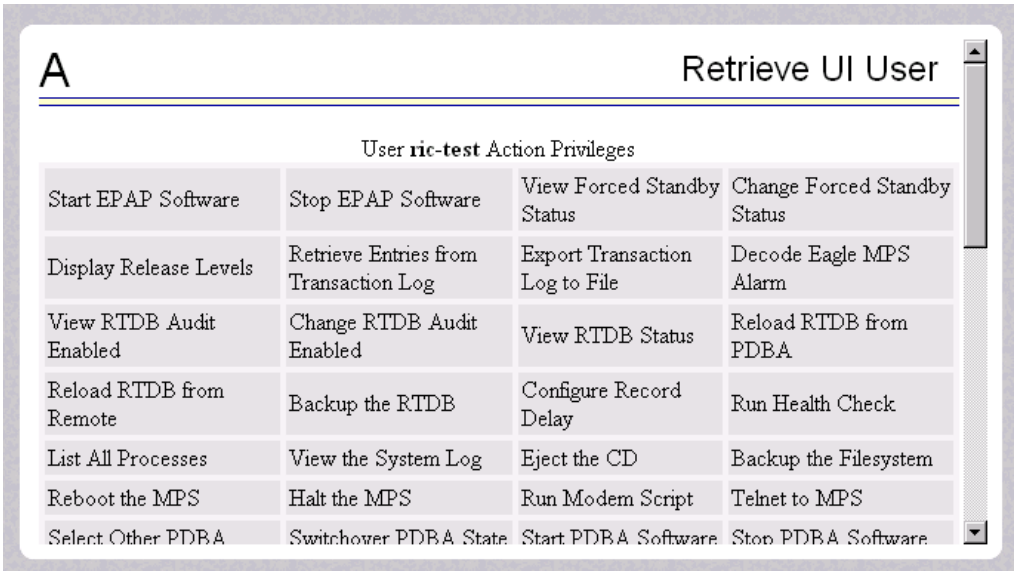
After you examine this screen, you can also continue to the view the group membership by clicking the View Group Membership button. You see the user's memberships in Figure 3-209.

Figure 3-209. Viewing the UI User's Group Membership Screen



When you click the View Specific Actions in the Retrieve UI User screen in Figure 3-208, you see the user privileges shown in Figure 3-210. This screen contains many privileges to display. Figure 3-211 shows the continuation of the screen.

Figure 3-210. Viewing User Privileges

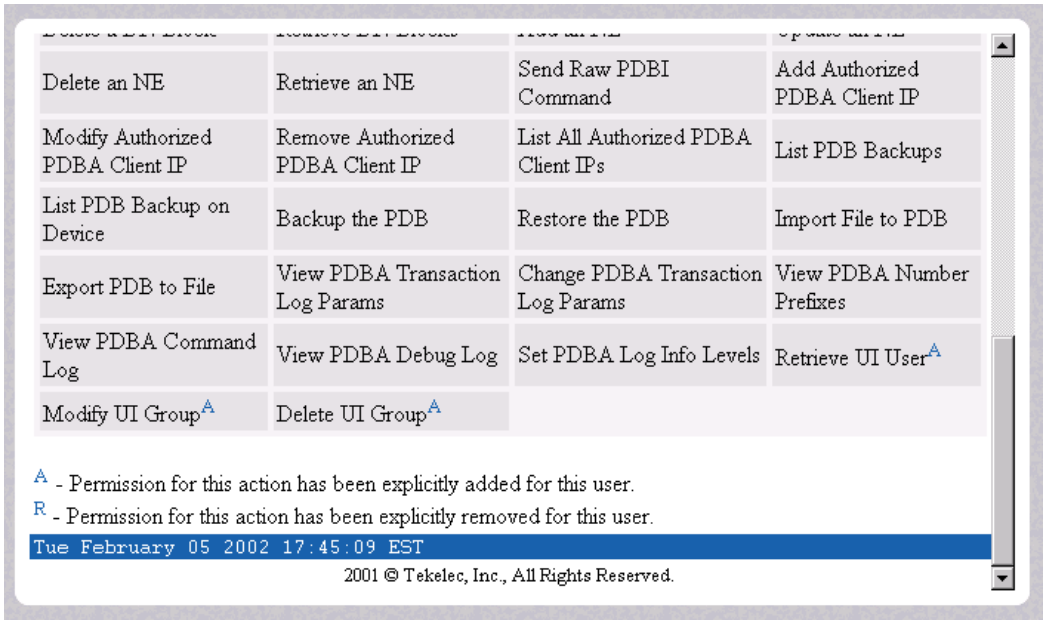


The bottom of Figure 3-211 also can have explanatory notes:

- 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 3-211.

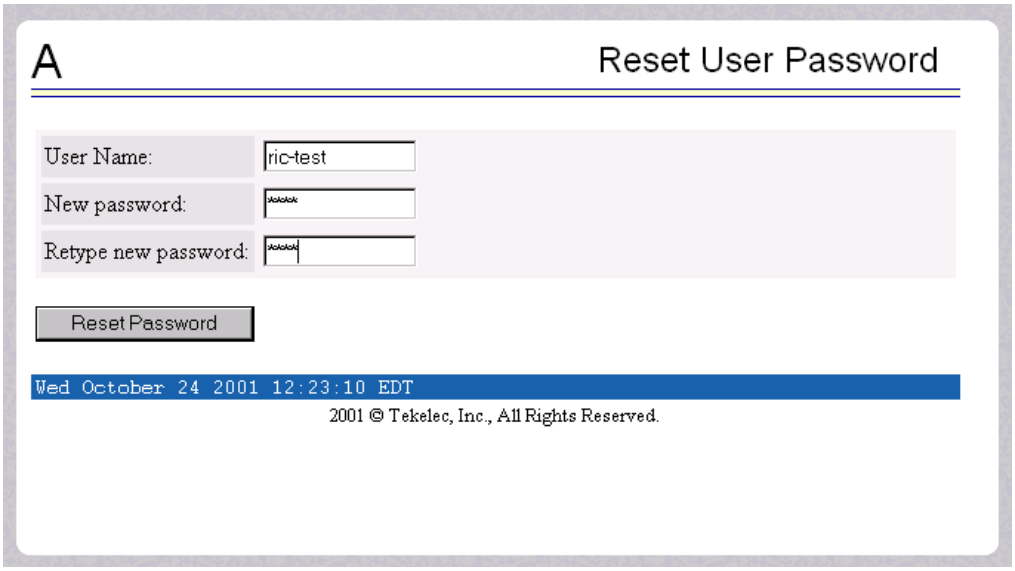
Figure 3-211. Continue Viewing User Privileges



Reset Password

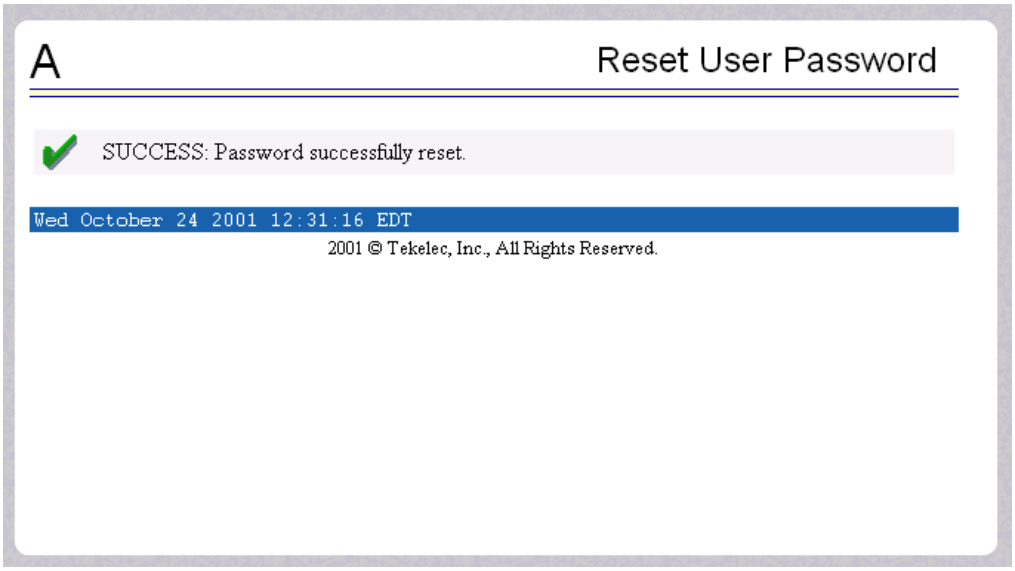
The User Administration / Users / Reset User Password screen lets you select a user name and change the password. See Figure 3-212.

Figure 3-212. Reset User Password Screen



Next, a confirmation screen appears when you correctly update the user's password, shown in Figure 3-213.

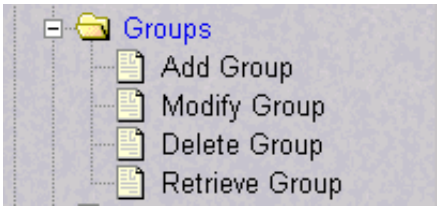
Figure 3-213. Confirming the Reset User Password



Groups

The User Administration / Groups menu allows the user to administer group functions such as add, modify, delete, and retrieve. See the Groups menu in Figure 3-214.

Figure 3-214. 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 menu.

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

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

- **maint**
- **database**
- **platform**
- **debug**
- **pdba**
- **admin**

One additional pre-defined group used is introduced to EPAP (at version 2.0). 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" on page 3-149
- "Modify Group" on page 3-150
- "Delete Group" on page 3-152
- "Retrieve Group" on page 3-153

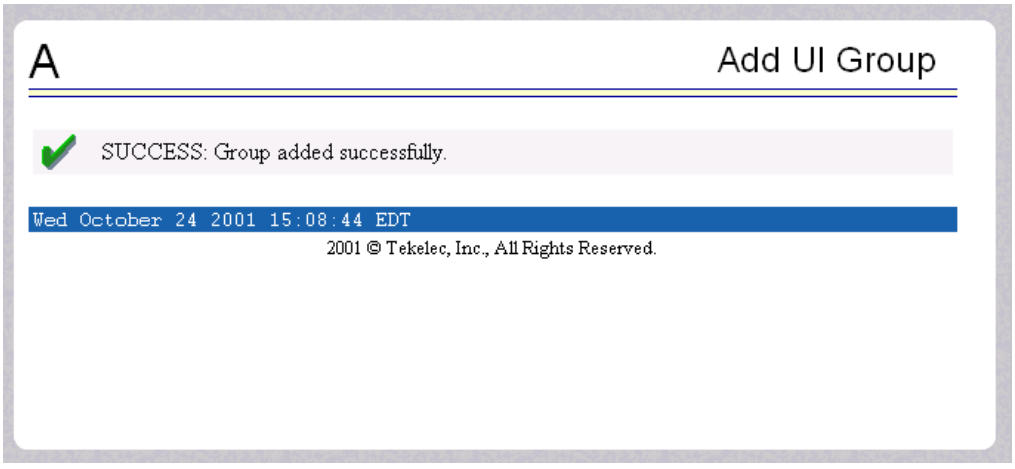
Add Group

The User Administration / Groups / Add UI Group screen lets you enter a new group and assign action privileges with the new group. See Figure 3-215 for the Add UI Group screen.

Figure 3-215. Add UI Group Screen

Figure 3-216 shows the screen confirmation of the newly added group.

Figure 3-216. Confirming a New Group

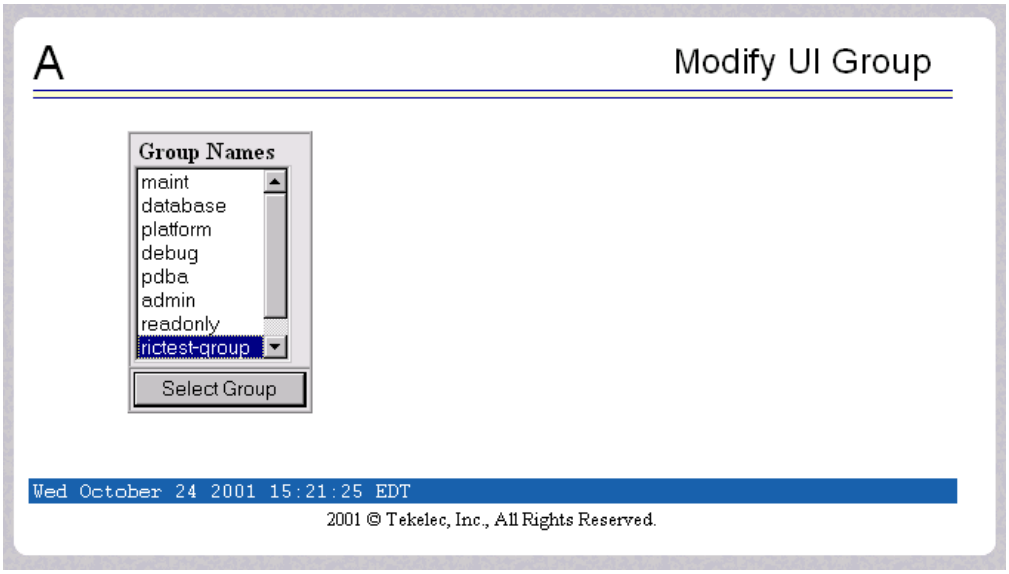


When you receive the successful group added message, you should proceed to the "Modify Group" on page 3-150 and assign the Action Privileges for the new group.

Modify Group

The User Administration / Group / Modify UI Group screen lets you administer group permission profiles. Select the Group Name, and click the Select Group button. Figure 3-217 shows sample Modify UI Group screen.

Figure 3-217. Modify UI Group Screen



When you have selected the group, the Modify Group Permission Profiles screen shows the current action privileges assigned to the group. See Figure 3-218 and Figure 3-219 for the beginning and end of the Action Privileges, with some sample privileges chosen.

Figure 3-218. Viewing a Group for Modification

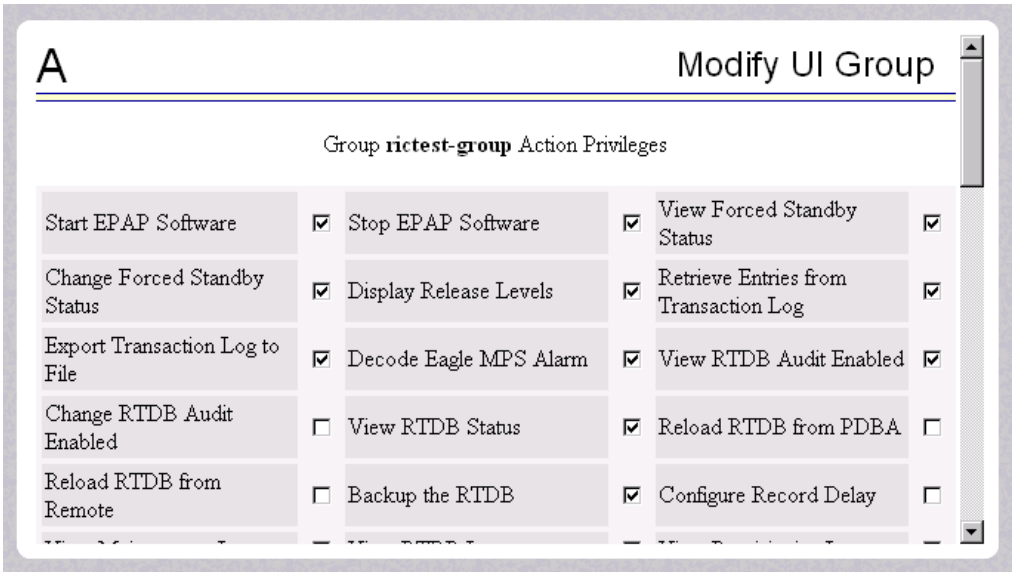
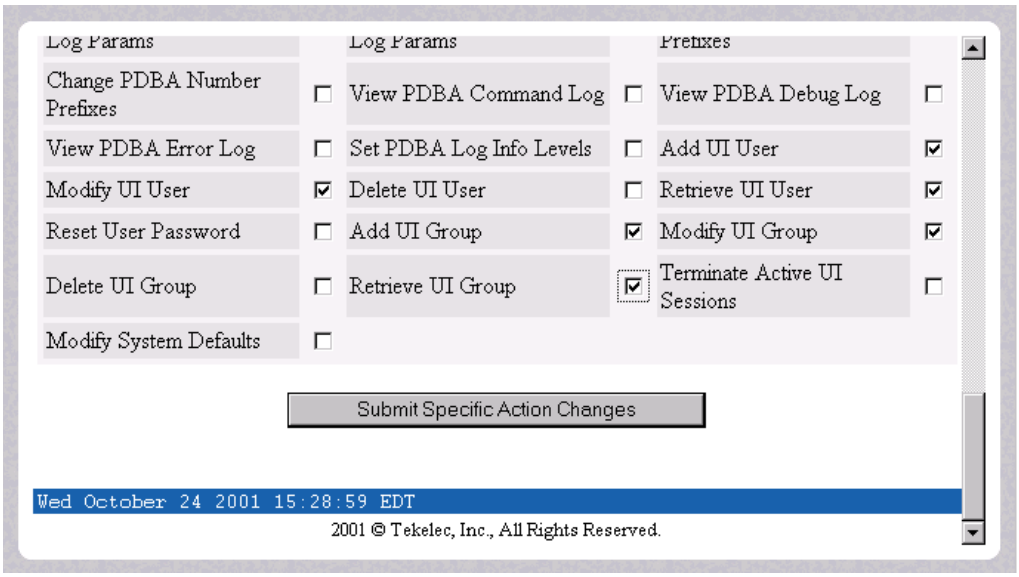
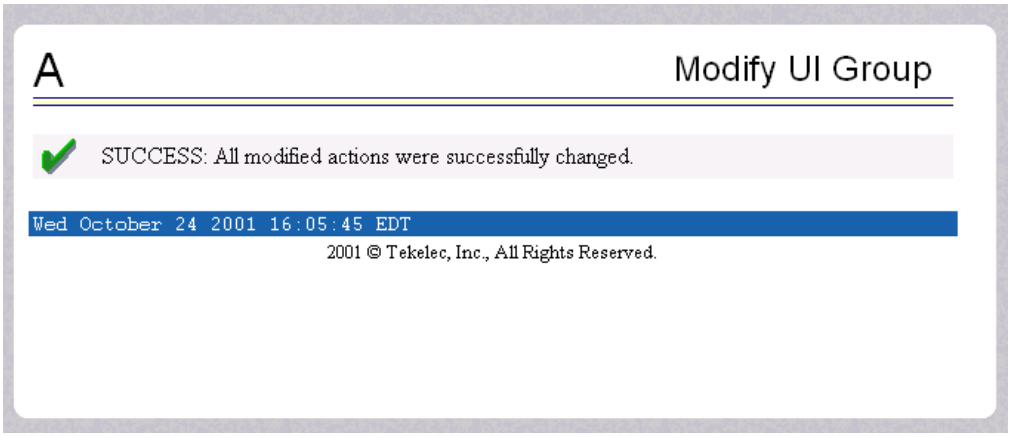


Figure 3-219. Continuing to View a Group for Modification



When you specify the Action Privileges you want to assign to this group and click the Submit Specific Action Changes, you see the screen confirming the changes, as in Figure 3-220.

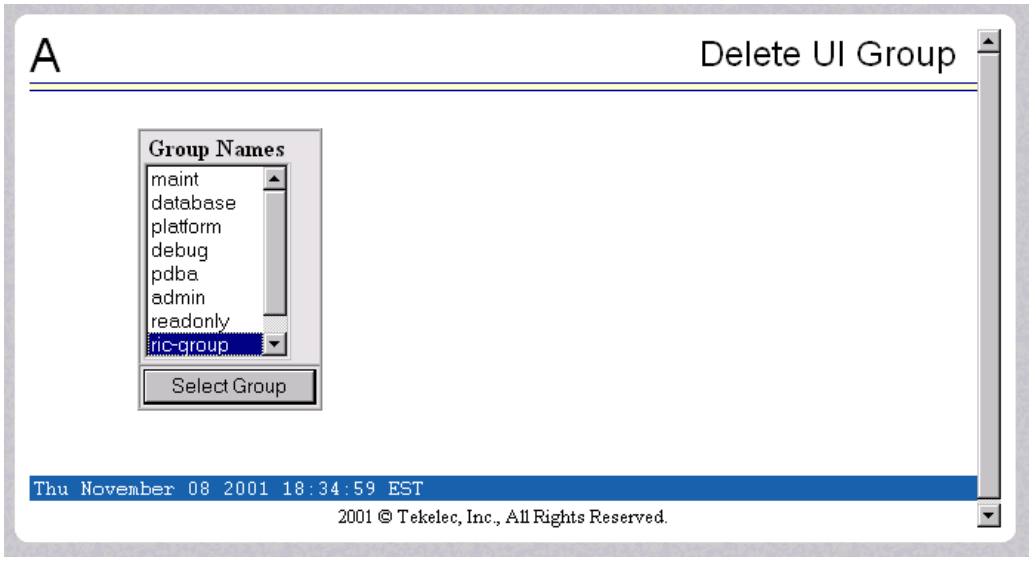
Figure 3-220. Confirming Modify UI Group Action Privileges



Delete Group

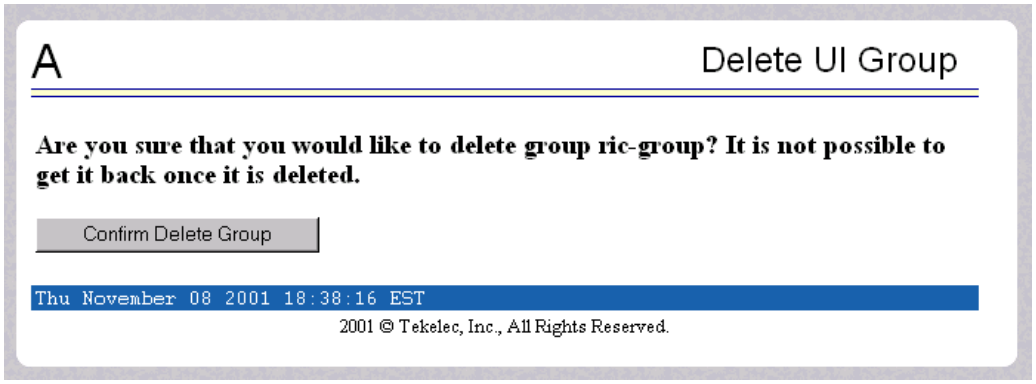
The User Administration / Group / Delete UI Group Profile screen lets you remove a group from the user interface information. The administrator must first select the group name for deletion, as shown in Figure 3-221.

Figure 3-221. Delete UI Group Screen



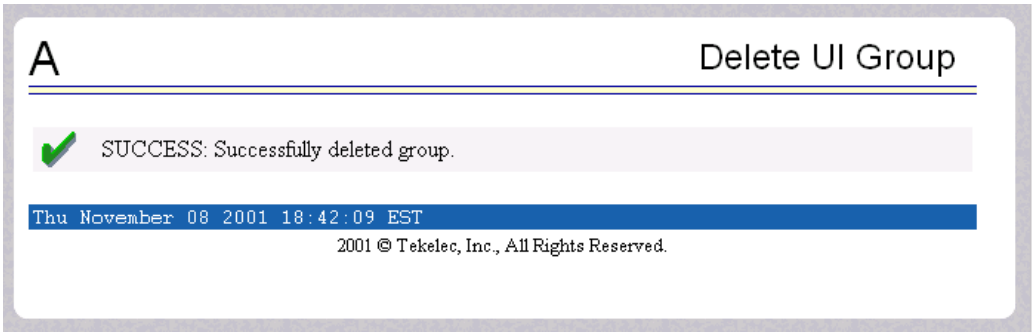
When you click the Select Group button, a confirmation banner and button appear, as shown in Figure 3-222.

Figure 3-222. Confirming the Delete UI Group



Finally, select the Confirm Delete Group button to delete the group name and its permissions. See Figure 3-223.

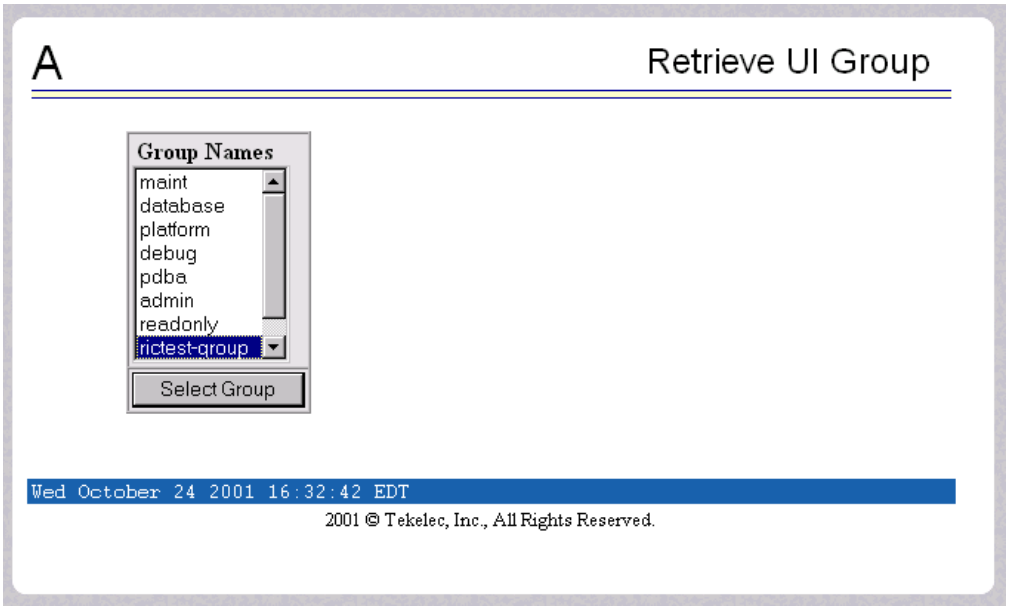
Figure 3-223. Success in Delete UI Group



Retrieve Group

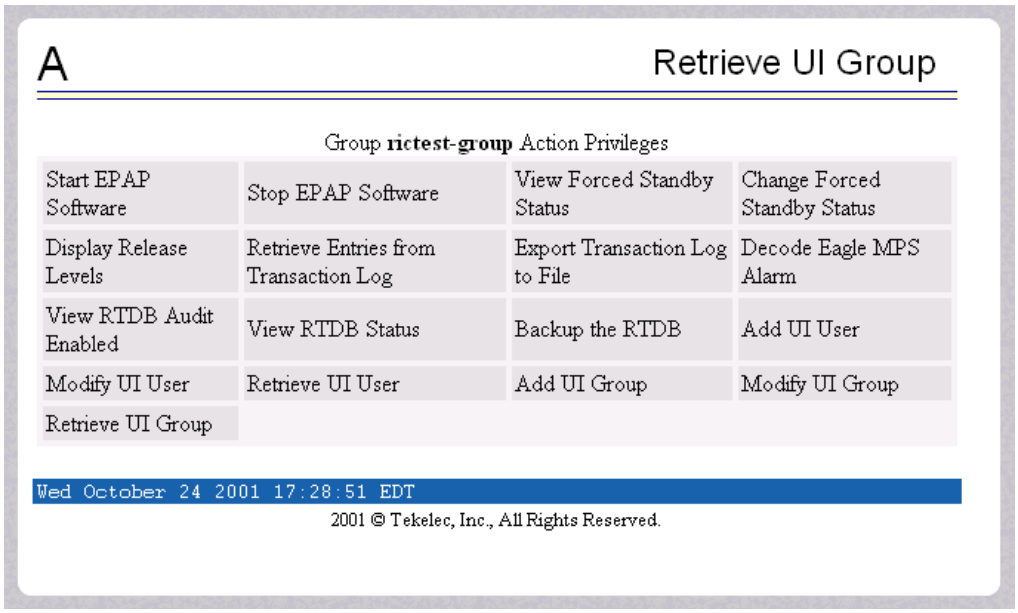
The User Administration / Users / Retrieve UI Group screen lets you display the permission profiles for groups from the user interface information. First select a group name to be retrieved, and click the Select Group button, as shown in Figure 3-224.

Figure 3-224. 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 3-225. There you can view the permissions allowed to this group. All you see is the actions supported for the group, as illustrated in Figure 3-225.

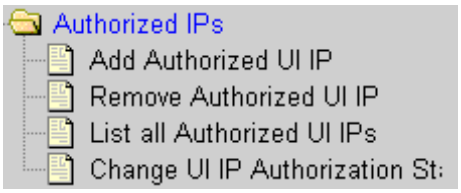
Figure 3-225. Retrieval of UI User Information Screen



Authorized IPs

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 3-226 shows the Authorized IP menu.

Figure 3-226. Authorized IP Menu



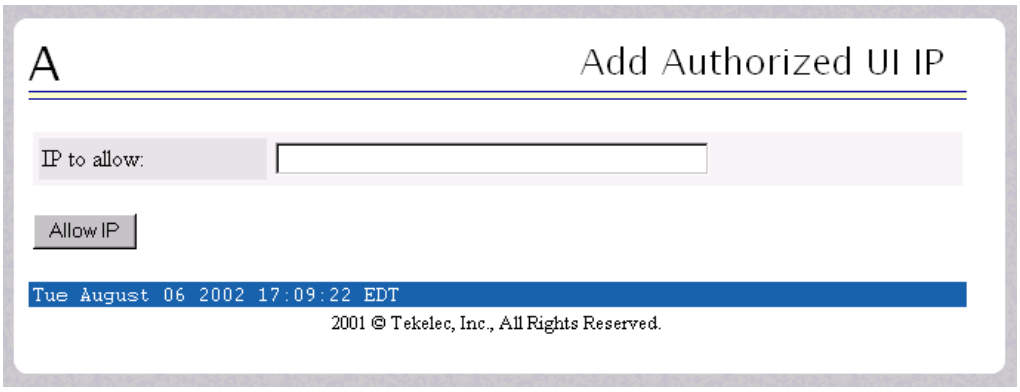
The PDBA / Authorized IP List menu provides these actions:

- "Add Authorized UI IP" on page 3-155
- "Remove Authorized UI IP" on page 3-156
- "List All Authorized UI IPs" on page 3-157
- "Change UI IP Authorization Status" on page 3-158

Add Authorized UI IP

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 3-227 for the Add Authorized UI IP screen.

Figure 3-227. 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 3-228.

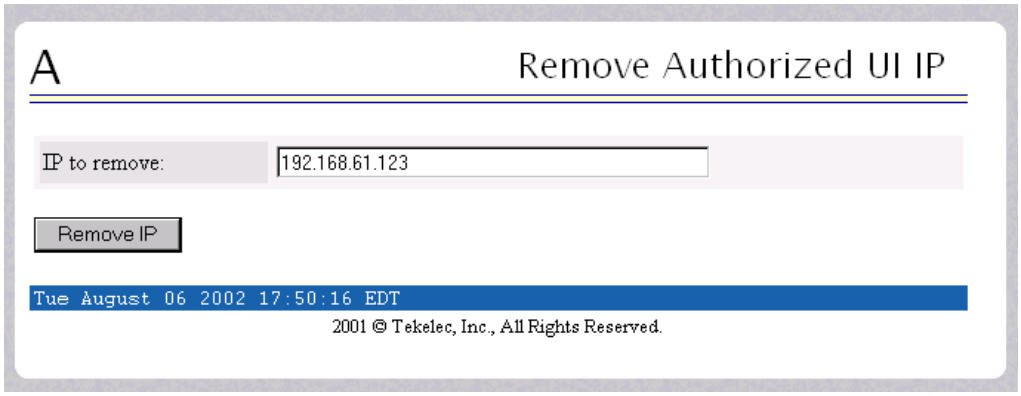
Figure 3-228. Successfully Adding an Authorized UI IP Address

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

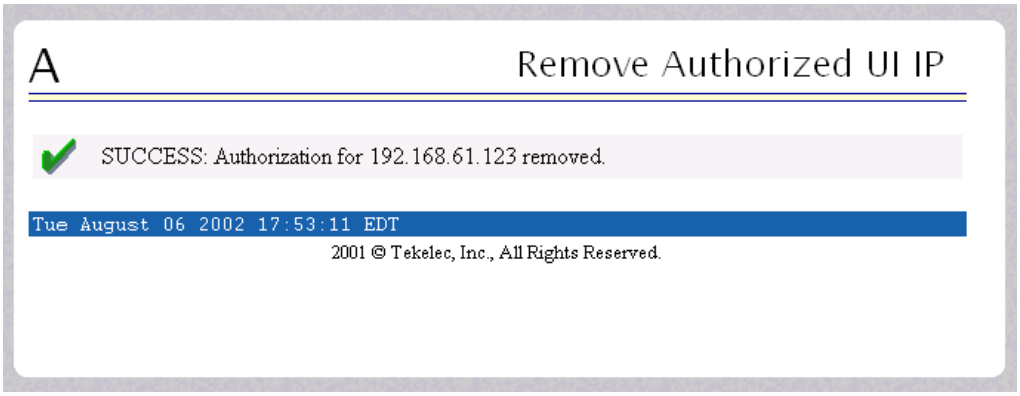
The User Administration / Authorized IP / Remove Authorized UI IP screen lets you remove an IP address from the list of authorized IP addresses. You must enter the individual IP address or CIDR IP format in the 'IP to Remove' input field. A pop-up syntax box appears when the cursor is positioned over that input field. See Figure 3-229 for an example of the Remove Authorized UI IP screen.

Figure 3-229. 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 3-230.

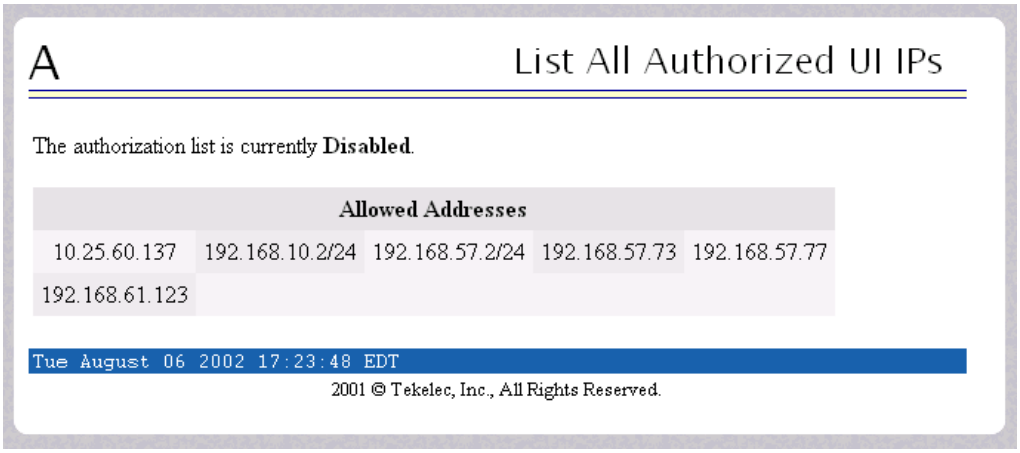
Figure 3-230. Successfully Removing an Authorized UI IP Address



List All Authorized UI IPs

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 3-231 for an example of the List All Authorized UI IP address screen.

Figure 3-231. List All Authorized UI IP Addresses Screen



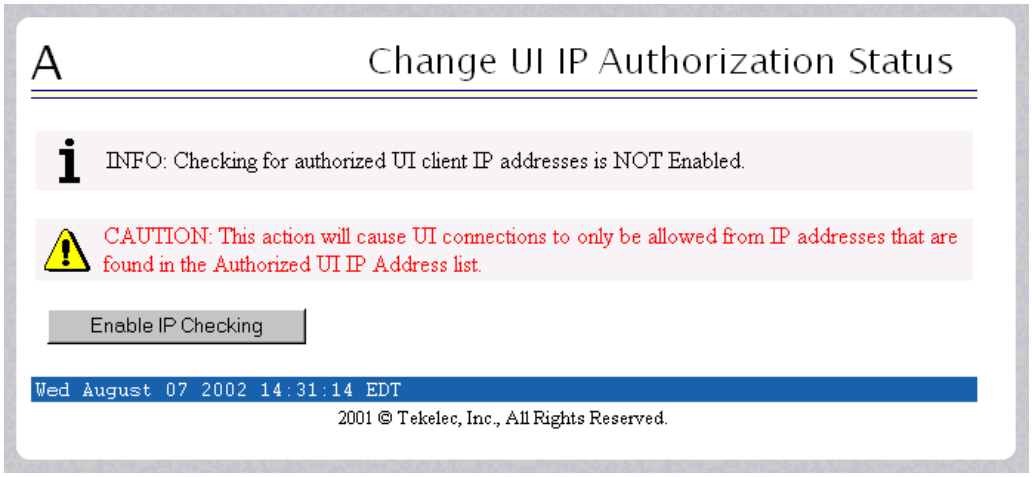
For information about enabling and disabling the authorization list, see “Change UI IP Authorization Status” on page 3-158.

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.'

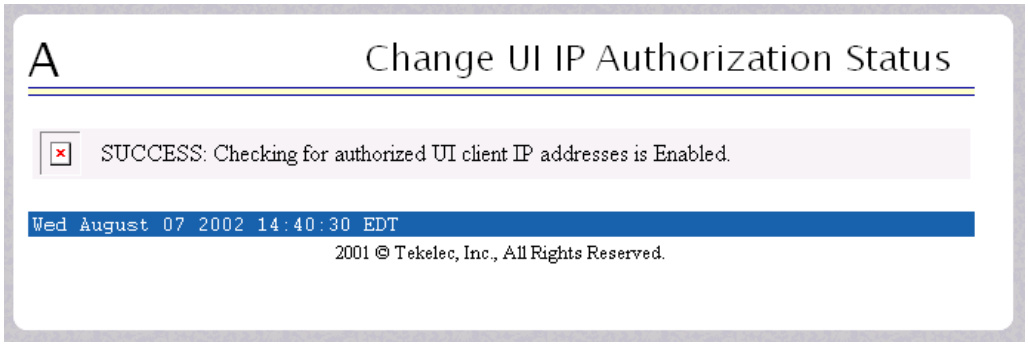
When this menu option is chosen, the current authorization state is displayed in the INFO field. See Figure 3-232 for an example of the Change UI IP Authorization Status screen.

Figure 3-232. 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 3-233 for an example of the authorization status having been successfully toggled to the opposite state, now 'Enabled.'

Figure 3-233. Toggling the UI IP Authorization Status

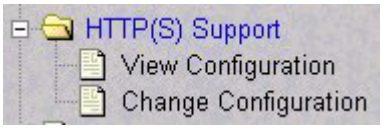


The enforcement of the checking for authorization status is immediate. The IP address of every message of every IP device using the GUI is checked as soon as the authorization status is enabled. The checking for authorized IPs does not occur only when devices log in.

HTTP(S) Support

The User Administration / HTTP(S) Support menu lets you view or change the HTTP(S) configuration. Figure 3-226 shows the HTTP(S) Support menu.

Figure 3-234. HTTP(S) Support Menu



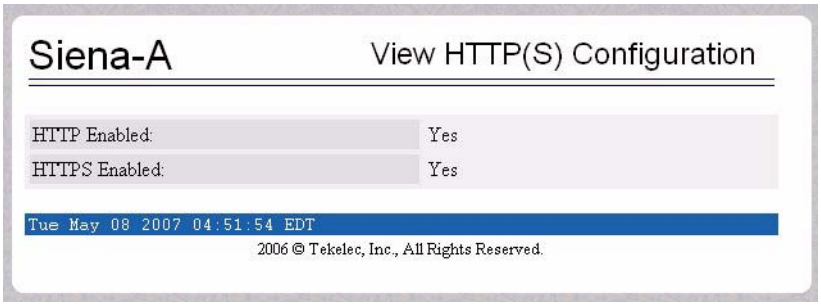
The HTTP(S) Support menu provides these actions:

- "Add Authorized UI IP" on page 3-155
- "Remove Authorized UI IP" on page 3-156

View Configuration

The User Administration / HTTP(S) Support / View Configuration screen lets you view the current HTTP(S) configuration. See Figure 3-227 for the View Configuration screen.

Figure 3-235. View Configuration Screen

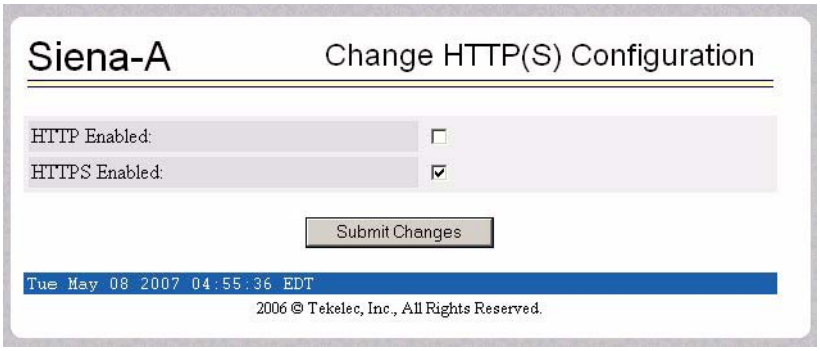


The example shown in Figure 3-235 shows that both the HTTP and HTTPS (secure HTTP) connections are enabled.

Change Configuration

The User Administration / HTTP(S) Support / Change Configuration screen lets you change the current HTTP(S) configuration. See Figure 3-227 for the Change Configuration screen.

Figure 3-236. View Configuration Screen

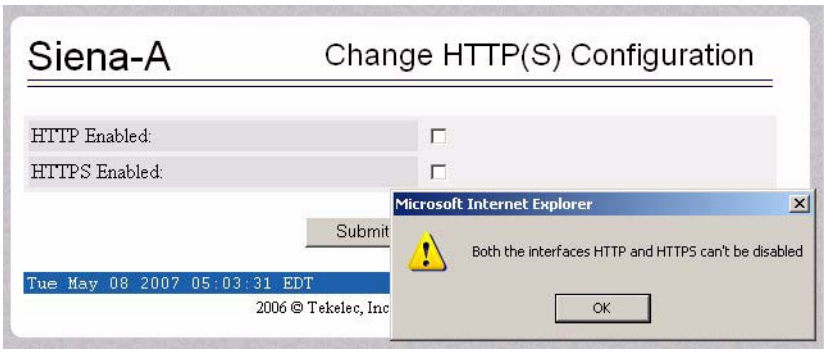


To change the HTTP(S) configuration, click the checkboxes:

- **HTTP Enabled checkbox:** By default, this checkbox is checked. To disable the use of HTTP for the EPAP GUI, uncheck this box.
- **HTTPS Enabled checkbox:** By default, this checkbox is unchecked. To enable the use of HTTPS for the EPAP GUI, check this box.

You cannot disable both HTTP and HTTPS interfaces simultaneously. If you uncheck both checkboxes, an alert message is displayed as shown in Figure 3-237.

Figure 3-237. Disabled HTTP and HTTPS Alert Message

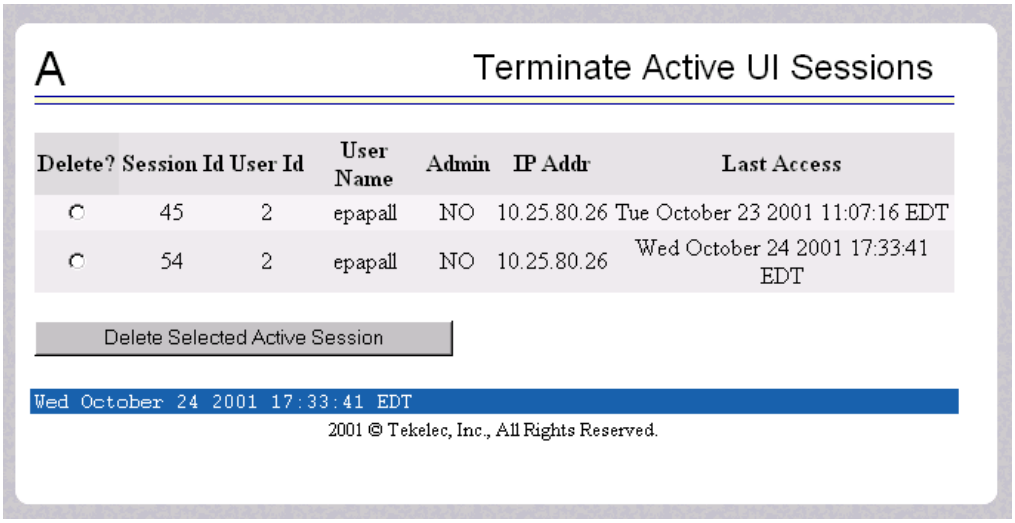


If the HTTP interface is disabled, any existing GUI sessions that use HTTP will stop working. If the HTTPS interface is disabled, any existing GUI sessions that use HTTPS will stop working. (In each case, a browser error that says "The page cannot be displayed" is displayed.)

Terminate UI Sessions

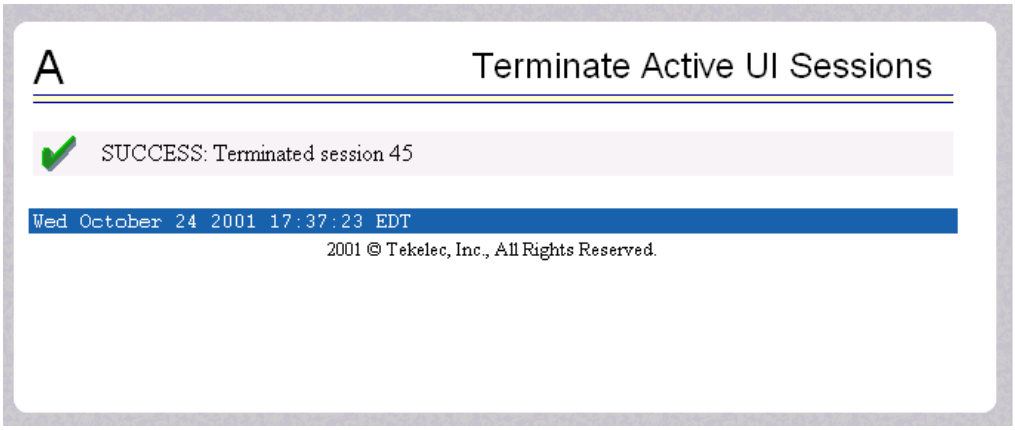
The User Administration / Terminate Active UI Sessions screen allows the administrator to selectively close individual active sessions. See the Terminate Active UI Sessions screen in Figure 3-238.

Figure 3-238. Terminate Active UI Sessions Screen



The administrator selects a session for closing, by clicking a Session in its **Delete?** column. A successful termination is shown in Figure 3-239.

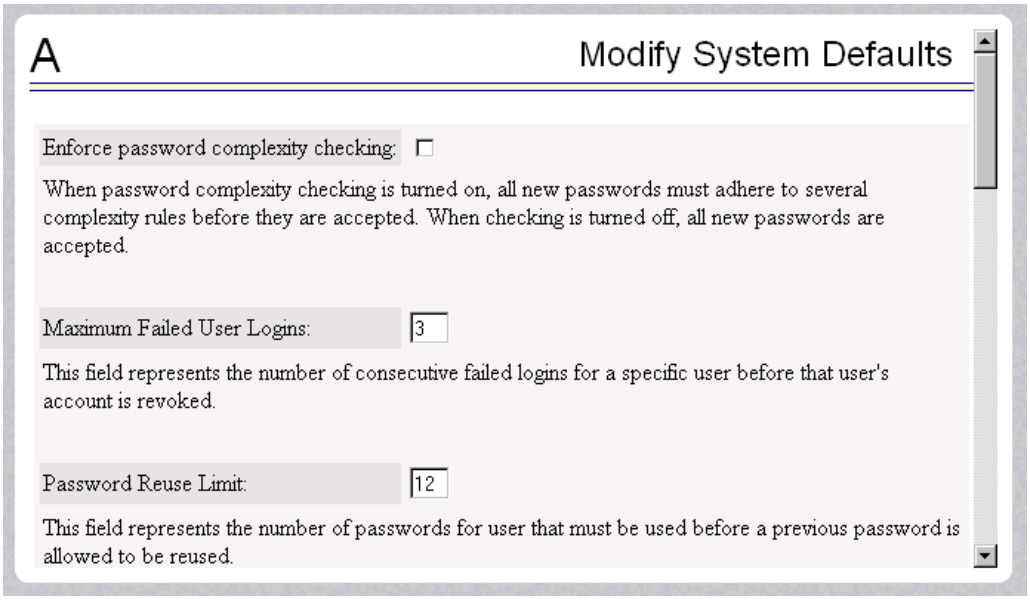
Figure 3-239. Confirmation of UI Session Termination



Modify 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 3-240.

Figure 3-240. Modify System Defaults Screen



The System Defaults for you to modify are specifically 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 EPAP 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 as follows:

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

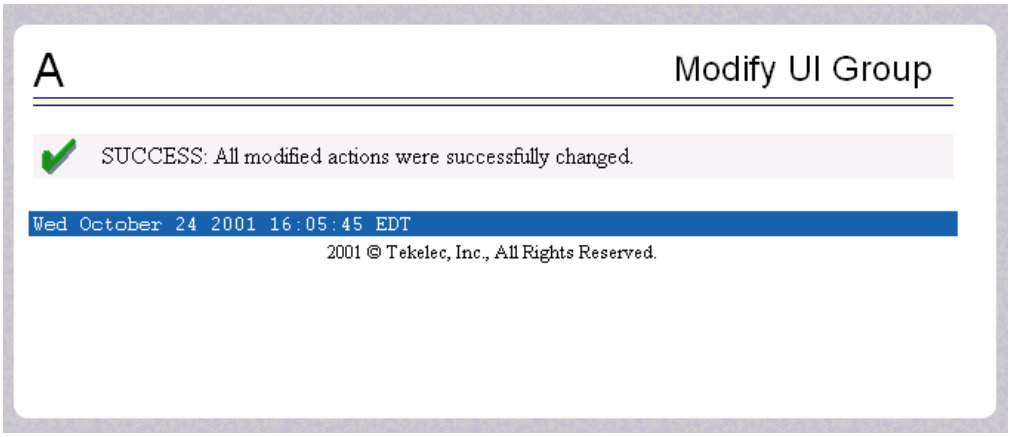
- New User Default Groups: This field contains a list of group names (comma-delimited) with which newly created users are automatically assigned. The default group name is **readonly**.
- Unauthorized IP Access Message: This field contains the text message that will be displayed to the user when a connection is attempted from an IP address that does not have permission to use the UI. The default text is as follows:

  NOTICE: This workstation is not authorized to access the GUI.

- Status Refresh Time: This field contains the system default for the refresh time used for the View RTDB Status and View PDBA Status screens. Time must be either 5-600 seconds or 0 (no refreshing).

When you complete the changes to the Modify System Defaults, click the Submit Defaults button. Figure 3-241 shows your actions successfully changed.

Figure 3-241. Confirming Modify System Defaults Screen

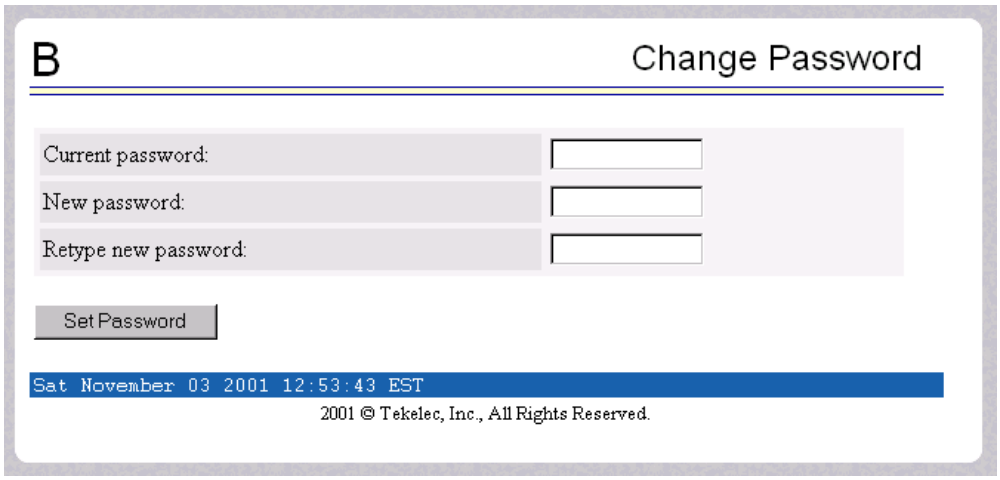


Change Password

The Change Password screen provides you, the EPAP user, with a screen to change your password. This basic action is available to all users and is accessible from the main menu (Figure 3-19, on page 3-19).

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 3-242.

Figure 3-242. 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 EPAP 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.

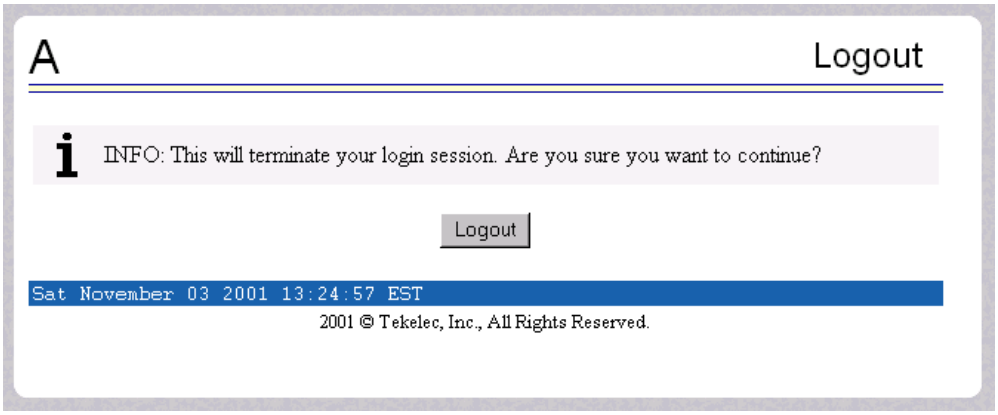
- Inactivity: Users can be forced to change their password if it is not used within the Maximum Account Inactivity time. The administrator can set a Maximum Account Inactivity time as a default for the system.
- Password Reuse: Users cannot reuse their last N passwords. N is a system-wide configurable 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 3-19, on page 3-19).

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 Logout button to complete the logout, shown in Figure 3-243.

Figure 3-243. Logout Screen



When you have continued with the logout, the screen returns to the screen showing the Tekelec EPAP User Interface login (Figure 3-9 on page 3-11).

EPAP Messages

This section includes tables with the EPAP error messages (Table 3-4), the EPAP informational messages (Table 3-5), and the EPAP alarm related banner messages (Table 3-6).

EPAP Error Messages

Table 3-4 lists all of the possible error codes and associated text that are generated by the EPAP user interface. The <> fields indicate values that are different for each error; they are filled in at run time.

Table 3-4. EPAP Error Messages

E1000	Unknown error <*error number*>. No error text is available.
E1001	Invalid menu selection: <*menu selection*>
E1002	Invalid syntax: <*input*>
E1003	Mate EPAPs may not have the same designation.
E1004	EPAP software is running. You must stop the EPAP software before performing this operation.
E1005	EPAP software is not running. You must start the EPAP software before performing this operation.
E1006	Mate EPAP 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 EPAP.
E1011	Cannot find EPAP <*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.

Table 3-4. EPAP Error Messages (Continued)

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	EPAP configuration failed. Please use the configuration menu to manually configure the EPAP sync and DSM networks.
E1037	One or more EPAP software processes did not start
E1038	One or more EPAP 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 EPAP was not available.
E1044	Remote EPAP software is running. You must stop the remote EPAP 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 EPAP. Config files could not be synchronized !!!
E1051	No feature(s) specified.
E1052	Both ELAP and EPAP features specified.

Table 3-4. EPAP Error Messages (Continued)

E1053	This action may only be performed on the local EPAP.
E1054	Another user is currently performing this same action.
E1055	Missing mandatory parameter: <*parameter*>
E1056	Unexpected parameter was provided: <*parameter*>
E1057	The EPAP 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 EPAP 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 EPAP 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.
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 be performed only on a provisionable MPS.
E1085	The specified address is local to this MPS.

EPAP Banner Messages

Table 3-5 lists the banner informational banner messages that appear on the UI browser screen in the Message Box described on page 3-13. These messages, sometimes referred to as 'scroll by messages, indicate the status of the EPAP machines.

Table 3-5. EPAP Informational Banner Messages

Another user has already started the EPAP Software
Another user is currently starting the EPAP Software
Attempt to correct MySQL replication failed
Auto FTP: Unable to connect to host
Automatic PDB Backup completed successfully
Automatic PDB Backup in progress
Automatic PDB Backup not completed successfully
Automatic RTDB Backup completed successfully
Automatic RTDB Backup in progress
Automatic RTDB Backup not completed successfully
Backup Filesystem Failed
Backup Filesystem Failed: No tape in drive
Backup filesystem in progress
Backup filesystem successful
Backup filesystem was aborted manually
Backup PDB completed successfully
Backup PDB failed
Backup PDB in progress
Backup RTDB completed successfully
Backup RTDB failed
Backup RTDB in progress
Export PDB completed successfully
Export PDB failed
Export PDB in progress
Failure within filesystem backup utility. View backup_fs.fail log.
GUI server returned error, cannot start the EPAP software
Import of <*file name*> in progress - <*xx.xx%*>
Import of <*file name*> completed
Import of <*file name*> failed (<*reason*>)

Table 3-5. EPAP Informational Banner Messages (Continued)

Import of <*file name*> postponed (to many connections)
Import PDB completed successfully
Import PDB failed
Import PDB in progress
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 PDB completed successfully
Restore PDB failed
Restore PDB in progress
Restore RTDB completed successfully
Restore RTDB failed
Restore RTDB in progress
The EPAP software couldn't be started
The EPAP software has been successfully started
The EPAP software has been successfully stopped.
Unable to connect to GUI server, cannot start the EPAP software
Unable to connect to host

Table 3-6 lists the alarm related banner messages that appear on the UI browser screen in the Message Box described on page 3-13. If any of the following alarm related messages appear, refer to the *MPS Platform Software and Maintenance Manual* for the related corrective procedure.

Table 3-6. EPAP Alarm Related Banner Messages

Major Platform Alarms
Server Fan Failure
Server Internal Disk Failure
Server Platform Error
Server File System Error
Server Platform Process Failure
Server Swap Space Storage Failure
Server Provisioning Network Error
Server Eagle Network A Error
Server Eagle Network B Error
Server Sync Network Failure
Server Disk Space Shortage Error
Server Default Route Network Error
Server Temperature Error
Server Mainboard Voltage Eror
Server Power Feed Unavailable
Server Disk Health Test Error
Server Disk Unavailable Error
Breaker Panel Feed Error
Breaker Panel Breaker Error
Breaker Panel Monitoring Error

Major Application Alarms
Mate EPAP Unavailable
RTDB Mate Unavailable
Congestion
RMTP Channels Down
Fatal Software Error
RTDB Corrupt
RTDB Inconsistent

Table 3-6. EPAP Alarm Related Banner Messages (Continued)

RTDB Incoherent
RTDB 100% Full
RTDB Resynchronization In Progress
RTDB Reload Is Required
Mate PDBA unreachable
PDBA Connection failure
PDBA Replication failure
RTDB DSM Over-Allocation
RTDB Maximum Depth Reached
No PDBA Proxy to Remote PDBA Connection

Minor Platform Alarms
Server Disk Space Shortage Warning
Server Application Process Error
Server Hardware Configuration Error
Server Swap Space Shortage warning
Server Default Router Not Defined
Server Temperature Warning
Server NTP Daemon Not Synchronized
Server CMOS Battery Voltage Low
Server Disk Self Test Warning
Server Core File Detected
Server Reboot Watchdog Initiated

Minor Application Alarms
RMTP Channel A Down
RMTP Channel B Down
RTDB 80% Full
Standby PDBA Falling Behind
PDB Backup failed
Automatic PDB backup failed
RTDB backup failed
Automatic RTDB backup failed
Automatic backup cron entry does not exist

4

Messages, Alarms, and Status Reporting

MPS and EPAP 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 EPAP. See "Run Health Check" on page 3-57 and refer to the *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 EPAP application.

On the MPS front panel, there are three LEDs that correspond directly to alarm severities: critical, major, and minor. 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 EPAP 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 EAGLE 5 ISS through the primary DSM.

The Active EPAP generates and sends Maintenance Blocks to the primary DSM. One Maintenance Block is sent as soon as the IP link is established between the Active EPAP and the primary DSM. Additional Maintenance Blocks are sent whenever the EPAP 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 EPAP 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 EPAP is restricted to sending no more than one EPAP Maintenance Block per second.

EPAP Maintenance Block Contents

The EPAP 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 EPAP 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

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 the EAGLE 5 ISS. The information that is transferred is described in "MPS Platform and Application Alarms" and "MPS Alarm Recovery Procedures" of the *MPS Platform Software and Maintenance Manual*.

Alarm Priorities

The EPAP 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 EPAP 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.

DSM Status Requests

When the EPAP needs to know the status of a DSM, it can send a DSM Status Request to that DSM. Because status messages are sent over UDP, the EPAP broadcasts the DSM Status Request and all DSMs return their status.

DSM Status Reporting to the EPAP

The EPAP needs to know the current status of various aspects of the DSMs. Accordingly, the DSM sends a DSM status message to the EPAP when the following events occur:

- When the DSM is booted
- When the DSM receives a DSM Status Request message from the EPAP
- When the DSM 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 DSM starts receiving DB downloads or DB updates.

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

DSM Status Message Fields

The DSM status message provides the following information to the EPAP:

- DSM Memory Size

  When the DSM is initialized, it determines the amount of applique memory present. The EPAP uses this value to determine if the DSM 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 EPAP 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 DSM, the DSM keeps track of the database level number. The database level number will be included in all Status messages sent from the DSM. A level number of 0 signifies that no database has been loaded into the DSM (this can be done any time the DSM wants to request a full database download).

- Database Download Starting Record Number

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

System Hardware Verification

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

- Validity of the DSM motherboard
- Verification of daughterboard memory size

CAUTION: Refer to the *Dimensioning Guide for EPAP Advanced DB Features Technical Reference* for important information on the dimensioning rules and the DSM database capacity requirements.

DSM Motherboard Verification

An AMD-K6 (or better) motherboard is required to support the G-Flex/ G-Port/INP/EIR VSCCP application on the DSM card. EAGLE 5 ISS maintenance stores the validity status of the VSCCP card's motherboard configuration. The system does not allow the G-Flex, G-Port, INP, or EIR feature to be enabled if the hardware configuration is invalid.

When the VSCCP application is initializing, it determines the motherboard type. The SCCP Maintenance Block is the mechanism that relays the motherboard information to OAM. This requires the application software to be loaded to the VSCCP card and then verification of the motherboard information received in the SCCP Maintenance Block. If the motherboard is determined to be invalid for the G-Flex/G-Port/INP/EIR application, loading of the VSCCP card is automatically inhibited and the card is booted via PMTC. Booting the card in this manner suppresses any obituary.

DSM Daughterboard Memory Verification

The VSCCP application performs two types of memory validation to determine whether or not a DSM has sufficient memory to run G-Flex/G-Port/INP/EIR: 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 VSCCP card. (See the *Commands Manual* for a description of the **rept-stat-sccp** command output.)

The VSCCP application performs two types of memory validation to determine whether or not a DSM has sufficient memory to run G-Flex/G-Port/INP/EIR: Local Memory validation and Real-Time Memory validation.

Local Memory Validation

When the G-Flex, G-Port, or INP feature bit is first enabled (a Feature Access Key is used for the EIR feature), or any time the G-Flex, G-Port, INP, or EIR feature is enabled and the DSM is initializing, VSCCP checks to see if the DSM has at least one D1G daughterboard. The G-Flex, G-Port, or INP feature bit cannot be enabled if any of the DSMs have less than 1 GB of memory installed.

Real-Time Memory Validation

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

Actions Taken When Hardware Determined to be Invalid

When the hardware configuration for a DSM card is determined to be invalid for the G-Flex/G-Port/INP/EIR application, SCM automatically inhibits loading for that specific DSM card. A major alarm is generated indicating that card loading for that DSM card failed and was automatically inhibited (that is, prevented from reloading again). Refer to the *Maintenance Manual* for the specific alarm that is generated. 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 DSM card determined to be invalid:

- The DSM will not download the EAGLE 5 ISS databases.
- The DSM will not download the RTDB from the EPAP.
- The DSM will not accept RTDB updates (additions, changes, and deletes) from the EPAP.

The **rept-stat-sccp** command supports the DSM cards running the VSCCP application and reports G-Flex, G-Port, INP, and EIR statistics. See "Commands" on page 4-9 for more details on the **rept-stat-sccp** command.

Unstable Loading Mode

At some point, having a number of invalid DSM 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 DSMs 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 VSCCP 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 VSCCP) card.

- There is insufficient SCCP service, which occurs if an insufficient number of IS-NR VSCCP cards are available to service at least 80% of the number of IS-NR LIMs.

  It is possible for LIMs or VSCCP cards to be inhibited or to have problems that prevent them from operating normally. If enough VSCCP cards are out of service, it may not be possible for the remaining IS-NR VSCCP 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 When the System is in an Unstable Loading Mode" on page 4-7).

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

Actions Taken When the System is in an 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 VSCCP 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 DSM 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 37.0.0

------------------------------------------------------------------------
    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:00-08-08  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.

System Status Reporting

The following status reporting is described in this section:

- System status
- G-Flex status
- G-Port status
- INP status
- EIR status
- DSM memory capacity status
- Loading mode support status

System Status Reporting

The **rept-stat-sccp** command supports the DSM cards running the VSCCP application, and reports G-Flex, G-Port, INP, and EIR statistics. See "rept-stat-sccp" on page 4-9 for details on the **rept-stat-sccp** command.

G-Flex/G-Port/INP/EIR Status Reporting

The **rept-stat-mps** command reports the status of the G-Flex/G-Port/INP/EIR provisioning system. The **rept-stat-sccp** command will separately report the statistics for G-Flex and G-Port. See "Commands" on page 4-9 for details on the **rept-stat-mps** and **rept-stat-sccp** commands.

DSM Memory Capacity Status Reporting

The DSM will send a message to the EPAP containing the amount of memory on the DSM board. The EPAP will determine whether the DSM has enough memory to store the RTDB and send an ACK or NAK back to the DSM indicating whether or not the DSM has an adequate amount of memory.

When the EPAP sends database updates to the DSMs, the update messages will include a field that contains the new database memory requirements. Each DSM will monitor the DB size requirements, and issue 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 DSM's memory, a major alarm will be issued.

The **rept-stat-mps:loc=xxxx** command will show the amount of memory used by the RTDB as a percent of available DSM memory (see "rept-stat-mps" on page 4-11).

Loading Mode Support Status Reporting

The OAM application can determine whether or not the system is in an unstable Loading Mode because it knows the state of all LIM, SCCP, and DSM cards in the system. When the loading mode is unstable, the **rept-stat-sys** command will report the existence of the unstable Loading Mode and the specific conditions which caused it. See "Unstable Loading Mode" on page 4-6 for more details on Loading Mode support.

Commands

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

rept-stat-sccp

The command handling and scroll area output for the **rept-stat-sccp** command includes the DSM card. You can add the **loc** parameter to display detailed card traffic statistics.

Samples of the reports produced by these commands are shown in Figure 4-2:

Figure 4-2. **`rept-stat-sccp`** Command Report Examples

```
    rept-stat-sccp
    Command entered at terminal #3.
;

      tekelecstp 00-06-23 13:34:22 EST EAGLE 37.0.0
    SCCP SUBSYSTEM REPORT IS-NR          Active      -----
    GSM  SUBSYSTEM REPORT IS-NR          Active      -----
    INP  SUBSYSTEM REPORT IS-ANR         Restricted  -----
         ASSUMING MATE'S LOAD
         INPQS: SSN STATUS = Allowed     MATE SSN STATUS  = Prohibited

SCCP Cards Configured= 4  Cards IS-NR= 2  Capacity Threshold = 100%
CARD   VERSION      PST          SST          AST       MSU USAGE  CPU USAGE
    ------------------------------------------------------------------------
1212   103-001-000  IS-NR        Active       ALMINH       45%         30%
1301 P 103-001-000  IS-NR        Active       ------       35%         40%
1305   -----------  OOS-MT       Isolated     ------        0%          0%
2112   -----------  OOS-MT-DSBLD Manual       ------        0%          0%
    ------------------------------------------------------------------------
SCCP Service Average MSU Capacity = 40%       Average CPU Capacity = 35%

    AVERAGE CPU USAGE PER SERVICE:
      GTT   = 15%  GFLEX =  5%  GPORT = 10%
      INPMR =  2%  INPQS =  3%

    TOTAL SERVICE STATISTICS:
      SERVICE    SUCCESS    ERRORS    WARNINGS    FORWARD TO GTT    TOTAL
      GTT:          1995         5           -                 -     2000
      GFLEX:         500         1           4                10      515
      GPORT:         800         0           2                 3      805
      INPMR:          50         5           0                15       70
      INPQS:         499         1           -                 -      500

    Command Completed.
;


Rept-stat-sccp:loc=1106
    Command entered at terminal #4.
;
    tekelecstp 00-06-23 13:34:22 EST EAGLE 37.0.0
    CARD  VERSION      TYPE    PST          SST       AST
    1106  103-010-000  DSM     IS-NR        Active    -----
    CARD ALARM STATUS       = No Alarms.
      GTT:   STAT = ACT       CPU USAGE = 10%
      GFLEX: STAT = ACT       CPU USAGE = 10%
      GPORT: STAT = ACT       CPU USAGE = 10%
      INPMR: STAT = ACT       CPU USAGE = 13%
      INPQS: STAT = ACT       CPU USAGE = 20%
    TOTAL CPU USAGE = 63%

    CARD SERVICE STATISTICS:
      SERVICE    SUCCESS    ERRORS    WARNINGS    FORWARD TO GTT    TOTAL
      GTT:          1995         5           -                 -     2000
      GFLEX:         500         1           4                10      515
      GPORT:         500         1           4                10      515
      INPMR:          50         2           3                15       70
      INPQS:         499         1           -                 -      500

   Command Completed.
```

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 reload from the PDB.

Figure 4-3. **rept-stat-db** Command Report Example

```
   rept-stat-db:display=all:db=mps
   Command entered at terminal #4.

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

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

There are two possible variants of this new command:

- **rept-stat-mps** - This produces a summary report showing the overall status of the G-Flex/G-Port/INP/EIR provisioning system and a moderate level of information for each DSM card.
- **rept-stat-mps:loc=xxxx** – This produces a more detailed report showing the G-Flex/G-Port/INP/EIR status of a specific DSM card.

  When the EPAP sends database updates to the DSMs, the update messages will 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 DSM memory.

Each DSM will monitor the DB size requirements, and issue 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 DSM's memory, a major alarm will be issued.

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

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

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

    Integrat40 00-06-24 10:37:22 EST EAGLE 37.0.0

                       VERSION       PST            SST        AST
    EPAP A             026-015-000   IS-NR          Active     -----
              ALARM STATUS = No Alarms
    EPAP B             026-015-000   IS-NR          Standby    -----
              ALARM STATUS = No Alarms

    CARD   PST          SST       GSM STAT   INP STAT
    1106 P IS-NR        Active    ACT        ACT
    1201   IS-ANR       Active    SWDL       SWDL
    1205   OOS-MT-DSBLD Manual    -------    -------
    1302   OOS-MT       Fault     -------    -------
    1310   IS-ANR       Standby   SWDL       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-mps:loc=1106
    Command entered at terminal #4.
;

    integrat40 99-09-24 10:37:22 EST EAGLE 37.0.0
    CARD  VERSION         TYPE    PST           SST        AST
    1106  101-9-000       DSM     IS-NR         Active     -----
      DSM PORT A                  IS-NR         Active     -----
      DSM PORT B                  IS-NR         Active     -----
      GSM STATUS          = ACT
      INP STATUS          = ACT
      ALARM STATUS        = No Alarms.
      DSM MEMORY USAGE    = xxx%

    Command Completed.
;
```

rept-stat-trbl

This command includes the G-Flex/G-Port Subsystem, INP Subsystem, EIR Subsystem, and DSM/EPAP IP link alarms.

Figure 4-5. **`rept-stat-trbl`** Command Output Example

```
    rept-stat-trbl
    Command entered at terminal #10.
;
    eagle10605 99-06-24 14:34:08 EST EAGLE 37.0.0
    Searching devices for alarms...
;
    eagle10605 99-06-24 14:34:09 EST EAGLE 37.0.0
    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
    3536.0084 ** EPAP B   7100         IP Connection Unavailable
    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 G-Flex/G-Port Subsystem, INP Subsystem, EIR Subsystem, and DSM/EPAP IP links.

Figure 4-6. **`rept-stat-alm`** Command Report Example

```
    rept-stat-alm
    Command entered at terminal #10.
;

    eagle10605 99-06-24 23:59:39 EST EAGLE 37.0.0
    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.
;
```

pass: cmd="Ping"

The 'ping' command allows for troubleshooting of the private EPAP-DSM IP network.

Figure 4-7. **`pass: cmd="Ping"`** Command Output Example

```
eagle10506 99-08-11 08:43:45 EST EAGLE 37.0.0
    pass:loc=1215:cmd="ping     -h"
    Command entered at terminal #2.
;

    eagle10506 99-08-11 08:43:45 EST EAGLE 37.0.0
    PASS: Command sent to card
;

    eagle10506 99-08-11 08:43:45 EST EAGLE 37.0.0

    Usage: ping <hostname | ipaddr> [-h] [-i size] [-n count]
    Options:
        -h        Displays this message
        -i count  Number of pings to send. Range=1..5. Default=3.
        -n size   Sets size of ICMP echo packet. Range=12..2048. Default=64.
        hostname  Name of machine to ping
        ipaddr    IP Address of machine to ping (d.d.d.d)

;
```

pass: cmd="netstat"

The '**`pass: cmd="netstat"`** command allows troubleshooting of network interface and routing configuration problems within the private EPAP-DSM IP network.

Figure 4-8. **`pass: cmd="netstat"`** Command Output Example

```
eagle10506 99-08-11 08:43:00 EST EAGLE 37.0.0
    pass:loc=1215:cmd="netstat  -h"
    Command entered at terminal #2.;
    eagle10506 99-08-11 08:43:00 EST EAGLE 37.0.0
    PASS: Command sent to card;
    eagle10506 99-08-11 08:43:00 EST EAGLE 37.0.0

    Usage: netstat [-a] [-i] [-h] [-m data|sys|dd] [-p icmp|ip|tcp|udp] [-r]

    Options:
        -a        display socket information for all protocols
        -h        Displays this message
        -i        display interface information for all interfaces
        -m        display buffer pool information for 1 of the system pools
        -p        display socket information for 1 of the protocols
        -r        display the route table information
;
```

Hourly Maintenance Report

The hourly maintenance report includes the alarm totals for the G-Flex/G-Port Subsystem, INP Subsystem, and DSM/EPAP IP links.

Figure 4-9. Hourly Maintenance Report Output Example

```
    eagle10506 99-10-10 16:00:01 EST EAGLE 37.0.0
    5072.0000 REPT COND GSM SS
    "GSM SS :0440,MTCEINT-0,SA,99-10-10,16:00:01,,,,*C"
;
    eagle10506 99-10-10 16:00:01 EST EAGLE 37.0.0
    5073.0000 REPT COND INP SS
    "INP SS :0440,MTCEINT-0,SA,99-10-10,16:20:01,,,,*C"
;
    eagle10506 99-10-10 16:00:01 EST EAGLE 37.0.0
    5077.0000 REPT COND EPAPDSM
    "EPAPDSM :0084,MTCEINT-0,SA,99-10-10,16:00:01,,,,**"
;
    eagle10506 99-10-10 16:00:01 EST EAGLE 37.0.0
    5007.0000 REPT COND CARD
    "CARD 1102:0422,SCMMA,SA,99-10-10,16:00:01,,,,**"
;
    eagle10506 99-09-13 16:00:01 EST EAGLE 37.0.0
    3561.0000 REPT COND ALARM STATUS
    "ALARMS:PERM. INHIBITED,0,0,0"
    "ALARMS:TEMP. INHIBITED,0,0,0"
    "ALARMS:ACTIVE,10,14,3"
    "ALARMS:TOTAL,10,14,3"
;
```

Unsolicited Alarm Messages and Unsolicited Information Messages

This section describes EPAP Unsolicited Alarm Messages (UAMs) and Unsolicited Information Messages (UIMs).

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.

The *MPS Platform Software and Maintenance Manual* (in "MPS Alarm Recovery Procedures") describes all EAGLE 5 ISS UAMs and the appropriate recovery actions.

MPS Platform and EPAP Application Alarms

MPS platform errors are detected by the system health check utility. The system health check output contains a 16-digit hexadecimal alarm data string for each detected platform or application error. The 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 utility, the alarm data strings, and the corrective procedures are described in detail in "MPS Alarm Recovery Procedures" of the *MPS Platform Software and Maintenance Manual.*

MPS platform and EPAP 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.

Table 4-1 defines the application and platform alarms that are forwarded to EAGLE 5 ISS when MPS and EPAP failures or errors are detected. Each alarm category is sent with a hexadecimal alarm data string that recovered from the MPS/EPAP (see "MPS and EPAP Status and Alarm Reporting" on page 4-1). 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 "MPS Alarm Recovery Procedures" in the *MPS Platform Software and Maintenance Manual*. .

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

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)
250	Clearing	MPS Available

Figure 4-10. Alarm Output Example

```
         1         2         3         4         5         6         7         8
12345678901234567890123456789012345678901234567890123456789012345678901234567890
    station1234 00-09-30 16:28:08 EST EAGLE 37.0.0-37.10.0
*C  0259.0370 *C MPS   B              Critical Platform Failure(s)
                ALARM DATA = h'0123456789ABCDEF
```

Figure 4-11. MPS Available Alarm

```
         1         2         3         4         5         6         7         8
12345678901234567890123456789012345678901234567890123456789012345678901234567890
    station1234 00-09-30 16:28:08 EST EAGLE 37.0.0-37.10.0
    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.

EPAP-to-DSM Connection Status

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

EPAP-DSM UAMs

Maintenance Blocks sent from the EPAP have a field to identify error message requests. (See "EPAP Maintenance Block Contents" on page 4-2). The DSM processes incoming Maintenance Blocks and generates the requested UAM. The DSM acts only as a delivery agent. The recovery actions for the EPAP-DSM UAMs are defined in "Corrective Maintenance"Chapter in the *Maintenance Manual*.

DSM-EPAP Link Status Alarms

Two alarms indicate the DSM-to-MPS link status:

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

Figure 4-12. DSM-EPAP Link Alarm Example

```
         1         2         3         4         5         6         7         8
12345678901234567890123456789012345678901234567890123456789012345678901234567890
    station1234 00-09-30 16:28:08 EST EAGLE 37.0.0-37.10.0
**  3582.0084 ** DSM B   1217          IP Connection Unavailable
```

RTDB Audit Alarms

During an audit of the DSM cards and the EPAPs, 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 37.0.0
*   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 EPAP 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 37.0.0
*   0012.0444 * CARD 1108 VSCCP        RTDB Database is inconsistent
```

3. When an inconsistent, incoherent, or corrupted RTDB has been fixed and the card or EPAP 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 37.0.0
    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 37.0.0
*   0012.0448 * CARD 1108 VSCCP        RTDB Database is incoherent
```

5. When a DSM 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 37.0.0
**  0012.0449** CARD 1108 VSCCP        RTDB resynchronization in progress
```

6. After a DSM 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 37.0.0
    0012.0450   CARD 1108 VSCCP        RTDB resynchronization complete
```

7. When a DSM 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 37.0.0
**  0012.0451** CARD 1108 VSCCP        RTDB reload required
```

8. After a DSM 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 37.0.0
    0012.0452   CARD 1108 VSCCP        RTDB reload complete
```

5

EPAP Software Configuration

Overview of the EPAP User Interface

The EAGLE Provisioning Application Processor (EPAP) User Interface provides two user interfaces:

- The Graphical User Interface provides GUI menus that maintain, debug, and operate the platform; the GUI and its associated error messages are described in Chapter 3, *"EPAP Graphical User Interface"*
- The Text-Based User Interface has the Configuration menu to initialize and configure the EPAP; the text-based UI 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 EPAP Configuration menu to perform the initial configuration.

To communicate with the EPAP graphical user interface, you use a PC with a network connection and a network browser. For information about using the EPAP GUI, see "EPAP Graphical User Interface" on page 3-2.

The EPAP text-based user interface is used to configure EPAP. For information about configuring the EPAP and how to set up its PC workstation, continue with this chapter.

Setting Up an EPAP Workstation

The customer workstation serving as a client PC (shown in Figure 3-1 on page 3-3) 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 EPAP user interface was designed and written to perform with Microsoft Internet Explorer 5.0 or later. The EPAP user interface is also compatible with Mozilla Firefox 1.0.2 or later. Do not use other browsers with the EPAP user interface. When using Firefox, you will encounter the following message when logging into the EPAP 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
```

Java

The EPAP GUI uses a Java "banner" applet to display real-time updates and status for both A and B sides of the MPS. A Java virtual machine version 1.5 or later is required.

The Java installation must be performed in the sequence shown:

- "Installing Java Plug-In" on page 5-3
- "Installing Java Policy File" on page 5-7
- "Adding Security Parameters to an Existing Java Policy File" on page 5-7 or "Creating a New Java Policy File" on page 5-9

Installing Java Plug-In

Because the Java applet is required for the EPAP GUI to operate, perform the following procedure to install the Java plug-in. You will perform this after completing the EPAP configuration described in "EPAP Configuration and Initialization" on page 5-10.

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 EPAP A machine. You will see the login screen. See Figure 3-9 on page 3-11.
2. Attempt to log in to the EPAP User Interface screen.
   If using Firefox, you will encounter the following message when logging into the EPAP 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

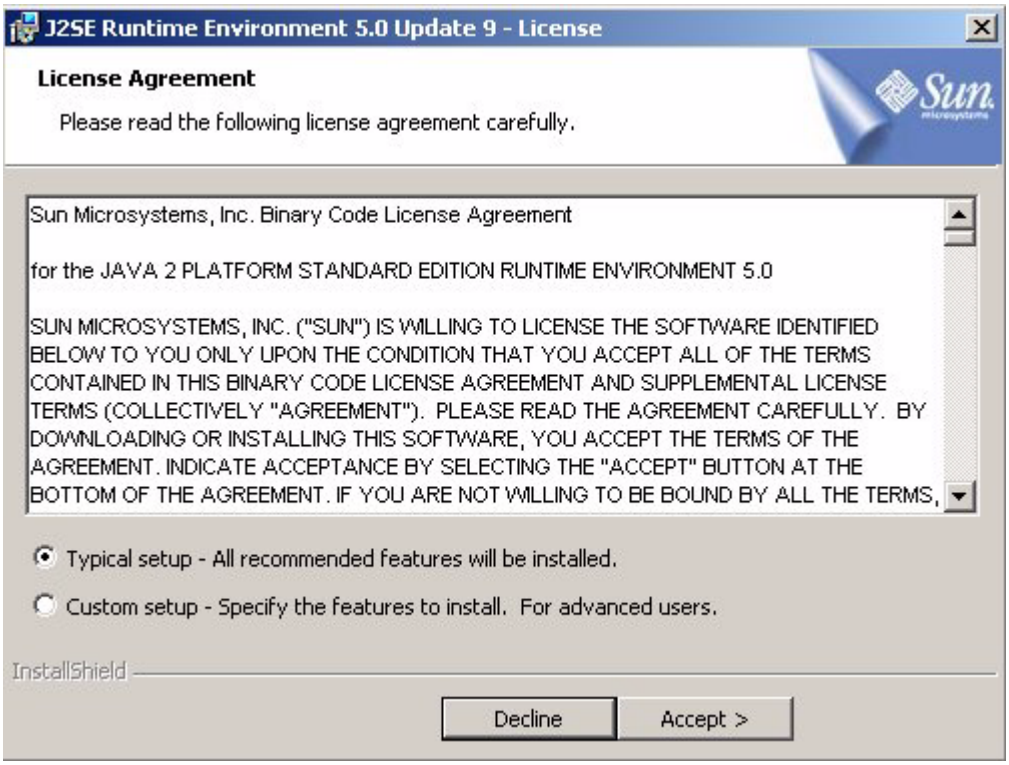
When you have successfully entered the Username and Password, the login process checks for the required Java plug-in. When it finds the Java 1.5 plug-in not present (but you had a previous version of Java installed), the system displays a 'Security Warning' window, shown in Figure 5-1.

Figure 5-1. Security Warning Window

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

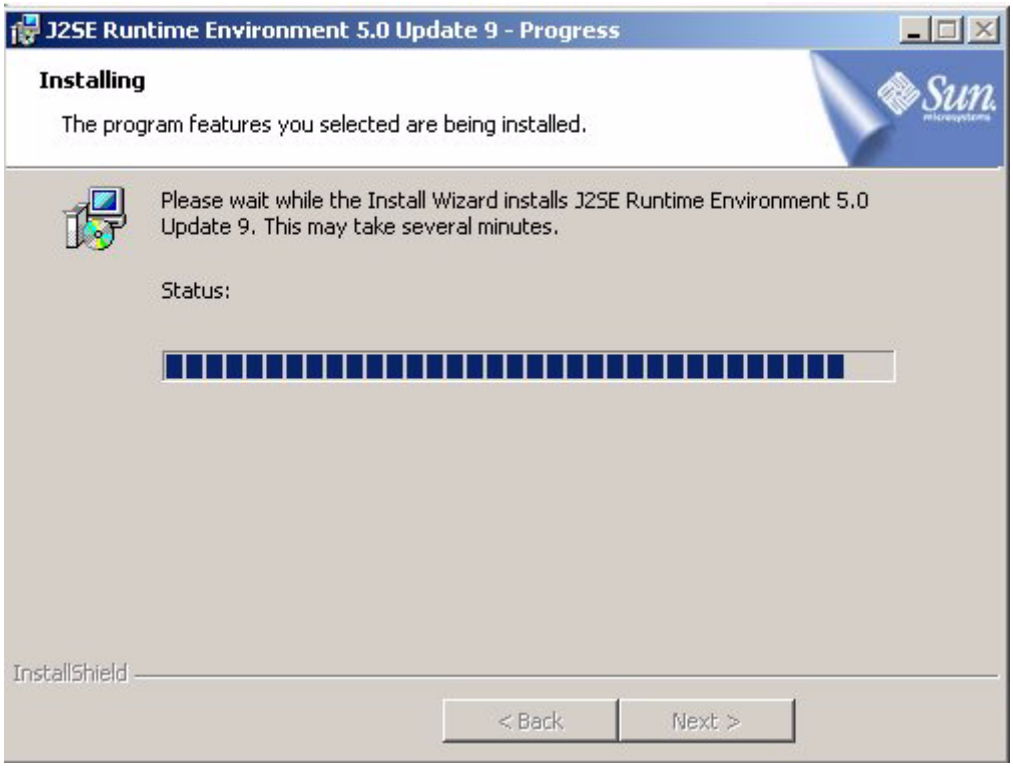
4. Next, the Java installation presents a Software Licensing Agreement screen shown in Figure 5-2.

Figure 5-2. Software Licensing Agreement



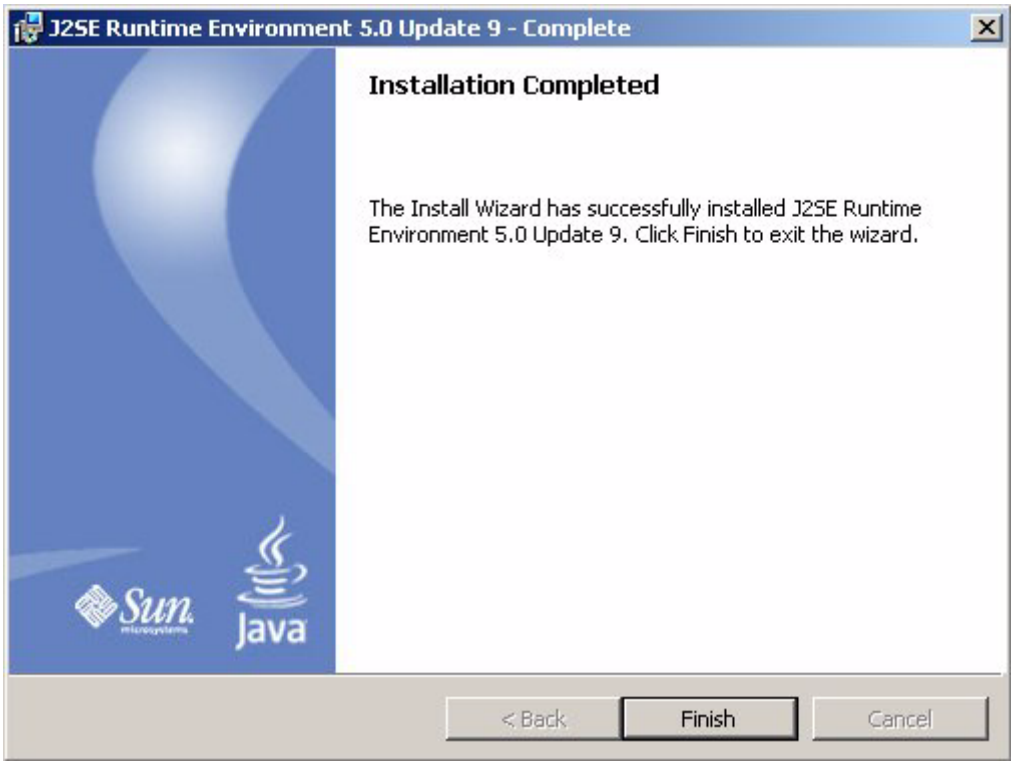
5. Ensure that the Typical Setup radio button is selected, and click the **Accept** button to accept the Sun Microsystems agreement.
6. The installation process starts, and a progress window displays, as shown in Figure 5-3.

Figure 5-3. Java Installation Progress Window



7. When the installation is complete, the Installation Complete window displays, as shown in 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 login screen in Figure 3-9 on page 3-11.

Installing Java Policy File

The banner applet makes a network connection to each MPS side. A Java policy file must be modified or created 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; for more information, see "VIOL" on page 3-15.

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.

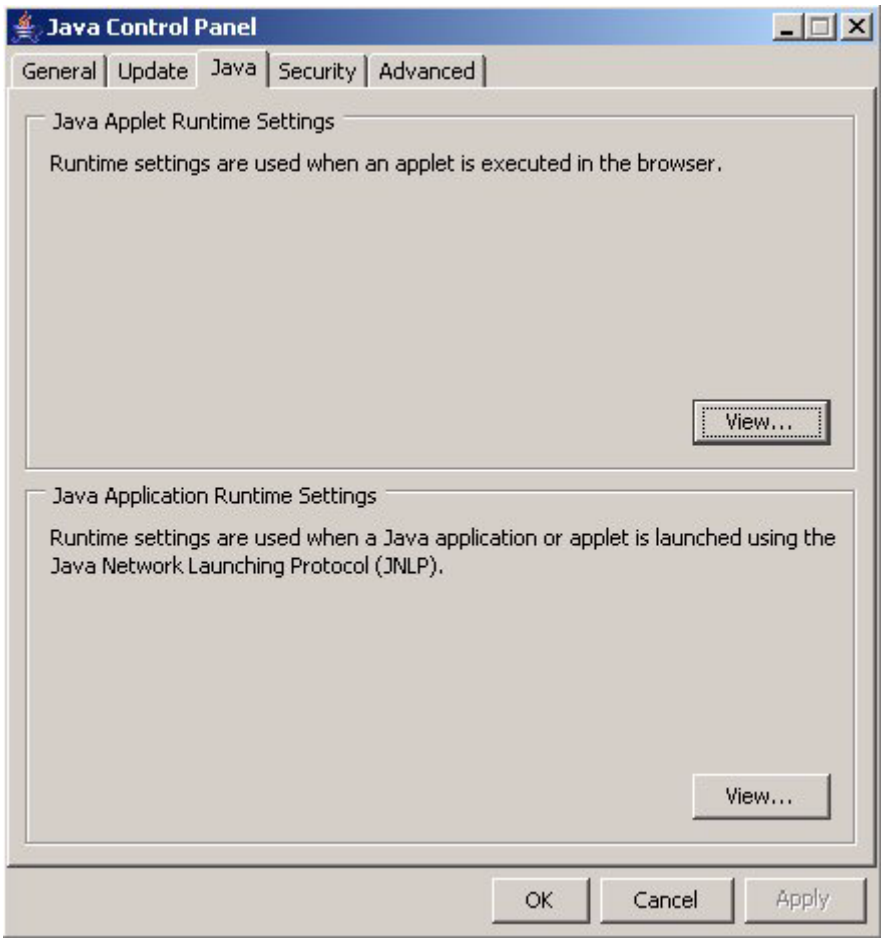
Adding Security Parameters to an Existing Java Policy File

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**.

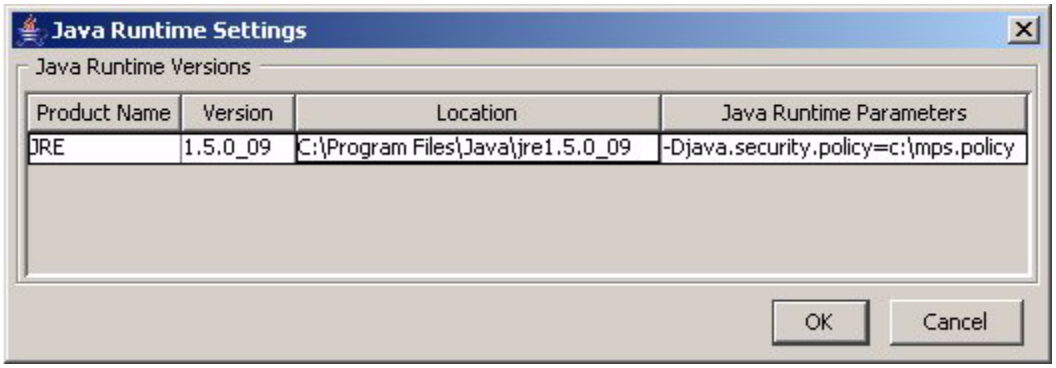
2. Select the Java Control Panel. When the Java Control Panel displays, click the **Java** tab. Figure 5-5 shows the **Java** tab contents.
3. Click the **Java** tab. The Control Panel displays as shown in Figure 5-5.

Figure 5-5. Java Control Panel, Java Tab



4. Click **View**. The Java Runtime Settings dialog box displays, as shown in Figure 5-6.

Figure 5-6. Java Runtime Settings Dialog Box



5. Adjust the width of the columns until you can read the contents of the Java Runtime Parameters column (at the far right).
6. Open the policy file indicated in the Java Runtime Parameters column, and insert the following text.

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

Creating 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 the steps 2 through 4 in the procedure in "Adding Security Parameters to an Existing Java Policy File" on page 5-7.
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}
```

EPAP Configuration and Initialization

Before you can begin using EPAP for provisioning, you must configure and initialize the EPAP software. The EPAP configuration and initialization is performed through the EPAP text-based user interface.

You connect a local (optional) customer terminal to eth0 (port 0 on GB card 1) on the MPS frame at each EAGLE 5 ISS. (Refer to the *Signaling Products Integrated Applications Installation Manual* .) To begin the initialization, you must log into EPAP A the first time as the "`epapconfig`" user. An automatic configuration is performed on both mated EPAPs.

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

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

Guideline Messages

The following messages are applicable to configuring the EPAP:

1. 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 **`epapdev`** user on the mate MPS server.
5. You must be prepared to designate this MPS as provisionable or non-provisionable. (Obtain and record the necessary information in the tables provided in "Required Network Address Information" on page 5-11. That data will be used in the configuration procedure.

Required Network Address Information

The following information is needed to configure the MPSs at EAGLE 5 ISS A, EAGLE 5 ISS B, and non-provisionable MPSs. Fill in the following tables for reference during the installation procedure.

Table 5-1. Information for Provisionable MPSs at EAGLE 5 ISS A

Common Information			
MPS A Provisioning Network Address		. . .	
MPS B Provisioning Network Address		. . .	
Netmask		. . .	
Default Router		. . .	
Backup Provisioning Network Information (Optional)			
MPS A Backup Provisioning Net. Addr.		. . .	
MPS B Backup Provisioning Net. Addr.		. . .	
Backup Netmask		. . .	
Backup Default Router		. . .	
RTDB Homing			
Select one: *(local MPS A address)*			
	Home to specific PDB	. . .	
	Active homing/allow alternate PDB		
	Active homing/disallow alternate PDB		
External Information			
MPS A Provisioning Network Address for MPS at EAGLE 5 ISS B (copy from Table 5-2)		. . .	
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 PDBI Port			
MPS A Forwarded Banner Port			
MPS B Forwarded Banner Port			
MPS A Provisioning Static NAT Addr.		. . .	
MPS B Provisioning Static NAT Addr.		. . .	
MPS A Forwarded HTTP Port for MPS at EAGLE 5 ISS B (Copy from Table 5-2)		. . .	

Table 5-2. Information for Provisionable MPSs at EAGLE 5 ISS B

Common Information		
MPS A Provisioning Network Address	. . .	
MPS B Provisioning Network Address	. . .	
Netmask	. . .	
Default Router	. . .	
Backup Provisioning Network Information (Optional)		
MPS A Backup Provisioning Net. Addr.	. . .	
MPS B Backup Provisioning Net. Addr.	. . .	
Backup Netmask	. . .	
Backup Default Router	. . .	
RTDB Homing		
Select one: *(local MPS A address)*		
Home to specific PDB	. . .	
Active homing/allow alternate PDB		
Active homing/disallow alternate PDB		
External Information		
MPS A Provisioning Network Address for MPS at EAGLE 5 ISS A (copy from Table 5-1)	. . .	
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 PDBI Port		
MPS A Forwarded Banner Port		
MPS B Forwarded Banner Port		
MPS A Provisioning Static NAT Addr.	. . .	
MPS B Provisioning Static NAT Addr.	. . .	
MPS A Forwarded HTTP Port for MPS at EAGLE 5 ISS A (Copy from Table 5-1)	. . .	

Table 5-3. Information for Non-Provisionable MPSs at EAGLE 5 ISS #1

Common Information	
MPS A Provisioning Network Address	. . .
MPS B Provisioning Network Address	. . .
Netmask	. . .
Default Router	. . .
Backup Provisioning Network Information (Optional)	
MPS A Backup Provisioning Net. Addr.	. . .
MPS B Backup Provisioning Net. Addr.	. . .
Backup Netmask	. . .
Backup Default Router	. . .
RTDB Homing	
Select one:	
☐ Home to specific PDB	. . .
☐ Active homing/allow alternate PDB	
☐ Active homing/disallow alternate PDB	
External Information	
MPS A Provisioning Network Address for MPS at EAGLE 5 ISS A (copy from Table 5-1)	. . .
MPS A Provisioning Network Address for MPS at EAGLE 5 ISS B (copy from Table 5-2)	. . .
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 Banner Port	
MPS B Forwarded Banner Port	
MPS A Provisioning Static NAT Addr.	. . .
MPS B Provisioning Static NAT Addr.	. . .

Table 5-4. Information for Non-Provisionable MPSs at EAGLE 5 ISS #2

Common Information				
MPS A Provisioning Network Address		.	.	.
MPS B Provisioning Network Address		.	.	.
Netmask		.	.	.
Default Router		.	.	.
Backup Provisioning Network Information (Optional)				
MPS A Backup Provisioning Net. Addr.		.	.	.
MPS B Backup Provisioning Net. Addr.		.	.	.
Backup Netmask		.	.	.
Backup Default Router		.	.	.
RTDB Homing				
Select one:				
	Home to specific PDB	.	.	.
	Active homing/allow alternate PDB			
	Active homing/disallow alternate PDB			
External Information				
MPS A Provisioning Network Address for MPS at EAGLE 5 ISS A (copy from Table 5-1)		.	.	.
MPS A Provisioning Network Address for MPS at EAGLE 5 ISS B (copy from Table 5-2)		.	.	.
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 Banner Port				
MPS B Forwarded Banner Port				
MPS A Provisioning Static NAT Addr.		.	.	.
MPS B Provisioning Static NAT Addr.		.	.	.

Configuration Menu Conventions

After you have logged into the EPAP user interface with the **epapconfig** 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. Figure 5-7 shows a sample configuration header format.

Figure 5-7. Configuration Menu Header Format

```
MPS Side A:  hostname: mpsa-d1a8f8  hostid: 80d1a8f8
             Platform Version: 9.0.0-22.0.0
             Software Version: EPAP 9.0.0-30.1.0
             Wed Jul 13 09:51:47 EST 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 return 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 EPAP user interface are listed in "EPAP Messages" on page 3-166. The possible error messages that can occur for each EPAP 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:

```
EXXXX: Error text
Press return to continue
```

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

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

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

EPAP Configuration Menu

Overview of EPAP Configuration

When you log into an EPAP with user name **epapconfig** after the first initialization of the EPAP, the configuration process begins. (See the details in "EPAP Configuration Procedure" on page 5-36.) The configuration process lets you change IP addresses, time zone, and password for "epapconfig". You can display the host ID and exchange secure shell keys. This section describes each configuration menu item.

Initial "epapconfig" User Logon

The first time the **epapconfig** 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 EPAPdev user on
                the mate MPS server.
             5. You must be prepared to designate this MPS as provisionable
                or non-provisionable.

Press return to continue...
```

If all five 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; the user is also notified if the sync network is not operational.

When the five 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
Password of epapdev:
Could not get authorized keys file from remote (mate).
Maybe it does not exist.  Continuing...
ssh is working correctly.
Password of root:
Could not get authorized keys file from remote (mate).
Maybe it does not exist.  Continuing...
ssh is working correctly.
Building the initial database on side A.
  Stopping local slave
  Stopping remote slave
EuiDB already exists.
  Starting local slave
  Starting remote slave
```

NOTE: Review the information required for the following section in "Required Network Address Information" on page 5-11. Make certain all required information is obtained and recorded in the tables provided.

Next, the installer declares the MPS to be provisionable or non-provisionable, as shown in Figure 5-10. The example illustrates this MPS as a provisionable MPS.

Figure 5-10. Designating Provisionable or Non-Provisionable MPS

```
The provisioning architecture of the EPAP software allows for exactly 2
customer provisionable sites.  Additional sites that are to receive the data
provisioned to the provisionable sites should answer 'N' here.

If there are only 2 mated sites, it is safe to answer 'Y' here.

Is this site provisionable? [Y]: y
```

Next, the installer is prompted for the **epapdev** user password on the mate MPS server. Figure 5-11 shows sample output that is generated after the correct password is entered.

Figure 5-11. Entering the **epapdev** Password

```
Password for EPAPdev@mate:

Connecting to mate...
ssh is working correctly.

still OK.
still OK.
Building the initial database on side A.
  Stopping local slave
  Stopping remote slave
No preexisting EuiDB database was detected.
Enabling replication:
  deleting old binary logs on local server
  resetting local slave.
  deleting old binary logs on remote server
  resetting remote slave
  Starting local slave
  Starting remote slave
There was no epap.cfg file.  Using default configuration.
```

Now is the first time the Configuration Menu will appear, and it is discussed next.

EPAP Configuration Menu

Following the report shown in Figure 5-11, the test-based EPAP Configuration Menu is displayed in Figure 5-12. The **epapconfig** user can now begin configuring the MPS local and remote servers.

Figure 5-12. EPAP Configuration Menu

```
MPS Side A:  hostname: mpsa-d1a8f8  hostid: 80d1a8f8
             Platform Version: 9.0.0-22.0.0
             Software Version: EPAP 9.0.0-30.1.0
             Wed Apr 18 09:51:47 EST 2007

 /-------EPAP 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         |
|----|-----------------------------------|
|  8 | PDB Configuration Menu            |
|----|-----------------------------------|
|  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.

Next the use of each of the menu options is explained.

Display Configuration

The Display Configuration option **1** displays a configuration of the EPAP. See an example of the Configuration Report in Figure 5-13.

Figure 5-13. Example of Configuration Report

```
MPS Side A:  hostname: mpsa-d1a8f8  hostid: 80d1a8f8
             Platform Version: 9.0.0-22.0.0
             Software Version: EPAP 9.0.0-30.1.0
             Wed Apr 18 09:51:47 EST 2007

EPAP A Provisioning Network IP Address = 192.168.66.60
EPAP B Provisioning Network IP Address = 192.168.66.61
Provisioning Network Netmask           = 255.255.255.0
Provisioning Network Default Router    = 192.168.66.250
EPAP A Backup Prov Network IP Address  = Not configured
EPAP B Backup Prov Network IP Address  = Not configured
Backup Prov Network Netmask            = Not configured
Backup Prov Network Default Router     = Not configured
EPAP A Sync Network Address            = 192.168.2.100
EPAP B Sync Network Address            = 192.168.2.200
EPAP A Main DSM Network Address        = 192.168.120.100
EPAP B Main DSM Network Address        = 192.168.120.200
EPAP A Backup DSM Network Address      = 192.168.121.100
EPAP B Backup DSM Network Address      = 192.168.121.200
EPAP A HTTP Port                       = 80
EPAP B HTTP Port                       = 80
EPAP A HTTP SuExec Port                = 8001
EPAP B HTTP SuExec Port                = 8001
EPAP A Banner Connection Port          = 8473
EPAP B Banner Connection Port          = 8473
EPAP A Static NAT Address              = Not configured
EPAP B Static NAT Address              = Not configured
PDBI Port                              = 5873
Remote MPS A Static NAT Address        = Not configured
Remote MPS A HTTP Port                 = 80
Local Provisioning VIP                 = 192.168.66.80
Remote Provisioning VIP                = 192.168.66.78
Local PDBA Address                     = 192.168.66.60
Remote PDBA Address                    = 0.0.0.0
Time Zone                              = America/New_York
PDB Database                           = None
Preferred PDB                          = 192.168.66.60
Allow updates from alternate PDB       = Yes
Auto DB Recovery Enabled               = No
PDBA Proxy Enabled                     = Yes

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 5-5 shows an example of IP addresses that could be used in the configuration process.

Table 5-5. Sample IP Addresses Used in Configuration

Provisioning Network Information	MPS EAGLE 5 ISS A (Local) IP Addresses	MPS EAGLE 5 ISS B (Remote) IP Addresses
EPAP A Provisioning Network IP Address (MPS A)	192.168.61.119	192.168.61.90
EPAP B Provisioning Network IP Address (MPS B)	192.168.61.120	192.168.61.91
Network Net Mask	255.255.255.0	255.255.255.0
Default Router	192.168.61.250	192.168.61.250

Configure Network Interfaces Menu

The Configure Network Interfaces Menu option **2** of the Configuration Menu displays the submenu shown in Figure 5-14. It supports the configuration of all the network interfaces for the EPAP.

Figure 5-14. Configure Network Interfaces Menu

```
MPS Side A:  hostname: mpsa-f0ad77  hostid: 80f0ad77
             Platform Version: 9.0.0
             Software Version: EPAP 9.0.0-20.18.0
             Wed Apr 18 09:51:47 EST 2007

 /-----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       |
|----|--------------------------------------|
|  7 | Configure Provisioning VIP Addresses  |
|----|--------------------------------------|
|  e | Exit                                 |
\-------------------------------------------/

Enter choice:
```

Configure Provisioning Network

The Configure Provisioning Network option **1** of the Configure Network Interfaces Menu configures the EPAP provisioning network. These include the provisioning network's IP address, netmask, and default router IP address. This information allows the EPAP to communicate with an existing customer network.

NOTE: You must configure these IP addresses. Obtain the values for the IP address, netmask, and default router from the customer's Information Services department. Record the values in the four tables in "Required Network Address Information" on page 5-11.

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 5-15 for the option **1** output.

Figure 5-15. Configure Provisioning Network Output

```
Verifying connectivity with mate ...
Enter the EPAP A provisioning network IP Address [192.168.61.90]:
Enter the EPAP B provisioning network IP Address [192.168.61.91]:
Enter the EPAP provisioning network netmask [255.255.255.0]:
Enter the EPAP provisioning network default router IP Address: 192.168.61.250

Press return to continue ...
```

NOTE: Take care in configuring the IP information. Incorrect information can prevent the EPAP from accepting provisioning data and establishing remote EPAP user interface connections over the customer network.

Configure Sync Network

The Configure Sync Network option **2** of the Configure Network Interfaces Menu lets you specify the Sync network IP address of the selected EPAP. Sync network IP addresses are configured to default values during EPAP initialization (see Figure 2-2 on page 2-5). The third octet of the address can be changed after EPAP initialization is complete.

NOTE: You must configure these IP addresses. Obtain the values for the IP address, netmask, and default router from the customer's Information Services department. Record the values in the four tables in "Required Network Address Information" on page 5-11.

See "Network Connections" on page 2-9 for a description of EPAP network IP address assignments. See Figure 5-16 for the option **2** output.

Figure 5-16. Configure Sync Network

```
Verifying connectivity with mate...
Enter the first 3 octets for the EPAP MPS sync Network [192.168.4]
Press return to continue...
```

CAUTION: Take care in entering the prompt responses. Entering incorrect information or rebooting at the wrong time may result in improper operation of the EPAP.

If you reboot at the wrong time, you need to contact Tekelec Customer Care Services for assistance in resolving this situation.

Configure DSM Network

The Configure DSM Network option **3** of the Configure Network Interfaces Menu prompts you for the EPAP DSM network IP addresses. This information allows the EPAP to communicate with the main and backup DSM networks.

NOTE: Unless there is a known network address conflict, the installer can bypass option 3.

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 "Network Connections" on page 2-9 for a description of EPAP network IP address assignments. See Figure 5-17 for the option **3** output.

Figure 5-17. Configure DSM Network

```
Verifying connectivity with mate ...
Enter the first 3 octets for the EPAP main DSM network [192.168.128]:
Enter the first 3 octets for the EPAP backup DSM network [192.168.129]:

Press Return to continue ...
```

NOTE: Take care in configuring the IP information. Incorrect information will prevent the EPAP from communicating with the EAGLE 5 ISS.

Configure Backup Provisioning Network

The Configure Backup Provisioning Network option **4** of the Configure Network Interfaces Menu prompts you for the EPAP Backup Provisioning Network IP addresses. This information allows the EPAP to communicate with the backup provisioning network. In response to each prompt, enter a dotted decimal IP address.

See "Network Connections" on page 2-9 for a description of EPAP network IP address assignments. See Figure 5-18 for the option **4** output.

Figure 5-18. Configure Backup Provisioning Network

```
Verifying connectivity with mate…
EPAP A backup provisioning network IP Address: 192.168.59.169
EPAP B backup provisioning network IP Address: 192.168.59.170
EPAP backup provisioning network netmask: 255.255.255.0
EPAP backup provisioning network default router IP Address: 192.168.59.250

Press return to continue ...
```

NOTE: Take care in configuring the IP information. Incorrect information will prevent the EPAP from communicating with the Backup Provisioning Network.

Configure Forwarded Ports

The Configure Forwarded Ports option **5** of the Configure Network Interfaces Menu provides the functionality to configure EPAP 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 Tables 5-1 and 5-2.

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 EPAP.

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 5-19 shows an example of a resulting prompt.

Figure 5-19. Configuring NAT Addresses Prompt

```
EPAP A Static NAT Address:
```

Configure Provisioning VIP Addresses

The Configure Provisioning VIP Addresses option **7** from the Configure Network Interfaces Menu provides the functionality to configure the PDBA Proxy feature.

The user must enter the VIP address for the local PDBA (MPS-A) and the remote PDBA. See Figure 5-21 for the option **7** output.

Figure 5-20. Configure Provisioning VIP Addresses Output

```
EPAP software is running.  Stop it? [N]: y
EPAP local provisioning Virtual IP Address [192.168.66.80]:
EPAP remote provisioning Virtual IP Address [192.168.66.78]:


Press return to continue...
```

Set Time Zone

The Select Time Zone option **3** prompts you for the time zone to be used by the EPAP. The time zone can be the zone where the EPAP 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 Figure 5-21 for the option **3** output.

Figure 5-21. Select Time Zone Menu

```
Caution: This action requires a reboot of the affected MPS servers to
         activate the change.  Operation of the EPAP software before
         the MPS servers are rebooted may have unpredictable consequences.

Press return to continue...

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 Appendix A 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 menu is described in "Reboot the MPS" on page 3-62.

Exchange Secure Shell Keys

The Exchange Secure Shell Keys option **4** accesses the Exchange Secure Shell Keys menu. This menu is used to enable connections between local and remote EPAPs. The EPAPs exchange encryption keys are required to run the secure shell.

The exchange normally occurs automatically during EPAP initialization. Use this menu item only if the exchange must be performed manually.

See Figure 5-22 for the option **4** output.

Figure 5-22. Exchange Secure Shell Keys Menu

```
MPS Side A:  hostname: tortola-a  hostid: a8c0883d
             Platform Version: 9.0.2-4.0.0_50.26.0
             Software Version: EPAP 9.0.1-4.0.0_50.34.0
             Wed Apr 18 09:51:47 EST 2007

 /-----Exchange Secure Shell Keys Menu-----\
/-----------------------------------------\
|  1 | Exchange Keys with Mate             |
|----|-------------------------------------|
|  2 | Exchange Keys with Remote           |
|----|-------------------------------------|
|  3 | Exchange Keys with Mate as Root User |
|----|-------------------------------------|
|  e | Exit                                |
\-----------------------------------------/

Enter Choice:
```

Option **1** is used for the initial configuration. Option **2** is used to do a reload of the RTDB from the remote server. Option **3** is required before using the PDBA Proxy feature. Before doing a reload from the remote server, you must exchange keys with the remote server.

The **epapconfig** user must know the password for the **epapdev@mate**. The notification "ssh is working correctly" in the following figure confirms the "ssh" (i.e., secure shell) exchange of keys has completed successfully.

See Figure 5-23 for the Option **1** output.

Figure 5-23. Exchange Secure Shell Keys Output

```
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...
Are you sure you wish to exchange keys with the mate? [N]: Y
Password for epapdev@mate:
Connecting to mate...
ssh is working correctly.
```

Change Password

The Change Password option **5** changes the text-based user interface password for the **epapconfig** login name for both MPS A and B.

See Figure 5-24 for the option **5** output.

Figure 5-24. 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

The EPAP Platform Option **6** accesses the Platform menu so that the **epapconfig** user can access and manage the platform functions shown in the menu. See Figure 5-25 for the option 6 output.

Figure 5-25. Platform Menu Output

```
 MPS Side A:  hostname: mpsa-d1a8f8  hostid: 80d1a8f8
              Platform Version: 9.0.0
              Software Version: EPAP 9.0.0-20.11.0
              Wed Apr 18 09:51:47 EST 2007

 /-----EPAP Platform Menu-\
/--------------------------\
|  1 | Initiate Upgrade    |
|----|---------------------|
|  2 | Eject CD            |
|----|---------------------|
|  3 | Reboot MPS          |
|----|---------------------|
|  4 | Halt MPS            |
|----|---------------------|
|  5 | File System Backup  |
|----|---------------------|
|  6 | MySQL Backup        |
|----|---------------------|
|  7 | RTDB Backup         |
|----|---------------------|
|  8 | PDB Backup          |
|----|---------------------|
|  e | Exit                |
\--------------------------/

Enter choice:
```

Initiate Upgrade

The Initiate Upgrade option **1** of the EPAP Platform Menu initiates an upgrade on the selected EPAP. For upgrade output or procedures, contact Tekelec Customer Care Services; refer to “Customer Assistance” on page 1-4.

Eject CD

The Eject CD option **2** of the EPAP Platform Menu initiates an ejection of the CD media on the selected EPAP. The default, as shown next, is 'BOTH'.

```
Eject CD tray of MPS A, MPS B or BOTH? [BOTH]:
```

Reboot MPS

The Reboot MPS option **3** of the EPAP Platform Menu initiates a reboot of either MPS or both. The default, as shown below, is BOTH.

NOTE: The `epapconfig` user can abort rebooting the MPS by pressing the Escape key at the displayed prompt.

```
Reboot MPS A, MPS B or [BOTH]:
```

NOTE: Rebooting the MPS stops all EPAP processes, and databases cannot be updated until the MPS has completely booted.

Halt MPS

The Halt MPS option **4** of the EPAP Platform Menu initiates a halt of one MPS or both. The default, as shown below, is BOTH.

NOTE: Halting an MPS stops all EPAP processes. Selecting the default to halt BOTH (MPS A and MPS B) requires a person to be physically present in order to reboot MPS to allow for further access!

```
Halt MPS A, MPS B or [BOTH]: y
```

NOTE: The `epapconfig` user can abort halting the MPS by pressing the Escape key at the displayed prompt.

File System Backup

The File System Backup option **5** of the EPAP Platform Menu backs up all system files. The output is shown below.

```
Are you sure you want to back up the file system on MPS A? [N]: y
Backing up MPS A file system...
```

NOTE: This option does not backup database files.

MySQL Backup

The MySQL Backup option **6** of the EPAP Platform Menu backs up the MySQL database. The output is shown below.

NOTE: EPAP software must be stopped or MySQL backup will abort and return to the EPAP Platform Menu.

```
EPAP software is running. Stop it? [N]: y

Are you sure you want to back up the MYSQL on MPS? [N]: y
Backing up MPS A file system...
```

RTDB Backup

The RTDB Backup option **7** of the EPAP Platform Menu backs up the RTDB database. The output is shown below.

```
EPAP software is running. Stop it? [N]: y

Are you sure you want to back up the RTDB database on MPS A? [N]: y
Backing up MPS A file system...
```

NOTE: EPAP software must be stopped, or the RTDB backup will abort and return to the EPAP Platform Menu.

PDB Backup

The PDB Backup option **8** of the EPAP Platform Menu backs up the PDB database. The output is shown next.

```
Are you sure you want to backup the PDB to
/var/TKLC/epap/free/pdbBackup_megalon-a_20030530104740_DBBirthdate_200305
30144717GMT_DBLevel_0.bkp? [N]: Y

Successfully started backup of PDB.
Status will be displayed on the GUI banner.
```

EPAP Platform Menu Exit

The Exit option **e** of the EPAP Platform Menu exits from the EPAP Platform Menu and returns to the EPAP Configuration Menu.

Configure NTP Server Menu

The Configure NTP Server Menu option **7** allows for the display, addition, and removal of an external NTP server. See Figure 5-26 for the option 9 output.

Figure 5-26. Configure NTP Server Menu

```
 /----EPAP 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 option **1** of the Configure NTP Server Menu 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 option **2** of the Configure NTP Server Menu adds an External NTP Server. The output below shows 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]: y
Enter the EPAP NTP Server IP Address: 192.168.61.69

Verifying NTP Server. It might take up to 1 minute.

External NTP Server [192.168.61.69]
has been added.

Press return to continue...
```

Remove External NTP Server

The Remove External NTP Server option **3** of the Configure NTP Server Menu 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...
```

EPAP Configure NTP Server Menu Exit

The EPAP Configure NTP Server Menu Exit option **e** exits the EPAP Configure NTP Server Menu, and returns to the EPAP Configuration Menu.

PDB Configuration Menu

The PDB Configuration Menu option **8** supports configuring the PDB network, homing of the RTDBs, changing the MPS provisionable status, creating the PDB, and the enabling of the Automated Database Recovery and PDBA Proxy features. See Figure 5-27 for the option **8** output.

Figure 5-27. Configure PDB Menu

```
 /-----Configure PDB Menu------------\
/-------------------------------------\
|  1 | Configure PDB Network          |
|----|--------------------------------|
|  2 | RTDB Homing Menu               |
|----|--------------------------------|
|  3 | Change MPS Provisionable State |
|----|--------------------------------|
|  4 | Create PDB                     |
|----|--------------------------------|
|  5 | Change Auto DB Recovery State  |
|----|--------------------------------|
|  6 | Change PDBA Proxy State        |
|----|--------------------------------|
|  e | Exit                           |
\-------------------------------------/

Enter Choice:
```

Configure PDB Network

The Configure PDB Network option **1** of the Configure PDB Menu identifies the provisioning network interface addresses of the remote PDB(s). For provisionable MPSs, the local provisioning interface address is known. The configuration user interface prompts for only the remaining remote address. Non-provisionable MPSs prompt for both remote PDB addresses.

Provisionable MPSs then prompt for the password of the **epapdev** user at the remote PDB address.

NOTE: If you accept the 'No' default (that is, not stopping EPAP software and the PBA from running), the configuration process will abort. The following examples show the responses required to continue the initial configuration.

Figure 5-28 shows the provisionable MPS configuration, and Figure 5-29 shows the non-provisionable MPS configuration.

Figure 5-28. Configure PDB Network for Provisionable MPS

```
This MPS is configured to be provisionable.  The EPAP local PDBA
address is 192.168.61.84.

EPAP software and PDBA are running. Stop Them? [N] y

Enter the EPAP remote PDBA address: 192.168.61.86

Password for epapdev@192.168.61.119:
Keys exchanged.
Verifying that ssh works correctly.

ssh is working correctly.

Press return to continue...
```

Figure 5-29. Configure PDB Network for Non-Provisionable MPS

```
This MPS is configured to be non-provisionable.  You will be prompted
for both of the remote PDB addresses.  Order does not matter.

EPAP software and PDBA are running. Stop Them? [N] y

Enter one of the two PDBA addresses: 192.168.61.84
Enter the other of the two PDBA address: 192.168.61.86

Press return to continue...
```

RTDB Homing Menu

The RTDB Homing Menu option **2** of the Configure PDB Menu provides a menu to configure specific and active homing of RTDBs to the PDBAs. For more information about active and specific homing, refer to "Selective Homing of EPAP RTDBs" on page 2-19. Figure 5-30 shows the option **2** output.

Figure 5-30. RTDB Homing Menu

```
/-------RTDB Homing Menu------------\
/-------------------------------------\
|  1 | Configure Specific RTDB Homing |
|----|--------------------------------|
|  2 | Configure Active RTDB Homing   |
|----|--------------------------------|
|  3 | Configure Standby RTDB Homing  |
|----|--------------------------------|
|  e | Exit                           |
\-------------------------------------/

Enter Choice:
```

Configure Specific RTDB Homing

The Configure Specific RTDB Homing option **1** of the RTDB Homing Menu sets the RTDB homing policy to "specific" and configures the address of the preferred PDB.

This configuration cannot be completed until the PDB network has been configured (see "Configure PDB Network" on page 5-32). Provisionable sites indicate the address of the local PDB with the text '(local)' and that site is the default value for the preferred PDB.

The text-based user interface prompts for the preferred PDB. When the choice is selected, the text confirms the choice and identifies the selection is 'specific' homing.

```
EPAP software and PDBA are running. Stop Them? [N] y

There are two configured PDBs for this MPS:
1. 192.168.61.84 (local)
2. 192.168.61.86

Select the preferred PDB from which to receive updates [1]: 1

The RTDB Homing policy is set to 'specific' and will prefer updates
from 192.168.61.84.
```

Configure Active RTDB Homing

The Configure Active RTDB Homing option **2** of the RTDB Homing Menu sets the RTDB homing policy to "active" and configures whether or not to allow updates from the alternate PDB. The prompt selection must be confirmed if updates are not allowed from the standby PDB.

The text-based user interface prompts for whether updates are to be allowed from the standby MPS. When the choice is entered, the text confirms the choices and identifies the selection is 'active' homing and whether updates are allowed from the standby MPS's PDB.

```
EPAP software and PDBA are running. Stop Them? [N] y

In the event that the active PDB is unavailable, should updates be
allowed to the RTDBs from the standby MPS? [Y]: N

Caution: If this option is selected, the standby PDB will not
provision the RTDBs at this site in the event that the active PDB is
not available.

Are you sure you want to disallow updates to the RTDBs from the
standby PDB? Y

The RTDB Homing policy is set to 'active' and will not allow updates
from the standby PDB.
```

Configure Standby RTDB Homing

The Configure Standby RTDB Homing option **3** of the RTDB Homing Menu sets the RTDB homing policy to "standby" and configures whether or not to allow updates from the active PDB. The prompt selection must be confirmed if updates are not allowed from the active PDB.

The text-based user interface prompts for whether updates are to be allowed from the active MPS. When the choice is entered, the text confirms the choices and identifies the selection is 'standby' homing and whether updates are allowed from the active MPS's PDB.

```
EPAP software and PDBA are running. Stop Them? [N] y

In the event that the standby PDB is unavailable, should updates be
allowed to the RTDBs from the active MPS? [Y]: N

Caution: If this option is selected, the active PDB will not provision
the RTDBs at this site in the event that the standby PDB is not
available.

Are you sure you want to disallow updates to the RTDBs from the active
PDB? Y

The RTDB Homing policy is set to 'standby' and will not allow updates
from the active PDB.
```

Change MPS Provisionable State

The Change MPS Provisionable State option **3** of the Configure PDB Menu specifies this site as 'provisionable' or 'non-provisionable.' (For more information, refer to "Provisioning Multiple EPAPs Support" on page 2-17.) This command essentially toggles (i.e., alternates) the states between provisionable and non-provisionable.

See Figure 5-10, on Page 5-18 for the prompt resulting from this menu item.

Create PDB

The Create PDB option **4** of the Configure PDB Menu creates and initializes a provisioning database (PDB) for the EPAP.

CAUTION: If the text-based UI is exited before the successful creation of the PDB on a provisionable MPS, this caution message is displayed.

```
PDB not created

Caution: This MPS has not been completely configured.  Applications may not
         run until all required parameters are entered through the text
         user interface.  Choose "Display Configuration" for a list of
         configurable parameters and their settings.

Press return to continue...
```

Change Auto DB Recovery State

The Change Auto DB Recovery State option **5** of the Configure PDB Menu is used to enable the Automated Database Recovery feature.

The text-based user interface prompts with the following text.

```
Auto DB Recovery is currently DISABLED.
Do you want to ENABLE Auto DB Recovery? [N]:
```

Change PDBA Proxy State

The Change PDBA Proxy State option **6** of the Configure PDB Menu is used to enable the PDBA Proxy feature.

The text-based user interface prompts with the following text.

```
PDBA PROXY is currently DISABLED.
Do you want to ENABLE PDBA Proxy? [N]:
```

PDB Configuration Menu Exit

The Exit option **e** of the PDB Configuration Menu exits and returns to the EPAP Configuration Menu, shown in Figure 5-12, on Page 5-19.

EPAP 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 **epapconfig** logs into MPS A, the system performs an auto-configuration on both MPS EPAP pairs. The sync network and main and backup DSM networks are initialized to their default values, described in "Network Connections" on page 2-9 and defined in the *Signaling Products Integrated Applications Installation Manual* . 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; the installer must also perform initial configuration on non-provisionable MPSs, if they are present.

Configuration Terms and Assumptions

- The initial configuration steps assume that each MPS has previously undergone successful Initial Platform Manufacture (IPM).
- The network path must be present and verified before the MPS servers are ready for EPAP 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 **epapconfig** 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 EPAPs 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. Up to 3 external servers are supported.

- The EPAP terms 'local' and 'remote' are relative with respect to the EPAP 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 EPAPs 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, or a non-provisionable MPS. To assist the installer, this manual uses these symbols to indicate individual instructions to be performed for those specific MPSs.

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.
	This symbol indicates installation instructions to be performed specifically for any non-provisionable MPSs.

Initial Setup and Connecting to MPSs

Installation personnel may choose to employ various methods for connecting to an MPS. The EPAP software requires that an MPS be configured from side A. Refer to the *Integrated Applications Installation Manual* for the correct installation procedure.

Procedure for Configuring EPAPs

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" on page 5-37), you can perform this procedure to configure the EPAPs in your network.

NOTE: Initial configuration cannot be performed through the GUI because 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 **epapconfig**. A note of caution appears, and the installer must evaluate the conditions listed. When all the conditions of the Caution notice are satisfied, the installer presses the Return key to continue.

```
mpsa-f0c7c3 console login: epapconfig
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 EPAPdev user on
                the mate MPS server.
             5. You must be prepared to designate this MPS as provisionable
                or non-provisionable.

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
Password of epapdev:
Could not get authorized keys file from remote (mate).
Maybe it does not exist.  Continuing...
ssh is working correctly.
Password of root:
Could not get authorized keys file from remote (mate).
Maybe it does not exist.  Continuing...
ssh is working correctly.
Building the initial database on side A.
  Stopping local slave
  Stopping remote slave
EuiDB already exists.
  Starting local slave
  Starting remote slave
```

MPS on EAGLE 5 SAS B:
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 on page 5-36).

---

3. Next, the installer declares whether the MPS is provisionable or non-provisionable. (This example shows this MPS as a provisionable MPS.)

MPS on EAGLE 5 SAS A:
The installer should answer y in this step.

MPS on EAGLE 5 SAS B:
The installer should answer y in this step.

Non-Provisionable MPS:
The installer should answer n in this step.

```
The provisioning architecture of the EPAP software allows for exactly
2 customer provisionable sites.  Additional sites that are to receive
the data provisioned to the provisionable sites should answer 'N'
here.

If there are only 2 mated sites, it is safe to answer 'Y' here.

Is this site provisionable? [Y]: y
```

---

4. Next, the installer is prompted for the **epapdev** 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 EPAPdev@mate:

Connecting to mate...
ssh is working correctly.

still OK.
still OK.
Building the initial database on side A.
  Stopping local slave
  Stopping remote slave
No preexisting EuiDB database was detected.
Enabling replication:
  deleting old binary logs on local server
  resetting local slave.
  deleting old binary logs on remote server
  resetting remote slave
  Starting local slave
  Starting remote slave
There was no epap.cfg file.  Using default configuration.
```

5. A successful configuration file setup results in the display (for the first time) of the EPAP 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: mpsa-d1a8f8  hostid: 80d1a8f8
             Platform Version: 9.0.0-22.0.0
             Software Version: EPAP 9.0.0-30.1.0
             Wed Apr 18 09:51:47 EST 2007

 /-------EPAP 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         |
|-----|-----------------------------------|
|  8  | PDB Configuration Menu            |
|-----|-----------------------------------|
|  e  | Exit                              |
\----------------------------------------/

Enter Choice:
```

6. Choose option **1** for Display Configuration, which provides a means of verifying EPAP A and EPAP B Provisioning Network IP addresses, the Time Zone, and other provisioning values for the MPS on EAGLE 5 ISS A.

```
EPAP A Provisioning Network IP Address = 192.168.66.60
EPAP B Provisioning Network IP Address = 192.168.66.61
Provisioning Network Netmask           = 255.255.255.0
Provisioning Network Default Router    = 192.168.66.250
EPAP A Backup Prov Network IP Address  = Not configured
EPAP B Backup Prov Network IP Address  = Not configured
Backup Prov Network Netmask            = Not configured
Backup Prov Network Default Router     = Not configured
EPAP A Sync Network Address            = 192.168.2.100
EPAP B Sync Network Address            = 192.168.2.200
EPAP A Main DSM Network Address        = 192.168.120.100
EPAP B Main DSM Network Address        = 192.168.120.200
EPAP A Backup DSM Network Address      = 192.168.121.100
EPAP B Backup DSM Network Address      = 192.168.121.200
EPAP A HTTP Port                       = 80
EPAP B HTTP Port                       = 80
EPAP A HTTP SuExec Port                = 8001
EPAP B HTTP SuExec Port                = 8001
EPAP A Banner Connection Port          = 8473
EPAP B Banner Connection Port          = 8473
EPAP A Static NAT Address              = Not configured
EPAP B Static NAT Address              = Not configured
PDBI Port                              = 5873
Remote MPS A Static NAT Address        = Not configured
Remote MPS A HTTP Port                 = 80
Local Provisioning VIP                 = 192.168.66.80
Remote Provisioning VIP                = 192.168.66.78
Local PDBA Address                     = 192.168.66.60
Remote PDBA Address                    = 0.0.0.0
Time Zone                              = America/New_York
PDB Database                           = None
Preferred PDB                          = 192.168.66.60
Allow updates from alternate PDB       = Yes
Auto DB Recovery Enabled               = No
PDBA Proxy Enabled                     = Yes

Press return to continue...
```

7. Press `Return` to return to the `EPAP Configuration Menu`.

8. Choose option **2**, Configure Network Interfaces Menu.

```
 /-------EPAP 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        |
|-----|----------------------------------|
|  8  | PDB Configuration Menu           |
|-----|----------------------------------|
|  e  | Exit                             |
\---------------------------------------/

Enter Choice: 2
```

9. Choose option **1**, Configure Provisioning Network from the `Configure Network Interfaces Menu`.

```
MPS Side A:  hostname: dakar  hostid: a8c03c42
             Platform Version: 9.0.4-0.19570
             Software Version: EPAP 9.0.8-0.19570
             Wed Apr 18 09:51:47 EST 2007

 /-----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       |
|-----|--------------------------------------|
|  7  | Configure Provisioning VIP Addresses |
|-----|--------------------------------------|
|  e  | Exit                                 |
\-------------------------------------------/

Enter choice: 1
```

10. The Configure Provisioning Network lets the installer accept the default IP address values presented by the configuration software for EPAP A and EPAP 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 through Table 5-4 for the correct addresses.

NOTE: No default value is provided for the EPAP 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 EPAP A provisioning network IP Address [192.168.61.90]:
Enter the EPAP B provisioning network IP Address [192.168.61.91]:
Enter the EPAP provisioning network netmask [255.255.255.0]:
Enter the EPAP provisioning network default router IP Address:
192.168.61.250

Press return to continue…
```

11. Press the Return key, to return to the `Configure Network Interfaces Menu`.

NOTE: Note: Unless there is a known network address conflict, the installer should skip all steps related to option 2, Configure Sync Network and continue with step 16.

12. Enter option **2**, Configure Sync Network 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       |
|-----|--------------------------------------|
|  7  | Configure Provisioning VIP Addresses |
|-----|--------------------------------------|
|  e  | Exit                                 |
\--------------------------------------------/

Enter choice: 2
```

13. A sample output follows:

```
Verifying connectivity with mate...
Enter the first 3 octets for the EPAP MPS sync Network [192.168.4]
Press return to continue...
```

14. 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.

15. After accepting the default value or entering a specific EPAP Sync IP address octet value, the installer returns to the Configure Network Interfaces Menu.

NOTE: Unless there is a known network address conflict, the installer should skip all steps (Step 16 through Step 19) related to option 3, Configure DSM Network.

16. Choose option **3**, Configure DSM Network 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        |
|----|---------------------------------------|
|  7 | Configure Provisioning VIP Addresses  |
|----|---------------------------------------|
|  e | Exit                                  |
\--------------------------------------------/

Enter choice: 3
```

17. 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 EPAP main DSM network and the EPAP 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 EPAP main DSM network [192.168.136]:
Enter the first 3 octets for the EPAP backup DSM network [192.168.137]:
```

18. After accepting the default value or entering a specific EPAP backup DSM network octet IP address value, the installer returns to the Configure Network

NOTE: If no backup provisioning network interface is desired at this time, the installer should skip this step. Proceed to step 22.

19. Choose option **4**, Configure Backup Provisioning Network 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       |
|-----|--------------------------------------|
|  7  | Configure Provisioning VIP Addresses |
|-----|--------------------------------------|
|  e  | Exit                                 |
\--------------------------------------------/

Enter choice: 4
```

20. This menu selection prompts the installer for all information necessary to set up a second interface for the customer's Provisioning Network. The address information should be received from the customer for the MPS. Refer to the information recorded in Table 5-1 through Table 5-4 for the correct addresses.

The IP address for this interface must be on a different class C subnet than the primary Provisioning Network address. The installer also has the option of setting up a second default router address to coincide with the Backup Provisioning Network. If the default router field is left empty, a second default route will not be added.

There are no default values for any of these fields. The customer must supply all the information.

```
Verifying connectivity with mate…
EPAP A backup provisioning network IP Address: 192.168.59.169
EPAP B backup provisioning network IP Address: 192.168.59.170
EPAP backup provisioning network netmask: 255.255.255.0
EPAP backup provisioning network default router IP Address:
192.168.59.250

Press return to continue ...
```

21. Press the Return key, to return to the `Configure Network Interfaces Menu`.

NOTE: Unless the MPS is separated from the GUI workstations and provisioning systems by a port forwarding firewall, the following Steps for configuring forwarding ports can be skipped. Continue with Step 26.

22. Choose option **5**, `Configure Forwarded Ports` 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       |
|-----|--------------------------------------|
|  7  | Configure Provisioning VIP Addresses |
|-----|--------------------------------------|
|  e  | Exit                                 |
\--------------------------------------------/

Enter choice: 5
```

23. 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.

A Options 1, 3, 5, and 7 are valid.

B Options 2, 4, and 6 are valid.

```
 /-----Configure Forwarded Ports Menu------\
/--------------------------------------------\
|  1  | Change EPAP A HTTP Port              |
|-----|--------------------------------------|
|  2  | Change EPAP B HTTP Port              |
|-----|--------------------------------------|
|  3  | Change EPAP A HTTP SuExec Port       |
|-----|--------------------------------------|
|  4  | Change EPAP B HTTP SuExec Port       |
|-----|--------------------------------------|
|  5  | Change EPAP A Banner Connection Port |
|-----|--------------------------------------|
|  6  | Change EPAP B Banner Connection Port |
|-----|--------------------------------------|
|  7  | Change PDBI Port                     |
|-----|--------------------------------------|
|  8  | Change Remote MPS A HTTP Port        |
|-----|--------------------------------------|
|  e  | Exit                                 |
\--------------------------------------------/
Enter choice:
```

24. Enter the appropriate information. Press return once to return to the `Configure Forwarded Ports Menu`.

```
EPAP A HTTP Port [80]:
```

25. Enter the option number or enter `e` to return to the `Configure Network Interfaces Menu`.

NOTE: Unless the MPS is separated from the GUI workstations and provisioning systems by a firewall performing static NAT, the following Steps for configuring static NAT can be skipped. Continue with Step 32.

26. From the `Configure Network Interfaces Menu`, 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       |
|-----|--------------------------------------|
|  7  | Configure Provisioning VIP Addresses |
|-----|--------------------------------------|
|  e  | Exit                                 |
\--------------------------------------------/

Enter choice: 6
```

27. Enter the appropriate option to configure the Static NAT Address. 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.

A Options 1 and 3 are valid.

B Option 2 is valid.

The following table shows an example of a resulting prompt.

```
/-----Configure Static NAT Addresses Menu---\
/-------------------------------------------\
|  1 | Change EPAP A NAT Address             |
|----|---------------------------------------|
|  2 | Change EPAP B NAT Address             |
|----|---------------------------------------|
|  3 | Change Remote MPS A Static NAT Address|
|----|---------------------------------------|
|  e | Exit                                  |
\-------------------------------------------/
```

---

28. Enter a valid NAT IP address from Table 5-1 or Table 5-2.

```
EPAP A Static NAT Address:
```

---

29. Choose option **e** on the `Configure Static NAT Addresses Menu` to return to the Configure Network Interfaces Menu.

NOTE: If no VIP provisioning is desired at this time, the installer should skip this step. Proceed to step 32.

30. Choose option **7**, Configure Provisioning VIP 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       |
|-----|--------------------------------------|
|  7  | Configure Provisioning VIP Addresses |
|-----|--------------------------------------|
|  e  | Exit                                 |
\--------------------------------------------/

Enter choice: 7
```

31. Enter the VIP addresses for the local PDBA and the remote PDBA

```
EPAP local provisioning Virtual IP Address [192.168.66.80]:
EPAP remote provisioning Virtual IP Address [192.168.66.78]:
```

32. Choose option **e**, `Exit` from the `Configure Network Interfaces Menu` to return to the `EPAP 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". If the time zone was correct for this installation, as shown in the output of the Display Configuration (step 6), the installer can skip this menu option 3. Proceed to Step 36.

33. Choose option **3**, Set Time Zone on the `EPAP Configuration Menu`.

```
 /-------EPAP 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        |
|-----|----------------------------------|
|  8  | PDB Configuration Menu           |
|-----|----------------------------------|
|  e  | Exit                             |
\---------------------------------------/

Enter Choice: 3
```

34. 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 EPAP software before
         the MPS servers are rebooted may have unpredictable
          consequences.

Press return to continue...
```

35. 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 EPAP 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 EPAP 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:
```

(This list of valid time zones is also in Appendix A, 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.

36. After setting the time zone successfully, the installer is returned to the `EPAP Configuration Menu`.

37. After setting the time zone successfully, the installer returns to the `EPAP Configuration Menu`.

NOTE: The following option 4, Exchange Secure Shell Keys, is successfully performed automatically by the configuration software at the start of configuration. (The configuration software would not have proceeded to this point if the exchange had not been successful.)
Therefore, the installer may normally skip this step and continue with the next configuration option; proceed to step 43.

38. Choose option **4**, `Exchange Secure Shell Keys`, from the `EPAP Configuration Menu`.

```
 /-------EPAP 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         |
|-----|-----------------------------------|
|  8  | PDB Configuration Menu            |
|-----|-----------------------------------|
|  e  | Exit                              |
\----------------------------------------/

Enter Choice: 4
```

39. The Exchange Secure Shell Keys Menu is output. Select Option **1** to Exchange Keys with the mate.

```
MPS Side A:  hostname: tortola-a  hostid: a8c0883d
             Platform Version: 9.0.2-4.0.0_50.26.0
             Software Version: EPAP .1-4.0.0_50.34.0
             Wed Apr 18 09:51:47 EST 2007

 /-----Exchange Secure Shell Keys Menu-----\
/------------------------------------------\
|  1 | Exchange Keys with Mate              |
|----|--------------------------------------|
|  2 | Exchange Keys with Remote            |
|----|--------------------------------------|
|  3 | Exchange Keys with Mate as Root User |
|----|--------------------------------------|
|  e | Exit                                 |
\------------------------------------------/

Enter Choice: 1
```

---

40. The following is output.

```
Are you sure you wish to exchange keys? [N]: y
```

---

41. 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...
```

---

42. 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 Customer Care Services for the password; refer to “Customer Assistance” on page 1-4.)

After entering the appropriate password, a verification of the exchange is displayed. The installer is returned to the `EPAP Configuration Menu`.

```
Are you sure you wish to exchange keys with the mate? [N]: y
Password for EPAPdev@mate:
Keys exchanged.
Verifying that ssh works correctly.

ssh is working correctly.
```

NOTE: If required by the customer to change the text-based UI password for the MPSs at this site, the installer selects option `5`, Change Password. Otherwise, this step can be skipped, and the installer can proceed to step 46.

43. Enter option **`5`,** Change Password, from the `EPAP Configuration Menu` to change the text-based user interface password for the **`epapconfig`** login name for both MPS A and B at this site.

```
 /-------EPAP 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         |
|-----|-----------------------------------|
|  8  | PDB Configuration Menu            |
|-----|-----------------------------------|
|  e  | Exit                              |
\----------------------------------------/

Enter Choice: 5
```

44. The installer is prompted to confirm the action of changing the password for both the MPS A and MSP 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 ...
```

45. Successful entry of the new password returns the installer to the `EPAP Configuration Menu`.

NOTE: If an NTP server does not need to be added at this time, the installer can skip all steps related to option 7 Configure NTP Server Menu, and proceed to step 53.

46. Enter option **7**, Configure NTP Server Menu, from the `EPAP Configuration Menu` to add an NTP Server.

```
 /-------EPAP 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         |
|-----|-----------------------------------|
|  8  | PDB Configuration Menu            |
|-----|-----------------------------------|
|  e  | Exit                              |
\----------------------------------------/

Enter Choice: 7
```

47. Choose option **2**, `Add External NTP Server` from the `EPAP Configure NTP Server Menu`.

```
 /-----EPAP Configure NTP Server Menu-\
/--------------------------------------\
|  1  | Display External NTP Server     |
|-----|---------------------------------|
|  2  | Add External NTP Server         |
|-----|---------------------------------|
|  3  | Remove External NTP Server      |
|-----|---------------------------------|
|  e  | Exit                            |
\--------------------------------------/

Enter Choice: 2
```

48. 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.

Ⓑ **MPS on EAGLE 5 SAS B:**

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.

Non-Provisionable MPS:

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 EPAP NTP Server IP Address: 192.168.61.69

Verifying NTP Server. It might take up to 1 minute.

External NTP Server [192.168.61.69]
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 `EPAP Configure NTP Server Menu`.

49. Enter option **1**, Display External NTP Server from the `EPAP Configure NTP Server Menu`, to confirm successful addition of the NTP server

```
 /-----EPAP Configure NTP Server Menu-\
/--------------------------------------\
|  1  | Display External NTP Server     |
|-----|---------------------------------|
|  2  | Add External NTP Server         |
|-----|---------------------------------|
|  3  | Remove External NTP Server      |
|-----|---------------------------------|
|  e  | Exit                            |
\--------------------------------------/

Enter Choice: 1
```

50. The following output is displayed. Verify that the External NTP Server IP address is correct.

```
ntpserver1 192.168.61.157

Press return to continue...
```

51. Press the Return key to return to the `EPAP Configure NTP Server Menu`.

52. Enter option **e** to exit the EPAP Configure NTP Server Menu and return to the EPAP Configuration Menu.

```
 /-----EPAP Configure NTP Server Menu-\
/--------------------------------------\
|  1  | Display External NTP Server     |
|-----|---------------------------------|
|  2  | Add External NTP Server         |
|-----|---------------------------------|
|  3  | Remove External NTP Server      |
|-----|---------------------------------|
|  e  | Exit                            |
\--------------------------------------/

Enter Choice: e
```

53. Enter option **8**, PDB Configuration Menu, from the EPAP Configuration Menu, to configure the PDB network

```
 /-------EPAP 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         |
|-----|-----------------------------------|
|  8  | PDB Configuration Menu            |
|-----|-----------------------------------|
|  e  | Exit                              |
\----------------------------------------/

Enter Choice: 8
```

54. Enter option **1**, Configure PDB Network, from the Configure PDB Menu.

```
 /-----Configure PDB Menu------------\
/-------------------------------------\
|  1  | Configure PDB Network          |
|-----|--------------------------------|
|  2  | RTDB Homing Menu               |
|-----|--------------------------------|
|  3  | Change MPS Provisionable State |
|-----|--------------------------------|
|  4  | Create PDB                     |
|-----|--------------------------------|
|  5  | Change Auto DB Recovery State  |
|-----|--------------------------------|
|  6  | Change PDBA Proxy State        |
|-----|--------------------------------|
|  e  | Exit                           |
\-------------------------------------/

Enter Choice: 1
```

55. Refer to Table 5-1through Table 5-4 for the required information:

- For provisionable MPSs, perform step 56, skip step 57, and resume with step 58.
- For non-provisionable MPSs, skip step 56, and resume with step 57 and 58.

56. Only for provisionable MPSs (MPS of EAGLE 5 ISS A or MPS of EAGLE 5 ISS B):

MPS on EAGLE 5 SAS A:
The installer must have the IP address for the MPS A of EAGLE 5 ISS B (recorded in Table 5-2 on page 5-12).

MPS on EAGLE 5 SAS B:
The installer must have the IP address for the MPS A of EAGLE 5 ISS A (recorded in Table 5-1 on page 5-11).

Option **1** requires the installer to provide the IP address of the MPS A on EAGLE 5 ISS A and requires the installer to provide the IP address for the MPS A on EAGLE 5 ISS B where the remote PDBA database is to reside. (See the following NOTE about the use of 'local' and 'remote'.) The installer must then enter the password for MPS A on EAGLE 5 ISS B. If configuration of the PDB network is successful, the output confirms the secure shell keys are successfully exchanged, as shown in the output for provisionable MPSs. If configuring the PDBA Proxy feature, the IP address for MPS B (mate non-provisionable MPS) on EAGLE 5 ISS B is required.

NOTE: Remember that references to 'local' and 'remote' by the software configuration are relative to the MPS on which the configuration software is executing at that time.

```
This MPS is configured to be provisionable.  The EPAP local PDBA
address is 192.168.61.84.

EPAP software and PDBA are running. Stop Them? [N] y

Enter the EPAP remote PDBA address: 192.168.61.86

Password for epapdev@192.168.61.119:
Keys exchanged.
Verifying that ssh works correctly.

ssh is working correctly.

Press return to continue...
```

The installer is then returned to the `Configure PDB Menu`.

The installer of a provisionable MPS now should proceed to step 58.

57. Only for non-provisionable MPSs:

Non-Provisionable MPS:

The installer must have the IP addresses for the MPS A of EAGLE 5 ISS A and
MPS A of EAGLE 5 ISS B (recorded in Table 5-1 and Table 5-2 on page 5-12).

Option **1** requires the installer to provide the IP addresses for the MPS A on EAGLE 5 ISS A and the MPS A on EAGLE 5 ISS B, as shown in the output for non-provisionable MPSs.

```
This MPS is configured to be non-provisionable. You will be prompted
for both of the remote PDB addresses.  Order does not matter.

EPAP software and PDBA are running. Stop Them? [N] y

Enter one of the two PDBA addresses: 192.168.61.84
Enter the other of the two PDBA address: 192.168.61.86

Press return to continue...
```

The installer is then returned to the `Configure PDB Menu`.

The installer of all MPSs should continue with the next step.

Resuming for all MPSs)

NOTE: The default homing policy for a pair of provisionable MPSs is specific homing to the local PDB. Unless the customer has specifically requested active/standby homing, the installer can skip this step and proceed with Step 66.

58. Enter option **2**, `RTDB Homing Menu` from the `Configure PDB Menu` to configure the homing policy.

```
 /-----Configure PDB Menu-----------\
/-------------------------------------\
|  1  | Configure PDB Network         |
|-----|-------------------------------|
|  2  | RTDB Homing Menu              |
|-----|-------------------------------|
|  3  | Change MPS Provisionable State|
|-----|-------------------------------|
|  4  | Create PDB                    |
|-----|-------------------------------|
|  5  | Change Auto DB Recovery State |
|-----|-------------------------------|
|  6  | Change PDBA Proxy State       |
|-----|-------------------------------|
|  e  | Exit                          |
\-------------------------------------/

Enter Choice: 2
```

---

59. Enter option 1, 2, or 3 from the RTDB Homing Menu. the installer can specify 'specific' homing, 'active' homing, or 'standby' homing for this MPS. (For more information about the homing feature, refer to "Selective Homing of EPAP RTDBs" on page 2-19.)

```
 /-------RTDB Homing Menu------------\
/-------------------------------------\
|  1  | Configure Specific RTDB Homing |
|-----|--------------------------------|
|  2  | Configure Active RTDB Homing   |
|-----|--------------------------------|
|  3  | Configure Standby RTDB Homing  |
|-----|--------------------------------|
|  e  | Exit                           |
\-------------------------------------/

Enter Choice: (1, 2, or 3)
```

60. After choosing, continue using the following information:

- Option 1 for specific homing: the installer must choose one of the two IP addresses on the list, as shown in this output:

```
EPAP software and PDBA are running. Stop Them? [N] y

There are two configured PDBs for this MPS:
1. 192.168.61.84 (local)
2. 192.168.61.86

Select the preferred PDB from which to receive updates [1]: 1

The RTDB Homing policy is set to 'specific' and will prefer updates
from 192.168.61.84.
```

- Option 2 for active homing: the installer decides whether to allow updates from the standby PDB. If updates from the nearby PDB are not allowed, the choice must be confirmed, as shown in this output:

```
EPAP software and PDBA are running. Stop Them? [N] y

In the event that the active PDB is unavailable, should updates be
allowed to the RTDBs from the standby MPS? [Y]: N

Caution: If this option is selected, the standby PDB will not
provision the RTDBs at this site in the event that the active PDB is
not available.

Are you sure you want to disallow updates to the RTDBs from the
standby PDB? Y

The RTDB Homing policy is set to 'active' and will not allow updates
from the standby PDB.
```

- Option 3 for standby homing: the installer decides whether to allow updates from the active PDB. If updates from the active PDB are not allowed, the choice must be confirmed, as shown in this output:

```
EPAP software and PDBA are running. Stop Them? [N] y

In the event that the standby PDB is unavailable, should updates be
allowed to the RTDBs from the active MPS? [Y]: N

Caution: If this option is selected, the active PDB will not provision
the RTDBs at this site in the event that the standby PDB is not
available.

Are you sure you want to disallow updates to the RTDBs from the active
PDB? Y

The RTDB Homing policy is set to 'standby' and will not allow updates
from the active PDB.
```

The installer is then returned to the RTDB Homing Menu.

61. Enter option **e** to exit the `RTDB Homing Menu` to the `Configure PDB Menu`.

```
 /-------RTDB Homing Menu------------\
/-------------------------------------\
|  1  | Configure Specific RTDB Homing |
|-----|--------------------------------|
|  2  | Configure Active RTDB Homing   |
|-----|--------------------------------|
|  3  | Configure Standby RTDB Homing  |
|-----|--------------------------------|
|  e  | Exit                           |
\-------------------------------------/

Enter Choice: e
```

62. Enter option **5**, `Change Auto DB Recovery` from the `Configure PDB Menu` to enable the Automated Database Recovery feature. Steps **62** and **63** must be performed on both provisionable MPS A of a mated pair.

```
 /-----Configure PDB Menu------------\
/-------------------------------------\
|  1  | Configure PDB Network          |
|-----|--------------------------------|
|  2  | RTDB Homing Menu               |
|-----|--------------------------------|
|  3  | Change MPS Provisionable State |
|-----|--------------------------------|
|  4  | Create PDB                     |
|-----|--------------------------------|
|  5  | Change Auto DB Recovery State  |
|-----|--------------------------------|
|  6  | Change PDBA Proxy State        |
|-----|--------------------------------|
|  e  | Exit                           |
\-------------------------------------/

Enter Choice: 5
```

63. The following output is displayed.

```
Auto DB Recovery is currently DISABLED.
Do you want to ENABLE Auto DB Recovery? [N]: y
```

64. Steps **64** and **65** must be performed on both provisionable MPS A of a mated pair if this feature is utilized. Enter option **6**, `Change PDBA Proxy State` from the `Configure PDB Menu` to enable the PDBA Proxy feature.

```
 /-----Configure PDB Menu------------\
/-------------------------------------\
|  1  | Configure PDB Network          |
|-----|--------------------------------|
|  2  | RTDB Homing Menu               |
|-----|--------------------------------|
|  3  | Change MPS Provisionable State |
|-----|--------------------------------|
|  4  | Create PDB                     |
|-----|--------------------------------|
|  5  | Change Auto DB Recovery State  |
|-----|--------------------------------|
|  6  | Change PDBA Proxy State        |
|-----|--------------------------------|
|  e  | Exit                           |
\-------------------------------------/

Enter Choice: 6
```

65. The following output is displayed.

```
PDBA PROXY is currently DISABLED.
Do you want to ENABLE PDBA Proxy? [N]: y
```

NOTE: The next action to be taken depends on what stage of the configuration procedure the installer is performing, specifically, which MPS is being configured. Follow the steps appropriate to the configuration currently being performed for the MPSs on EAGLE 5 ISS A, MPSs on EAGLE 5 ISS B, or any non-provisionable MPS pairs.

MPS on EAGLE 5 SAS A:
The installer proceeds to step 66 and continues there.

Non-Provisionable MPS:
The installer proceeds to step 69 and continues there.

MPS on EAGLE 5 SAS B:
The installer proceeds directly to step 72 and continues there.

MPS on EAGLE 5 SAS A:

Steps 66 through 68 are to be performed for only MPS A and B on EAGLE 5 ISS A.

66. Enter option **e** to exit the `Configure PDB Menu` and return to the `EPAP Configuration Menu`.

```
 /-----Configure PDB Menu------------\
/-------------------------------------\
|  1  | Configure PDB Network          |
|-----|--------------------------------|
|  2  | RTDB Homing Menu               |
|-----|--------------------------------|
|  3  | Change MPS Provisionable State |
|-----|--------------------------------|
|  4  | Create PDB                     |
|-----|--------------------------------|
|  5  | Change Auto DB Recovery State  |
|-----|--------------------------------|
|  6  | Change PDBA Proxy State        |
|-----|--------------------------------|
|  e  | Exit                           |
\-------------------------------------/

Enter Choice: e
```

67. Enter option **e** to exit the `EPAP Configuration Menu`.

```
 /-------EPAP 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         |
|-----|-----------------------------------|
|  8  | PDB Configuration Menu            |
|-----|-----------------------------------|
|  e  | Exit                              |
\----------------------------------------/

Enter Choice: e
```

68. Enter **y** in response to the cautionary message stating that the current MPS is not completely configured. This is correct procedure at this time. .

```
PDB not created

Caution: This MPS has not been completely configured.  Applications may not
         run until all required parameters are entered through the text
         user interface.  Choose "Display Configuration" for a list of
         configurable parameters and their settings.

Press return to continue...
```

MPS on EAGLE 5 SAS A:

The configuration of the MPSs on EAGLE 5 ISS A is not completed until its PDB is created. The creation of the MPSs on the EAGLE 5 ISS A PDB will be done during the initial configuration of the MPS A on EAGLE 5 ISS B, which procedure automatically replicates the PDB on the MPS on EAGLE 5 ISS A at the same time.

The installer has completed the initial configuration of MPSs on EAGLE 5 ISS A, and can now begin the configuration of the MPSs on EAGLE 5 ISS B.

NOTE: Do not attempt to reboot the MPSs on EAGLE 5 ISS A now. Rebooting the MPSs at EAGLE 5 ISS A and EAGLE 5 ISS B will be performed concurrently when the configuration of the MPSs at EAGLE 5 ISS B is completed.

Non-Provisionable MPS:

Steps 69 through 70 are to be performed only for a non-provisionable MPS.

69. Enter option **e** to exit the `Configure PDB Menu` and return to the `EPAP Configuration Menu`.

```
 /-----Configure PDB Menu------------\
/-------------------------------------\
|  1  | Configure PDB Network          |
|-----|--------------------------------|
|  2  | RTDB Homing Menu               |
|-----|--------------------------------|
|  3  | Change MPS Provisionable State |
|-----|--------------------------------|
|  4  | Create PDB                     |
|-----|--------------------------------|
|  5  | Change Auto DB Recovery State  |
|-----|--------------------------------|
|  6  | Change PDBA Proxy State        |
|-----|--------------------------------|
|  e  | Exit                           |
\-------------------------------------/

Enter Choice: e
```

70. Enter option **6**, `Platform Menu` from the `EPAP Configuration Menu`.

```
 /-------EPAP 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         |
|-----|-----------------------------------|
|  8  | PDB Configuration Menu            |
|-----|-----------------------------------|
|  e  | Exit                              |
\----------------------------------------/

Enter Choice: 6
```

71. Continue with **Step 75.**

MPS on EAGLE 5 SAS B:

The following steps 72 and 73 are to be performed only for MPS A and B on EAGLE 5 ISS B.

72. Enter option **4**, `Create PDB` from the `Configure PDB Menu`.

```
 /-----Configure PDB Menu-----------\
/-----------------------------------\
|  1  | Configure PDB Network       |
|-----|-----------------------------|
|  2  | RTDB Homing Menu            |
|-----|-----------------------------|
|  3  | Change MPS Provisionable State |
|-----|-----------------------------|
|  4  | Create PDB                  |
|-----|-----------------------------|
|  5  | Change Auto DB Recovery State |
|-----|-----------------------------|
|  6  | Change PDBA Proxy State     |
|-----|-----------------------------|
|  e  | Exit                        |
\-----------------------------------/

Enter Choice: 4
```

73. The PDB is now created on the present EPAP, and is automatically replicated on the former EPAP as well.

After the output indicating successful creation of the PDBs, the installer is returned to the `EPAP Configuration Menu`.

NOTE: During configuration of MPSs on EAGLE 5 ISS B, if the time zone was not changed (step 33) and if the Backup Provisioning Network (step 19) was not configured on either MPS, the EPAP initial configuration of MPSs on EAGLE 5 ISS B is now complete.

Otherwise the installer must continue with this step because both MPS pairs on EAGLE 5 ISS A and on EAGLE 5 ISS B must now be rebooted.

74. Enter option **6**, `Platform Menu`, from the `EPAP Configuration Menu`.

```
 /-------EPAP 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        |
|-----|----------------------------------|
|  8  | PDB Configuration Menu           |
|-----|----------------------------------|
|  e  | Exit                             |
\---------------------------------------/

Enter Choice: 6
```

75. Enter option **3**, `Reboot MPS` from the `EPAP Platform Menu`, to reboot the MPS.

```
 /-----EPAP Platform Menu-\
/-------------------------\
|  1  | Initiate Upgrade  |
|-----|-------------------|
|  2  | Eject CD          |
|-----|-------------------|
|  3  | Reboot MPS        |
|-----|-------------------|
|  4  | Halt MPS          |
|-----|-------------------|
|  5  | File System Backup|
|-----|-------------------|
|  6  | MySQL Backup      |
|-----|-------------------|
|  7  | RTDB Backup       |
|-----|-------------------|
|  8  | PDB Backup        |
|-----|-------------------|
|  e  | Exit              |
\-------------------------/

Enter Choice: 3
```

76. Enter **BOTH** (the default value) when prompted on whether MPS A, MPS B or BOTH sides are to be rebooted.

```
Reboot MPS A, MPS B or [BOTH]:
```

The reboot of both MPS A and MPS B begins when the Return key is pressed.

77. 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.

78. When a **ssh** session is closed, the installer is returned to the previous ssh session. In this case, the installer is now back at the system prompt of MPS A of EAGLE 5 ISS A. The installer must now log in as **epapconfig** to invoke the EPAP Configuration. Type the following command and the password.

```
$su epapconfig

Password:
```

79. Enter option **6**, `Platform Menu`, from the `EPAP Configuration Menu`.

```
 /-------EPAP 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         |
|-----|-----------------------------------|
|  8  | PDB Configuration Menu            |
|-----|-----------------------------------|
|  e  | Exit                              |
\----------------------------------------/

Enter Choice: 6
```

80. Enter option **3**, `Reboot MPS` from the `EPAP Platform Menu`.

```
 /-----EPAP Platform Menu-\
/--------------------------\
|  1  | Initiate Upgrade   |
|-----|--------------------|
|  2  | Eject CD           |
|-----|--------------------|
|  3  | Reboot MPS         |
|-----|--------------------|
|  4  | Halt MPS           |
|-----|--------------------|
|  5  | File System Backup |
|-----|--------------------|
|  6  | MySQL Backup       |
|-----|--------------------|
|  7  | RTDB Backup        |
|-----|--------------------|
|  8  | PDB Backup         |
|-----|--------------------|
|  e  | Exit               |
\--------------------------/

Enter Choice: 3
```

81. Enter **BOTH** (the default value) when prompted on whether MPS A, MPS B or BOTH sides are to be rebooted.

```
Reboot MPS A, MPS B or [BOTH]:
```

The reboot of both MPS A and MPS B begins when the Return key is pressed.

82. The console logon appears at the system prompt signifying the EPAP initial configuration is complete.

NOTE: The console logon will be preceded by many lines of reboot output.

MPS on EAGLE 5 SAS B:

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.

The installer should now configure the non-provisionable MPSs, if appropriate, for the system being configured.

Non-Provisionable MPS:

The initial configuration of the non-provisionable MPSs is now complete.

The non-provisionable MPS A and B for the current site being configured are now configured and rebooted. Repeat this procedure, if necessary, until all remaining non-provisionable MPSs are configured.

A

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 EPAP software configuration. The initial default value for the time zone is “US/Eastern”.

The Select Time Zone menu (refer to “Set Time Zone” on page 5-25) prompts you for the time zone to be used by the EPAP. The time zone can be the zone where the EPAP is located, Greenwich Mean Time, or another zone that is selected by the customer to meet the needs of the system.

The following text appears when you install the EPAP with the EPAP Configuration Menu.

```
Enter a time zone file (relative to /usr/share/lib/zoneinfo):

Valid time zone files are:
Australia/Broken_Hill     Australia/LHI             Australia/NSW
Australia/North           Australia/Queensland      Australia/South
Australia/Tasmania        Australia/Victoria        Australia/West
Australia/Yancowinna      Australia/ACT             Brazil/Acre
Brazil/DeNoronha          Brazil/East               Brazil/West
Canada/Atlantic           Canada/Central            Canada/East-Saskatchewan
Canada/Eastern            Canada/Mountain           Canada/Newfoundland
Canada/Pacific            Canada/Yukon              Chile/Continental
Chile/EasterIsland        Etc/GMT                   Etc/GMT+1
Etc/GMT+10                Etc/GMT+11                Etc/GMT+12
Etc/GMT+2                 Etc/GMT+3                 Etc/GMT+4
Etc/GMT+5                 Etc/GMT+6                 Etc/GMT+7
Etc/GMT+8                 Etc/GMT+9                 Etc/GMT-1
Etc/GMT-10                Etc/GMT-11                Etc/GMT-12
Etc/GMT-13                Etc/GMT-2                 Etc/GMT-3
Etc/GMT-4                 Etc/GMT-5                 Etc/GMT-6
Etc/GMT-7                 Etc/GMT-8                 Etc/GMT-9
Etc/GMT+0                 Etc/GMT-0                 Mexico/BajaNorte
Mexico/BajaSur            Mexico/General            Mideast/Riyadh87
Mideast/Riyadh88          Mideast/Riyadh89          US/Alaska
US/Aleutian               US/Michigan               US/Pacific-New
US/Samoa                  US/Arizona                US/Central
US/East-Indiana           US/Eastern                US/Hawaii
```

```
US/Mountain             US/Pacific              CET
CST6CDT                 Cuba                    EET
EST                     EST5EDT                 Egypt
Eire                    Factory                 GB
HST                     Hongkong                Iceland
Iran                    Israel                  Japan
Kwajalein               Libya                   MET
MST                     MST7MDT                 NZ
NZ-CHAT                 PRC                     PST8PDT
Poland                  Portugal                ROC
ROK                     Singapore               Turkey
W-SU                    WET                     africa
asia                    australasia             backward
etcetera                europe                  factory
northamerica            pacificnew              solar87
solar88                 solar89                 southamerica
GB-Eire                 GMT                     GMT+0
GMT+1                   GMT+10                  GMT+11
GMT+12                  GMT+13                  GMT+2
GMT+3                   GMT+4                   GMT+5
GMT+6                   GMT+7                   GMT+8
GMT+9                   GMT-0                   GMT-1
GMT-10                  GMT-11                  GMT-12
GMT-2                   GMT-3                   GMT-4
GMT-5                   GMT-6                   GMT-7
GMT-8                   GMT-9                   Greenwich
Jamaica                 Navajo                  UCT
UTC                     Universal               Zulu

Enter a time zone file (relative to /usr/share/lib/zoneinfo):
```

The time zone change does not take effect until the next time the MPS is rebooted. The Reboot MPS menu is described in “Reboot the MPS” on page 3-62.

Index

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W