Tekelec EAGLE® 5

EPAP Administration Manual

910-6021-001 Revision A
March 2011

Copyright 2011 Tekelec. All Rights Reserved. Printed in USA.
Legal Information can be accessed from the Main Menu of the optical disc or on the
Tekelec Customer Support web site in the *Legal Information* folder of the *Product Support* tab.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

Topics:

This chapter provides a brief description of the EAGLE Provisioning Application Processor (EPAP). The chapter also includes the scope, audience, and organization of the manual; how to find related publications; and how to contact Tekelec for assistance.

Overview

This manual describes the administration of the EAGLE Provisioning Application Processor (EPAP) and the EPAP user interface menus used to perform configuration, maintenance, debug, and platform operations.

The EPAP program runs on the Multi Purpose Server (MPS), which is a hardware platform that supports high speed provisioning of large databases for the Tekelec EAGLE 5 Integrated Signaling System. EPAP supports the EPAP-related features. See the Glossary for a list of EPAP-related features.

Scope and Audience

This manual is intended for anyone performing EPAP administration or using the EPAP user interface. 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 five chapters and one appendix:

- *Introduction* includes an overview of the EAGLE Provisioning Application Processor (EPAP), the organization of this manual, documentation information, and how to request technical assistance.
- *Functional Description* provides a description of the EPAP design, features, and user interfaces.
- *EPAP Graphical User Interface* describes the EPAP Graphical User Interface and the EPAP user interface menus.
- *Messages, Alarms, and Status Processing* describes EPAP error messages, alarms, hardware verification, and status reporting.
- *EPAP Software Configuration* provides the EPAP configuration and initialization procedures using the text-based user interface.
- *Time Zone File Names* is an appendix that provides a listing of valid time zone file names.

Documentation Admonishments

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

Table 1: Admonishments

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

Customer Care Center

The Tekelec Customer Care Center is your initial point of contact for all product support needs. A representative takes your call or email, creates a Customer Service Request (CSR) and directs your requests to the Tekelec Technical Assistance Center (TAC). Each CSR includes an individual tracking number. Together with TAC Engineers, the representative will help you resolve your request.

The Customer Care Center is available 24 hours a day, 7 days a week, 365 days a year, and is linked to TAC Engineers around the globe.

Tekelec TAC Engineers are available to provide solutions to your technical questions and issues 7 days a week, 24 hours a day. After a CSR is issued, the TAC Engineer determines the classification of the trouble. If a critical problem exists, emergency procedures are initiated. If the problem is not critical, normal support procedures apply. A primary Technical Engineer is assigned to work on the CSR and provide a solution to the problem. The CSR is closed when the problem is resolved.

Tekelec Technical Assistance Centers are located around the globe in the following locations:

Tekelec - Global

Email (All Regions): support@tekelec.com

- **USA and Canada**

  Phone:

  1-888-FOR-TKLC or 1-888-367-8552 (toll-free, within continental USA and Canada)

  1-919-460-2150 (outside continental USA and Canada)

  TAC Regional Support Office Hours:

  8:00 a.m. through 5:00 p.m. (GMT minus 5 hours), Monday through Friday, excluding holidays

- **Central and Latin America (CALA)**

  Phone:

  USA access code +1-800-658-5454, then 1-888-FOR-TKLC or 1-888-367-8552 (toll-free)

TAC Regional Support Office Hours (except Brazil):

10:00 a.m. through 7:00 p.m. (GMT minus 6 hours), Monday through Friday, excluding holidays

- **Argentina**

  Phone:

  0-800-555-5246 (toll-free)

- **Brazil**

  Phone:

  0-800-891-4341 (toll-free)

  TAC Regional Support Office Hours:

  8:30 a.m. through 6:30 p.m. (GMT minus 3 hours), Monday through Friday, excluding holidays

- **Chile**

  Phone:

  1230-020-555-5468

- **Colombia**

  Phone:

  01-800-912-0537

- **Dominican Republic**

  Phone:

  1-888-367-8552

- **Mexico**

  Phone:

  001-888-367-8552

- **Peru**

  Phone:

  0800-53-087

- **Puerto Rico**

  Phone:

  1-888-367-8552 (1-888-FOR-TKLC)

- **Venezuela**

  Phone:

  0800-176-6497

- **Europe, Middle East, and Africa**

  Regional Office Hours:

  8:30 a.m. through 5:00 p.m. (GMT), Monday through Friday, excluding holidays

  - **Signaling**

Phone:

+44 1784 467 804 (within UK)

- **Software Solutions**

  Phone:

  +33 3 89 33 54 00

- **Asia**
  - **India**

    Phone:

    +91 124 436 8552 or +91 124 436 8553

    TAC Regional Support Office Hours:

    10:00 a.m. through 7:00 p.m. (GMT plus 5 1/2 hours), Monday through Saturday, excluding holidays
  - **Singapore**

    Phone:

    +65 6796 2288

    TAC Regional Support Office Hours:

    9:00 a.m. through 6:00 p.m. (GMT plus 8 hours), Monday through Friday, excluding holidays

Emergency Response

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

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

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

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

Related Publications

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

Documentation Availability, Packaging, and Updates

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

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

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

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

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

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

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

Locate Product Documentation on the Customer Support Site

Access to Tekelec's Customer Support site is restricted to current Tekelec customers only. This section describes how to log into the Tekelec Customer Support site and locate a document. Viewing the document requires Adobe Acrobat Reader, which can be downloaded at www.adobe.com.

1. Log into the *Tekelec Customer Support* site.

Note: If you have not registered for this new site, click the **Register Here** link. Have your customer number available. The response time for registration requests is 24 to 48 hours.

2. Click the **Product Support** tab.
3. Use the Search field to locate a document by its part number, release number, document name, or document type. The Search field accepts both full and partial entries.
4. Click a subject folder to browse through a list of related files.
5. To download a file to your location, right-click the file name and select **Save Target As**.

Chapter 2

Functional Description

Topics:

This chapter provides a description of the EAGLE Provisioning Application Processor (EPAP) design, features, and user interfaces.

General Description

The EAGLE Provisioning Application Processor () platform, coupled with the Provisioning Database Application (PDBA), facilitates and maintains the database required by EPAP-related features. See the Glossary for a list of EPAP-related features. The EPAP serves two major purposes:

- Accept and store data provisioned by the customer
- Update customer provisioning data and reload databases on the Service Module cards in the Multi Purpose Server (MPS)

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).

During normal operation, information flows through the EPAP and 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. *EPAP Graphical User Interface* describes the EPAP and PDBA user interfaces. *EPAP Software Configuration* includes descriptions of the text-based user interface that performs initial EPAP configuration.

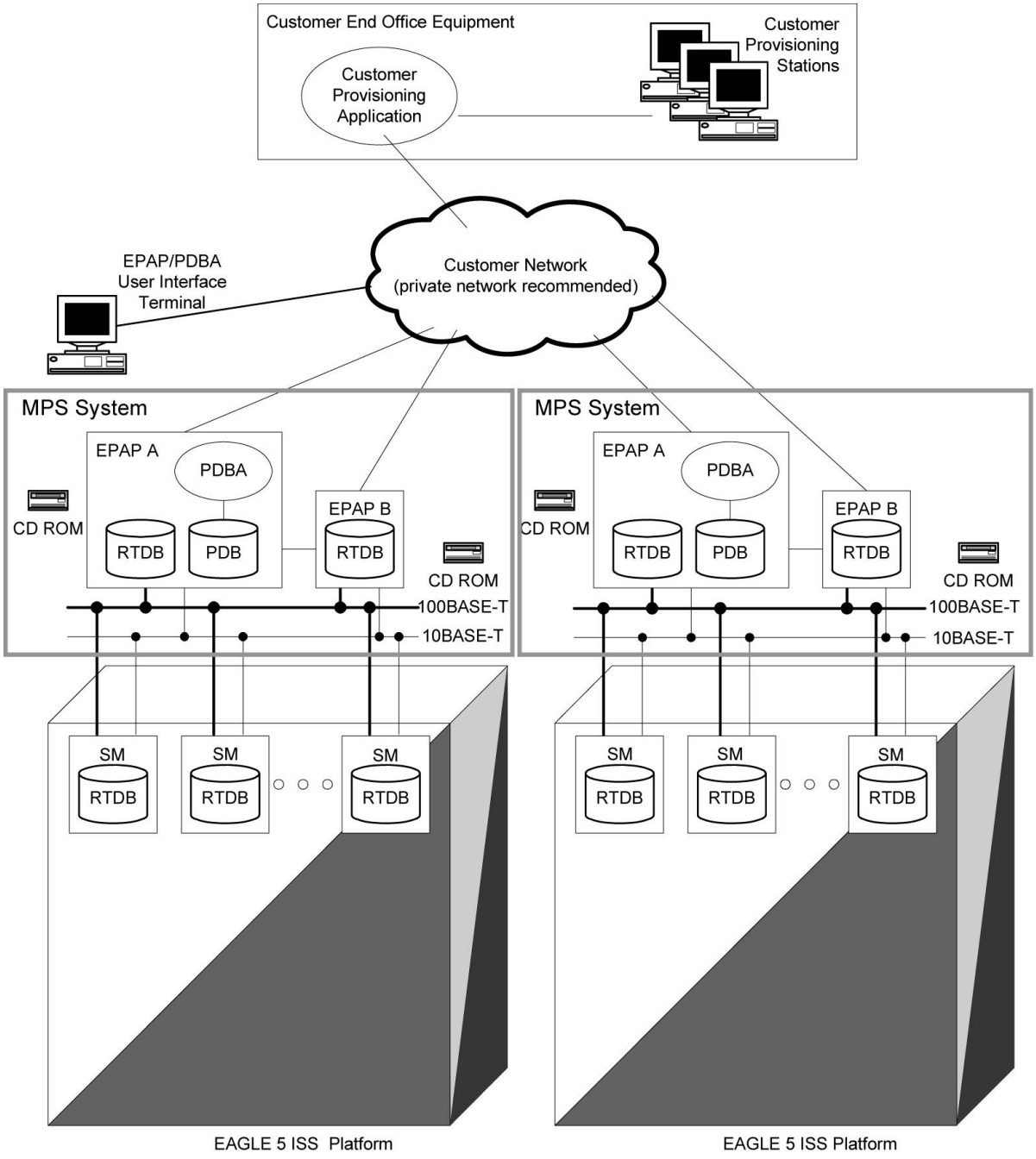

Figure 1: Mated EAGLE 5 ISS Platform Example

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 Service Module cards is part of the EAGLE 5 ISS. Each Service Module card stores a copy of the Real Time Database (RTDB),

The main and backup DSM networks are two high-speed Ethernet links, which connect the Service Module cards and the EPAPs. Another Ethernet link connects the two EPAPs and is identified as the EPAP Sync network.

Figure 2: Example EPAP Network IP Addresses shows the network layout and 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 Service Module 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 Service Module card database is provisioned through the main DSM network by the Active EPAP.

If the Active EPAP fails, the Standby EPAP takes over the role of Active EPAP and continues to provision the database. If the main DSM network fails completely and connectivity is lost for all EAGLE Service Modules cards, the Active EPAP switches to the backup DSM network to continue provisioning the Service Module cards. Any failure which has a limited impact on database provisioning will not automatically trigger a switchover to the backup DSM network. At any given time, only one Active EPAP uses one DSM network per EPAP system.

The Provisioning Multiple EPAPs Support feature provides the capability to connect to a single active provisionable EPAP A that is used to provision up to 22 non-provisionable EPAP systems. For more information about this feature, see *Provisioning Multiple EPAPs Support*.

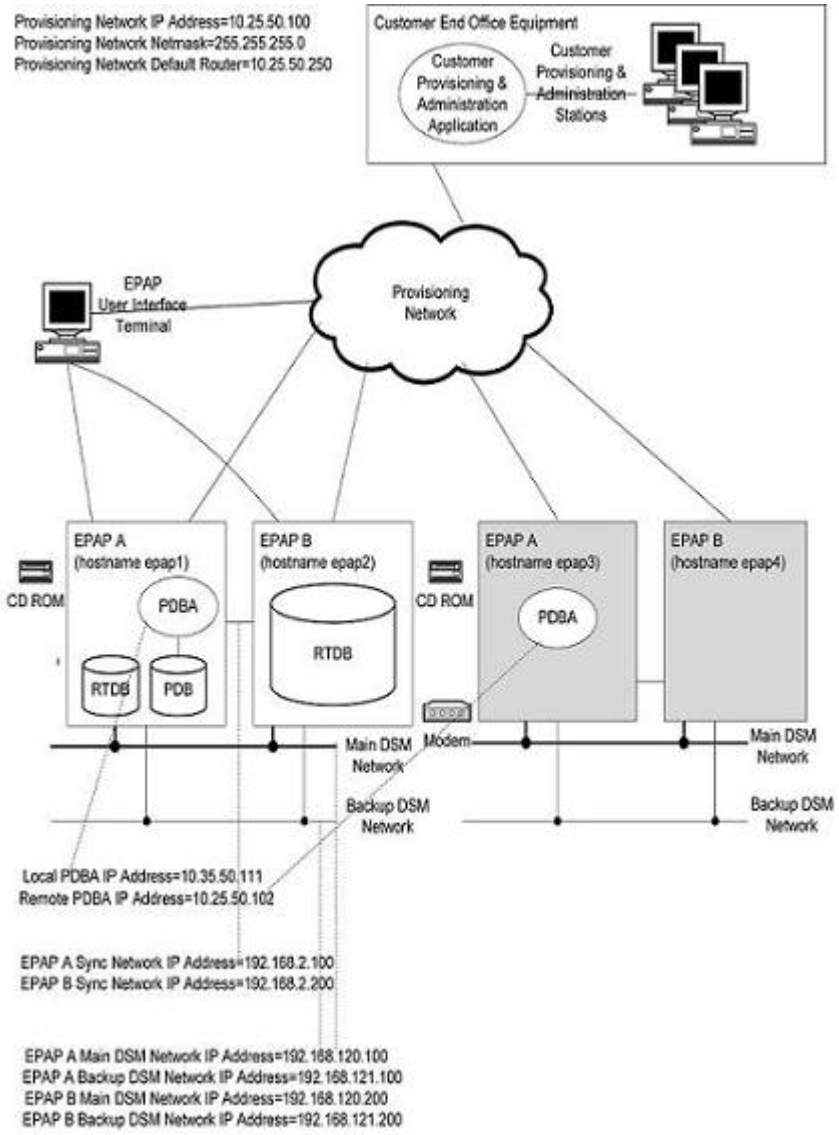

Figure 2: Example EPAP Network IP Addresses

EPAP Switchover

EPAPs assume an Active or a Standby role through negotiation and algorithm. This role affects how 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 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 conditions:

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

The maintenance subsystem has attempted and failed to establish communication with each of these:

- the mate maintenance task across the EPAP Sync network
- the mate maintenance task across the main DSM network
- any Service Module card on any DSM network

2. The RTDB becomes corrupt.
3. All of the RMTP channels have failed.
4. A fatal software error occurred.
5. The 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: EPAP Switchover Matrix* lists the possible combinations.

Table 2: 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* and *Change Status*.

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*.

EPAP Component Overview

The major components that run on the EAGLE Provisioning Application Processor (EPAP) are:

- Provisioning Database Application (PDBA) task
- Provisioning Database (PDB)
- Real Time Database (RTDB) task
- RTDB Audit
- Maintenance task
- DSM provisioning task

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

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

The Service Module card database can go out of sync (become incoherent) due to missed provisioning or card reboot. Out-of-sync Service Module cards are reprovisioned from the RTDB on the Active EPAP. The RTDB audit runs as part of the RTDB task.

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 Service Module card.

The DSM provisioning task resides on both EPAP A and EPAP B. The DSM provisioning task communicates internally with the RTDB task and the EPAP maintenance task. The DSM provisioning task uses Reliable Multicast Transport Protocol (RMTP) to multicast provisioning data to connected Service Module cards across the two DSM networks.

Provisioning Database Interface

Provisioning clients connect to the EPAPs through the Provisioning Database Interface (PDBI). The Provisioning Database Interface (PDBI) provides commands that communicate provisioning information from the customer database to the Provisioning Database (PDB) in the Active PDBA in an EAGLE 5 ISS. The customer issues provisioning commands using a provisioning application. This application uses the PDBI request/response messages to communicate with the EPAP Provisioning Database Application (PDBA) over the customer network.. The PDBI is described in *Provisioning Database Interface Manual*.

When provisioning the EPAP, the supported rate is 50 updates per second.

Network Connections

This section describes the four types of EPAP network connections.

- DSM Networks
- EPAP Sync Network
- Dial-up PPP Network
- Customer Network

DSM Networks

The DSM networks carry provisioning data from the RTDBs on the EPAP to the RTDBs on the Service Module cards. The networks also carry reload and maintenance traffic to the Service Module cards. Each network connects EPAP A and EPAP B to each Service Module card on a single EAGLE 5 ISS platform.

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

The DSM networks operate at different speeds as determined by the installed combinations of Service Module cards.

Network speeds when installed Sevice Module cards are only DSM cards or a mix of DSM and E5-SM4G cards:

- Main DSM network - 100 Mbps, half duplex
- Backup DSM network - 10 Mbps, half duplex

Network speeds when installed Sevice Module cards are all E5-SM4G cards:

- Main DSM network - 100 Mbps, full duplex
- Backup DSM network - 100 Mbps, full duplex

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 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 3: IP Addresses on the DSM Network 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*

Table 3: IP Addresses on the DSM Network

Octet	Derivation
1	192
2	168
3	Usually configured as: 120 for DSM main network 121 for DSM backup network
4	100 for EPAP A 200 for EPAP B 1 - 32 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 operates at full-duplex Gigabit Ethernet speed.

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. This octet value can be changed using the option 2 in *Configure Network Interfaces Menu* .

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

Dial-up PPP Network

The Point-To-Point Protocol (PPP) network, which is not shown in *Figure 2: Example EPAP Network IP Addresses*, allows multiple user interface sessions to be established to the EPAP from a remote workstation.

This network provides support for one modem per MPS server; each modem can be configured for PPP (TCP/IP and UDP/IP). With this capability, multiple networked applications can use the modem link simultaneously. Logging in as the root user is not supported across the modem link directly; however, after a PPP session is established, root logins can be accomplished using 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, or provisioning network, carries the following traffic:

- Customer queries and responses to the PDB (using 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. These 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. These RTDBs would then attempt to communicate with the PDBA on the mate EPAP system.
- PDBA import/export traffic (file transfer)
- Traffic from a PDBA reloading from its mate
- EPAP and PDBA user interface traffic

A dedicated network is recommended, but unrelated customer traffic can also use this network.

Network Time Protocol (NTP)

The Network Time Protocol (NTP) is an Internet protocol that is used to synchronize clocks of computers to Universal Time Coordinated (UTC) as a time reference. NTP reads the clock of a time server and transmits the result to one or more clients. Each client adjusts its own clock as required. NTP ensures 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. Without a synchronization protocol, 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. A free-running system runs on its own clocking source. This allows mated MPS servers to synchronize their clocks

All MPS servers running the EPAP application can 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 servers or NTP servers are defined.

The core MPS platform provides a default NTP configuration file. MPS configuration includes adding `ntppeerA` and `ntppeerB` NTP hostname aliases to the `/etc/hosts` file.

If the network is equipped with firewalls, configure the firewalls to pass NTP protocol on IP port 123 (both TCP and UDP) between the MPS servers and the NTP servers or peers. The ntpdate program uses TCP while the ntpd program 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 *universal* in UTC means that the time can be used anywhere in the world and is independent of time zones. To convert UTC to local time, add or subtract the same number of hours used to convert GMT to local time. The *coordinated* in UTC means that several institutions contribute their estimate of the current time. 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 time-dissemination services, including Global Position System (GPS) and other services operated by various national governments.

Because equipping every computer with a UTC receiver is too costly and inconvenient, a subset of computers can be equipped with receivers to relay the time to a number of clients connected by a common network. Some of these clients can disseminate the time, in which case these clients become lower stratum servers.

Understanding Network Time Protocol

Network Time Protocol (NTP) primary servers provide time to their clients that is accurate within a millisecond on a Local Area Network (LAN) and within a few tens of milliseconds on a Wide Area Network (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:

- 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 can continue up to a stratum-15 server which receives its time from a stratum-14 server.

Client workstations do not usually 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, redundant NTP servers and diverse network paths are required to protect against failing software, hardware, or network links. NTP works in one or more of these association modes:

- Client/server mode - A client receives synchronization from one or more servers, but does not provide synchronization to the servers.
- Symmetric mode - Either of two peer servers can synchronize to the other to provide mutual backup.
- Broadcast mode - Many clients synchronize to a single server or to a few servers. This mode reduces 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 Support of EAGLE ITU Duplicate Point Code feature allows point codes to be provisioned in the PDB using a two-character group code. This feature works 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. The EPAP Support of ITU Duplicate Point Code feature

allows group codes to be entered for Network Entity (SP or RN) point codes using 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.

Note: The EAGLE ITU Duplicate Point Code feature (ITUDUPPC) must be enabled and turned on to use the EPAP Support of ITU Duplicate Point Code feature. For information about enabling or turning on any feature in the EAGLE 5 ISS, refer to the `chg-feat` command in *Commands Manual*.

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 3: Network Example with DPC and Group Codes* shows a network that includes two countries, Country 1 and Country 2. Both countries have SSPs with a point code value of 2047.

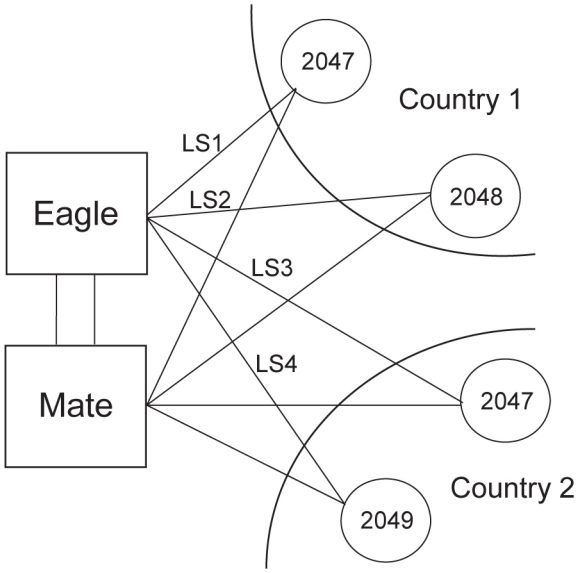

Figure 3: Network Example with DPC and Group Codes

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.

In the network example shown in *Figure 3: Network Example with DPC and Group Codes* , Country 1 can have only one point code with a value of 2047. Traffic coming from SSP 2047 in Country 1 can be destined only to other nodes within Country 1. In this network 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 (SP or RN) point codes via PDBI commands. These commands are described in *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 PDB-based feature databases.

All routing for PDB-based features 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 information about group codes, refer to *Group Codes* in *Database Administration Manual - SS7*.

Asynchronous Replication

Asynchronous replication is the method used to synchronize the various Provisioning Databases (PDBs) in a client network. Asynchronous replication means that the active PDB receives an update, commits to accept the change, and returns a code to the client indicating success or failure. This series of actions occurs before the active PDB forwards the update to the replicated database, which is the standby PDB.

Only successful updates are replicated. As a result, the response turnaround on the active PDB is shortened, and the overhead required to mantain database synchronization is reduced.

Potential Lag Introduced by Asynchronous Replication

Lag means that the database level of the standby PDB is lower than the database level of the active PDB. With any asynchronous data replication scheme, the receivers of replicated data may lag behind. The standby PDB and, depending upon the homing policy in effect, the RTDB applications are susceptible to lag.

During continual provisioning traffic, the active PDB is expected to be a small number of levels ahead of the standby PDB. Also, any RTDB that is homed to the standby PDB is expected to have a level lower than the active PDB. For more information, refer to *Selective Homing of EPAP RTDBs* .

Asynchronous Replication Alarms

If the replication lag between PDB database levels increases to a value deemed unacceptable by EPAP, the following alarms are raised.

- **PDBA Replication Failure** (REPLERR) is a major alarm that indicates a failure of PDBA replication. The user must call the *Customer Care Center*.
- **Standby PDBA Falling Behind** is a minor alarm that signals that one EAGLE 5 ISS of the pair may have received updates at a longer interval than the other EAGLE 5 ISS. This alarm condition does not indicate data loss or corruption.

EPAP Security Enhancements

The EPAP Security Enhancements feature controls access to an EPAP Graphical User Interface (GUI) to specific IP addresses. The specified allowed IP addresses are stored in an EPAP list and can be added to, deleted from, and retrieved only by an authorized user. The EPAP Security Enhancements feature also allows an authorized user to use the GUI to toggle on and off the IP authorization checking.

The administrator or a user with IP action privileges can add, delete, and retrieve IP addresses. Deleting an IP results in that IP address no longer residing in the IP table, hence preventing the IP address from being able to connect to an EPAP. While each of the IP action privileges can be assigned to any individual user, the *add* and *delete* IP action privileges should be granted to only those 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 ability is accessible through the EPAP GUI. Refer to *Authorized IPs* . The IP mechanism implemented in this feature provides the user with enhanced 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.

IP access and range constraints provided by the web server and the EPAP Security Enhancement feature cannot protect against IP spoofing, which refers to the creation of TCP/IP packets using another's IP address. IP spoofing is IP impersonation or misrepresentation. The customer must rely on the security of their intranet network to protect against IP spoofing.

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

IP addresses are not 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.

The EPAP Security Enhancements feature also provides the ability to enable and disable the IP address list after the list is provisioned. If the list is disabled, the provisioned IP addresses are retained in the database, but access is not blocked from the IP addresses that are not on the list. The EPAP GUI restricts permission to enable and disable the IP address list to specific user names and passwords.

The IP actions for adding, deleting, and retrieving authorized IP addresses and for toggling IP authorization checking are available from only the EPAP GUI, as described in *EPAP Graphical User Interface*, and are not available from the EPAP text-based user interface.

For additional security, kernel parameters in the etc/sysctl.conf fileare set to reduce the possibility of against network attacks and security breaches.

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 Provisioning Database Interface (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. After the customer observes the communications failure, the customer performs a manual switch to begin addressing the secondary port defined by the configuration procedure.

The Configure Network Interfaces Menu (see *Configure Network Interfaces Menu*) describes how to configure the primary and secondary provisioning network interface connections. For more information about configuring a Backup Provisioning Network, refer to *Configure 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 MPS contains an EPAP A and an EPAP B). The PDBI connects to and provisions an EPAP A and a Provisioning Database (PDB). The remaining three MPSs are automatically provisioned from the active EPAP A. This allows users to add additional EAGLE 5 ISSs without changing their provisioning systems and without provisioning the EAGLE 5 ISSs from multiple sources.

The Provisioning Multiple EPAPs Support feature is transparent to the PDBI clients. PDBI clients can provision data in the same manner regardless of whether provisioning a single MPS pair or multiple MPS pairs. The PDBI client connects to one PDB for provisioning. The remaining MPSs in the customer network automatically remain synchronized. EPAP software updates the RTDBs at the additional sites.

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.

The two MPSs that contain the PDB are identified as *provisionable* because the customer provisioning application connects to and updates these sites. The remaining MPSs are identified as *non-provisionable*. *Figure 4: Support for Provisioning Multiple EPAPs*shows a view of the provisionable and non-provisionable EPAPs.

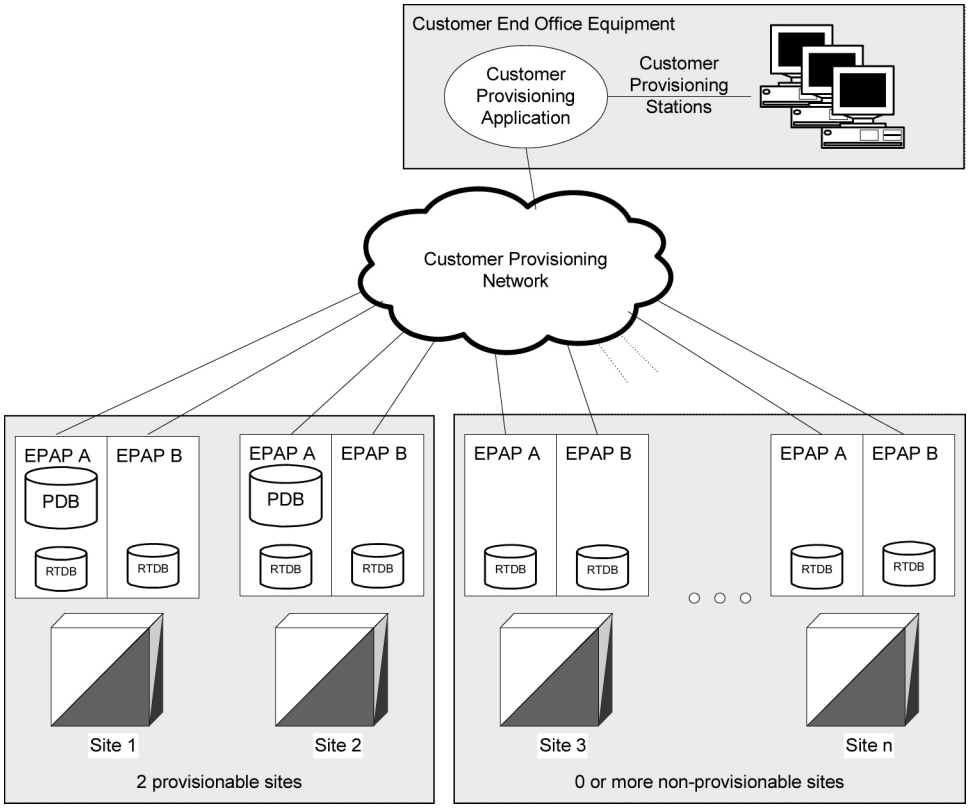

Figure 4: Support for Provisioning Multiple EPAPs

Selective Homing of EPAP RTDBs

The Selective Homing of EPAP RTDBs feature allows users to select the PDB from which updates are received. The homing selection is an option at EPAP configuration. Users can choose whether the RTDBs on an MPS node receive updates by one of the following methods:

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

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

An EPAP configuration option allows the user to select whether the RTDB of an EPAP will normally receive updates. The RTDB is homed to a specific PDBA, the active PDBA , or the standby PDBA. If the user selects specific homing for the RTDB, that RTDB will receive updates from the specified PDBA, regardless of whether the PDBA is active or standby.

If the RTDB cannot communicate with the specified PDBA, the RTDB will automatically begin to receive updates from its alternate PDBA. Before the Selective Homing of EPAP RTDBs feature, updates were received from the remote PDBA.

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.

Terminology used in Configuration Descriptions

specific PDBA *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. In a two-node MPS system, this corresponds directly to local homing. With more than two nodes, the user selects a specific PDBA without designating the PDBA as local or remote.

active PDBA *Active PDBA* is the PDBA selected by the user to receive updates from the user's provisioning system using the PDBI.

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

preferred PDB *Preferred PDB* is the PDB selected by the RTDB. The RTDB is homed to the preferred PDB. For more about standby PDB homing, see *Asynchronous Replication Serviceability Considerations*. When specific RTDB homing has been selected, the RTDB will receive updates from the alternate PDB if the preferred PDB is unreachable.

alternate PDB *Alternate PDB* is the PDB that is not selected. 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.

active homing If the user selects *active homing* for the RTDB, that RTDB always receives updates from the active PDBA. If the RTDB loses its connection with the active PDBA, the RTDB 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*.

Possible RTDB Configurations

These are the possible configurations of each RTDB in the system. Each configuration is also described in detail in the following sections.

- *Specific PDB Homing with Alternate PDB*
- *Active PDB Homing with Alternate PDB*
- *Active PDB Homing without Alternate PDB*
- *Standby PDB Homing with Alternate PDB*
- *Standby PDB Homing without Alternate PDB*

Specific PDB Homing with Alternate PDB

This RTDB configuration specifies the IP address of the PDB from which the RTDB receives updates. If the specified PDB is not reachable, the RTDB receives updates from the alternate PDB. *Table 4: Specific PDB Homing with Alternate PDB (RTDB Configuration 1)* shows the condition of each possible connection to the PDB from the RTDB perspective. The shaded cells indicate the PDB from which the RTDB receives updates.

Table 4: Specific PDB Homing with Alternate PDB (RTDB Configuration 1)

Site 1 PDB		Site 2 PDB		RTDB Data Source (Note 2)
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: PDB from which the RTDB receives updates				

See *RTDB Homing Considerations* to determine if this configuration is the most appropriate match for your installation.

Active PDB Homing with Alternate PDB

This RTDB configuration specifies that the RTDB receives updates from the active PDB. If the active PDB is not reachable, the RTDB receives updates from the standby PDB. *Table 5: Active PDB Homing with Alternate PDB (RTDB Configuration 2)* shows the condition of each possible connection to the PDB from the RTDB perspective. The shaded boxes indicate the PDB from which the RTDB receives updates.

Table 5: Active PDB Homing with Alternate PDB (RTDB Configuration 2)

Site 1 PDB		Site 2 PDB		RTDB Data Source (Note 2)
Reachable?	State	Reachable?	State	
Yes	Active	Yes	Standby	Site 1 PDB
Yes	Standby	Yes	Active	Site 2 PDB
Yes	Active	No	-	Site 1 PDB

Site 1 PDB		Site 2 PDB		RTDB Data Source (Note 2)
Reachable?	State	Reachable?	State	
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: PDB from which the RTDB receives updates				

See *RTDB Homing Considerations* to determine if this configuration is the most appropriate match for your installation.

Active PDB Homing without Alternate PDB

This RTDB configuration specifies that the RTDB receives updates from the active PDB. No alternate PDB is specified. *Table 6: Active PDB Homing without Alternate PDB (RTDB Configuration 3)* shows the condition of each possible connection to the PDB from the RTDB perspective. The shaded boxes indicate the PDB from which the RTDB receives updates.

Table 6: Active PDB Homing without Alternate PDB (RTDB Configuration 3)

Site 1 PDB		Site 2 PDB		RTDB Data Source (Note 2)
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

Site 1 PDB		Site 2 PDB		RTDB Data Source (Note 2)
Reachable?	State	Reachable?	State	
No	-	No	-	None
Note 1: Active = Preferred PDB		Standby = Alternate PDB		
Note 2: PDB from which the RTDB receives updates				

See *RTDB Homing Considerations* to determine if this configuration is the most appropriate match for your installation.

Standby PDB Homing with Alternate PDB

This RTDB configuration specifies that the RTDB receives updates from the standby PDB. If the standby PDB is not reachable, the RTDB receives updates from the active PDB. *Table 7: Standby PDB Homing with Alternate PDB (RTDB Configuration 4)* shows the condition of each possible connection to the PDB from the RTDB perspective. The shaded boxes indicate the PDB from which the RTDB will receive updates.

Table 7: Standby PDB Homing with Alternate PDB (RTDB Configuration 4)

Site 1 PDB		Site 2 PDB		RTDB Data Source (Note 2)
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: PDB from which the RTDB receives updates				

See *Asynchronous Replication Serviceability Considerations* to determine if this configuration is the most appropriate match for your installation.

Standby PDB Homing without Alternate PDB

This RTDB configuration specifies that the RTDB receives updates from the standby PDB. No alternate PDB is specified. *Table 8: Standby PDB Homing without Alternate PDB (RTDB Configuration 5)* shows the condition of each possible connection to the PDB from the RTDB perspective. The shaded boxes indicate the PDB from which the RTDB receives updates.

Table 8: Standby PDB Homing without Alternate PDB (RTDB Configuration 5)

Site 1 PDB		Site 2 PDB		RTDB Data Source (Note 2)
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: PDB from which the RTDB receives updates				

See *Asynchronous Replication Serviceability Considerations* 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 during installation and when new non-provisionable nodes are added. The configuration of all affected sites must be planned before the installation process begins.

Each MPS must be configured as provisionable or non-provisionable. Each network has two provisionable MPSs. (See *Figure 4: Support for Provisioning Multiple EPAPs*.) These MPSs must then be configured with a replicated PDB, which is described in *EPAP Software Configuration*. If non-provisionable MPSs are used, the non-provisionable MPSs are added after the provisionable MPSs are installed and configured.

Before the first MPS can be installed, the answers to these questions must be available:

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

For the configuration on each site, the answers to these questions 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 if the preferred PDB is unavailable. The RTDBs at the provisionable MPS prefer the local PDB. The remaining non-provisionable MPSs are divided evenly to prefer one PDB or the other. See *Specific PDB Homing with Alternate PDB* 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* for more information about this RTDB homing configuration.

Asynchronous Replication Serviceability Considerations

The type of RTDB homing policy selected affects serviceability by the user. Tekelec recommends for asynchronous PDB replication that Standby PDB Homing (RTDB configuration 4 or 5) is used. Although this policy may result in a slightly longer propagation time for updates from the PDB to the RTDB, the increased delay is beneficial in disaster recovery situations.

Keeping the RTDB homed to the standby PDB ensures that, except for 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. The homing methods provide proper function under all normal operating circumstances. Under these homing policies, the RTDB can possibly 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 to which the RTDB currently points.

Active and specific homing may create complications 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), the dataset of the RTDB can possibly conflict with the dataset of the only remaining PDB. This situation requires a RTDB reload from the remaining PDB, which can be a time-consuming process for any PDB with a large amount of data.

Asynchronous replication has one important effect on EPAP behavior. PDBA switchover can no longer be forced when the PDBAs are able to communicate and the standby is not current. Switchover involves allowing a 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 approach prevents database inconsistency. If the standby PDB cannot reach the active PDB to determine its level, the EPAP allows 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. The customer's provisioning system is responsible for detecting and processing socket errors. Tekelec recommends that the TCP *keep alive* interval on the customer's socket connection be set to a value that permits prompt detection and reporting of a socket disconnection problem.

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.

Although the default limit is 16 PDBI connections, Tekelec is able to configure and support up to 128 connections. If more than 16 connections are required, contact *Customer Care Center* for information.

File Transfer Options

Import Files

Manual import and automatic import are the available import file options. Both import options accept data only 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`

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 long time to complete. A write transaction lock is applied during the entire import for a manual import, and is applied intermittently during an automatic import. While the write transaction lock is in place during either type of import, no other updates to the database can be made.

Manual Import

The manual import mode is used to import data on a one-time or *as needed* basis. The manual import mode is configured with 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 Setup

When 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 five minutes. If a file exists in the directory and the file 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.

The automatic import option can import up to 16 files at one time. The number of files imported is limited by the available number of PDBI connections. If more than 16 files exist in the directory, another file is started after a previous file completes 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.

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

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

Automatic Import Status

When using the automatic import function, the following informational banner messages is displayed on the UI browser screen in the Message Box described in *Figure 18: EPAP Area*.

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

```
Import of <filename> completed (when complete)
```

If the import fails when the PDBA is not running and the automatic import was started by `cron`, the following informational banner message is displayed on the UI browser screen in the Message Box described in *Figure 18: EPAP Area*.

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

If the import fails when the connection to the PDBA is lost while the automatic import is in progress, the following informational banner message is displayed on the UI browser screen in the Message Box described in *Figure 18: EPAP Area*

```
Import of <filename> failed - PDBA died
```

If an automatic import fails, an automatic retry will occur every five minutes.

Export Files

The manual export and automatic export are the available export file options. Data can be exported in both PDBI and CSV formats. Refer to *Provisioning Database Interface Manual* for more information. The Manual File Export allows data to be exported to a specified location on a one-time or *as needed* basis, and is configured by the Export PDB to File Screen.

Automatic File Export

The Automatic File Export function allows scheduling the data export for a specific day and time. The export can be scheduled at a specific time for each of the following repeat periods: every N (up to 365) number of days, specified days of the week, specified day of the month, or specified day of the year. The Schedule Export screen displays any existing PDB export tasks and is used to create a task by specifying the type, export format (PDBI CSV), export mode (blocking, snapshot, or real-time), the time and repeat period. In addition, a comment field is available to describe the task. The output filename format is *pdbAutoExport_<hostname>_<YYYYMMDDhhmmss>*. 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 feature is used to back up all data stored in the PDB or RTDB, including G-Port, G-Flex, INP/AINPQ, A-Port, Migration, V-Flex, 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 backup is created on EPAP A and RTDB 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 or RTDB that is being backed up.
- **Mate** - Data is created on the local server and then sent using SCP to the mate EPAP server.
- **Remote** - Data file is created on the local EPAP server and then sent using 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.

For mate or remote backup destinations, an option exists to save a copy of the backup to the local drive. For mate or remote backup destinations, even if the user has selected the option to not save the local copy, the local copy will be saved if the file transfer fails after the backup file has been created on the local machine.

Both the PDB and RTDB backups are scheduled together, but executed separately. Based on the input parameters, RTDB backup always starts one hour before of the PDB backup. When setting up the feature, the time that the RTDB backup starts is selected. The PDB backup starts one hour later.

No link exists between backups of one MPS system with backup of the other MPS system. Backups can be scheduled and created only on provisionable pairs. The 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 Service Module card RTDB. RTDB backups are always created from the standby EPAP RTDB (A or B).

If backup failures occur, alarms and error messages are generated and logged. Two types of backup failures are:

- **Backup operationfailures**: This is a failure to create backup files on either of the systems - local or mate. Two alarms iare possible: 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. The backup files exist on the local machine. Two alarms are possible: one for the PDB and one for the RTDB.

A delay of up to five minutes is possible after the scheduled time before the actual start of the scheduled backup.

The effects of cancelling a back up while it is executing are:

- If the automatic backup of the RTDB is in progress, the RTDB backup will complete and the PDB backup will not start.
- If the RTDB backup has completed but the PDB has not started, the PDB backup will not start.
- If the RTDB backup has completed and the PDB has started, PDB backup will complete.

This feature is supported and configured using the Web-based GUI. Refer to *Automatic PDB/RTDB Backup* 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 one PDBA to become Active when two 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 its mate to become the Active PDBA; the PDBA that was the Standby most recently becomes the Active. No automatic reconciliation is performed because the system has insufficient information to ensure that the correct actions are taken.

To return the system to normal functionality, a manual PDB copy imust be performed from the PDBA that was chosen to be Active to the PDBA that is in the replication error (REPLERR) state. However, provisioning can be resumed until a maintenance period is available to perform the manual PDB copy.

The Customer Care Center must be contacted before performing the PDBA Copy procedure.

The EPAP Automated Database Recovery 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 that the EPAP systems properly process the updates.

EPAP Automated Database Reconciliation Example

Starting with PDBAs in the following current configuration.

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

Table 9: Example 1 EPAP ADR

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

Active PDBA (Node 1)	Standby PDBA (Node 2)
701	
702	
703	

Assume that 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.

Table 10: Example 2 EPAP ADR

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.
- Updates 701-703 on Node 1 are different from updates 701-703 on Node 2.

The PDBA that received an update with the latest timestamp (in this example, Node 2 PDBA) will automatically become the Active PDBA and continue accepting provisioning updates. The Node 1 PDBA is put in a REPLERR state and *PDBA Replication Failure* alarm initiates on Node 1 PDBA.

A replerr file (REPLERR 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 to reapply these updates to the Active PDBA.

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

The EPAP Automated Database Recovery feature is enabled through the text-based EPAP user interface.

EPAP PDBA Proxy Feature

The EPAP PDBA Proxy feature allows operators to maintain the existing (active) provisioning VIP address connection to the EPAP PDBA in the event of an active PDBA failure. The advantages of this feature are:

- Seamless, uninterrupted VIP connection for provisioning data to the standby EPAP PDBA if the active PDBA fails
- No need to perform a manual switchover to the standby PDBA or change the provisioning VIP address in operator provisioning software
- A means of reconciling both PDBAs when the failed PDBA becomes available again

The EPAP system uses two provisioning VIP addresses: one VIP for the local or active EPAP and one VIP for the remote or standby EPAP. However., provisioning can be performed only on the active provisioning VIP address. The EPAP PDBA Proxy feature maintains the existing, active provisioning VIP address connection to the previously active Node when the active PDBA fails. The previously active EPAP B on that Node proxies provisioning data to the temporarily active PDBA on the other Node.

With the EPAP PDBA Proxy feature, PDBA connection redundancy is accomplished by allowing the customer's provisioning system to maintain the connection to the previously active EPAP B using the active provisioning VIP address, even though the connection may be logically, by-proxy, to the previously standby PDBA on the other Node. When the previously active PDBA recovers, that PDBA is aware that the standby PDBA has become active and the PDBAs need to be reconciled.

EPAP PDBA Proxy Feature Requirements/Limitations

Some requirements and limitations of the EPAP PDBA Proxy feature are:

- The customer provisioning system loses connection to the PDBA:

  When the EPAP PDBA Proxy feature is first initiated upon server failure and switchover to the backup PDBA

  During recovery when service is being restored to the PDBA on the sever that had failed

  When the connection is lost, it must be re-established to the same VIP address.
- Both provisioning VIP addresses (the local or active EPAP VIP and the remote or standby EPAP VIP) must be configured using the text-based EPAP user interface. See *Configure Provisioning VIP Addresses*.
- The Change PDBA Proxy State procedure must be performed on both active and standby MPS-A PDBAs. See *Change PDBA Proxy State*.
- The EPAP PDBA Proxy feature does not provide PDBA connection redundancy in the case of PDBA (application) failure. The EPAP PDBA Proxy feature provides PDBA connection redundancy only after failure of the active EPAP A.
- The EPAP PDBA Proxy feature does not initiate in response to a Switchover PDBA State. A manual switchover requires the operator to change the provisioning VIP address in operator provisioning software.
- The EPAP PDBA Proxy feature does not require activation of the Automated Database Recovery (ADR) feature

Note: If a replication error (REPLERR) occurs while using the EPAP PDBA Proxy feature, manual intervention is required. Contact *Customer Care Center*.

EPAP PDBA Proxy Example

During normal provisioning operations:

- Operator provisioning system sends provisioning updates to the Active PDBA on Node 1 using the active provisioning VIP address (192.168.0.1).

- Active PDBA checks syntax and writes to the Active PDB.
- Active PDBA writes to a replication log on the EPAP A and local EPAP B.
- Active PDBA sends an ACK response to the operator provisioning system.
- Standby PDBA on Node 2 queries the EPAP A replication logs on Node 2 and updates the PDB on Node 2.

A fault (server failure) on the Node 1 with the active PDBA is shown in *Figure 5: Failure of Active PDBA*:

- With the EPAP PDBA Proxy feature enabled, the system continues using the active provisioning VIP address (192.168.0.1).

  Note: During the switchover to the PDBA on Node 2, the customer provisioning system loses connection to the PDBA. The connection must be re-established to the same VIP address.

- If the Standby PDBA on Node 2 is reachable, EPAP B on Node 1 transmits replication logs to the Node 2 PDBA.
- When the Node 2 PDBA has all the replication logs from the EPAP B on Node 1, the Node 2 PDBA becomes the Active by-proxy PDBA.
- Operator provisioning continues using provisioning VIP address 192.168.0.1 because EPAP B on Node 1 proxies provisioning data to the newly Active PDBA on Node 2.

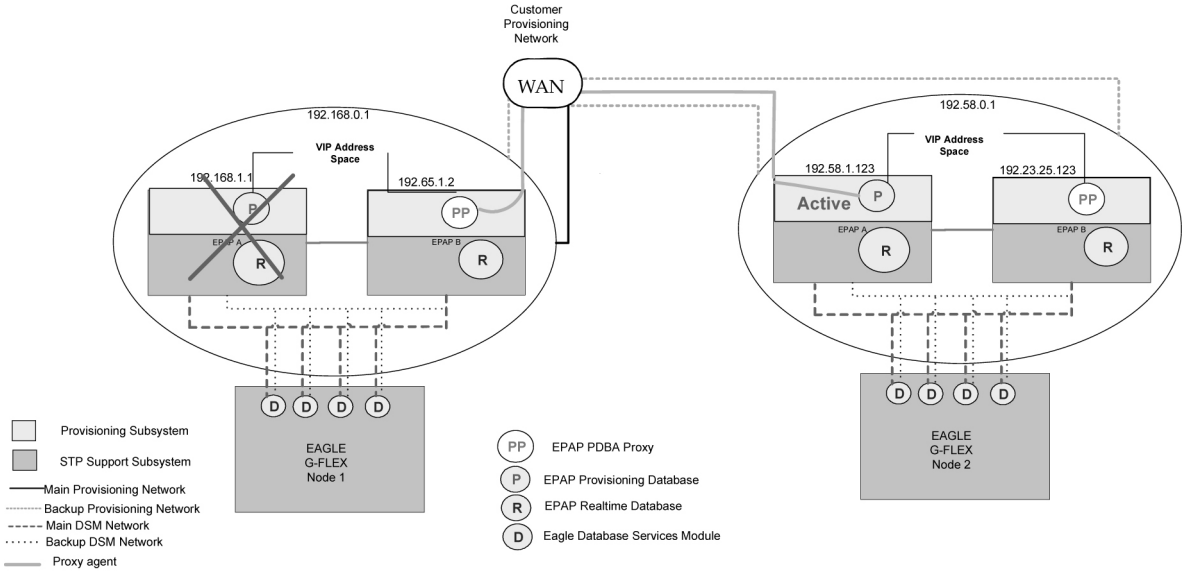

Figure 5: Failure of Active PDBA

When the Node 1 PDBA is restored to service:

- Updates sent to Node 2 PDBA while the Node 1 PDBA was down are forwarded to the Node 1 PDB.
- Records are replicated. Node 1 becomes the Active PDBA and Node 2 reverts to Standby status.

  Note: During recovery when the PDBA on Node 1 is being restored to service, the customer provisioning system loses connection to the PDBA. The connection must be re-established to the same VIP address.

This feature is enabled through the text-based EPAP user interface. See *PDB Configuration Menu* .

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 using the GUI or PDBI. The three modes of operation are:

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 database after export has started are not reflected in the export file. This mode provides a file that is the most useful for importing into the database at a later time.

   Note: This mode causes the server to run increasingly slower as updates are received on the other connections.
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 database after the export has started may or may not be reflected in the export file, depending upon whether the changes are to an area of the database that has already been exported. This mode provides a file that can be imported into the database at a later time, but is less useful because it is not a complete snapshot of the database at a given time.

EPAP 30-Day Storage or Export of Provisioning Logs Feature

The EPAP 30-Day Storage or Export of Provisioning Logs feature allows the EPAP to store provisioning logs on the EPAP hard drive for a configurable interval provided the disk partition does not become full within that interval. This feature also allows configuration of storage time for error logs and debug logs.

Table 11: Log Storage Intervals

Log Type	Configurable Storage Range	Default Value
Provisioning Logs	1 to 30 days	1 day
Error Logs	1 to 30 days	1 day
Debug Logs	1 to 7 days	1 day

Alarms notify the user when the log disk 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 issues a minor alarm. No files are removed at this point.
2. If the disk where the logs are stored becomes 90% full before the configured time period has elapsed, the EPAP issues a major alarm. No files are removed at this point.
3. If the disk where the logs are stored becomes 95% full before the configured time period has elapsed, the EPAP issues a major alarm. The EPAP will begin removing the oldest entries in the logs to free disk space 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, the 80% alarm is replaced by the 90% alarm until the 90% alarm clears. After the 90% alarm clears, the 80% alarm remains active until it is cleared.

EPAP User Interface

The EPAP provides two user interfaces that consist of sets of menus for configuration, maintenance, debugging, and platform operations. When a menu item is chosen, the user interface directs the system to perform the requested action.

- **Graphical User Interface**

  The Graphical User Interface (GUI) provides menus to perform routine operations that maintain, debug, and operate the platform. A PC with a network connection and a Web browser is used to communicate with the EPAP GUI. *Overview of EPAP Graphical User Interface (GUI)* describes GUI login, menu items, and associated outputs.

- **Text-based User Interface**

  The text-based User Interface provides the Configuration menu to initialize and configure the EPAP. The text-based User Interface is described in *EPAP Configuration Menu*. For information about configuring the EPAP and how to set up a PC workstation, refer to *Setting Up an EPAP Workstation*.

Service Module Card Provisioning

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

The 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 Service Module cards across two Ethernet networks. See *Network Connections*. The DSM provisioning network architecture is shown in *Figure 6: DSM Provisioning Network Architecture* and the DSM provisioning task interface is shown in *Figure 7: DSM Provisioning Task Interfaces*.

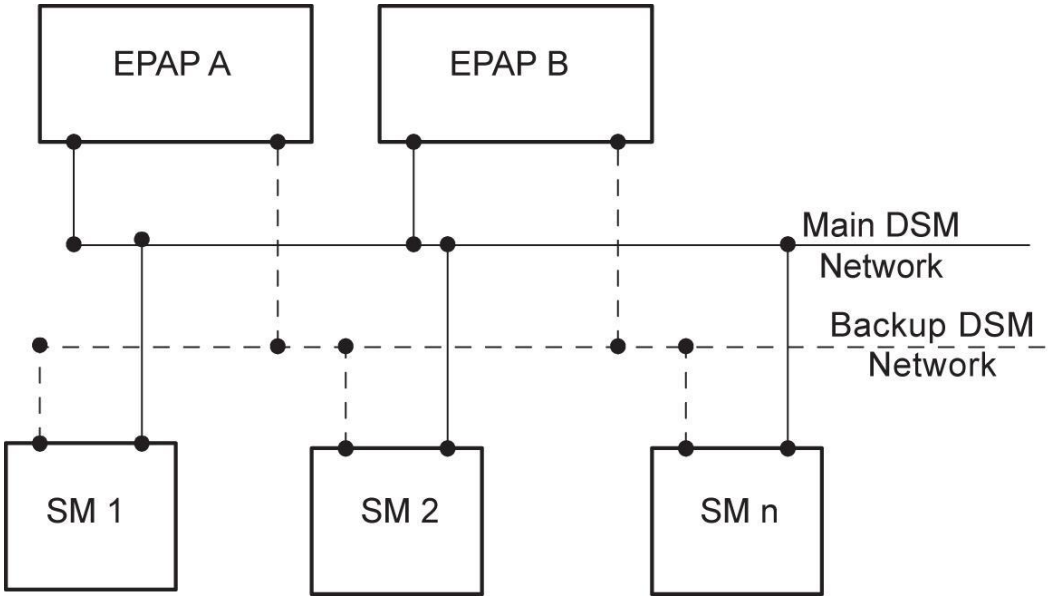

Figure 6: DSM Provisioning Network Architecture

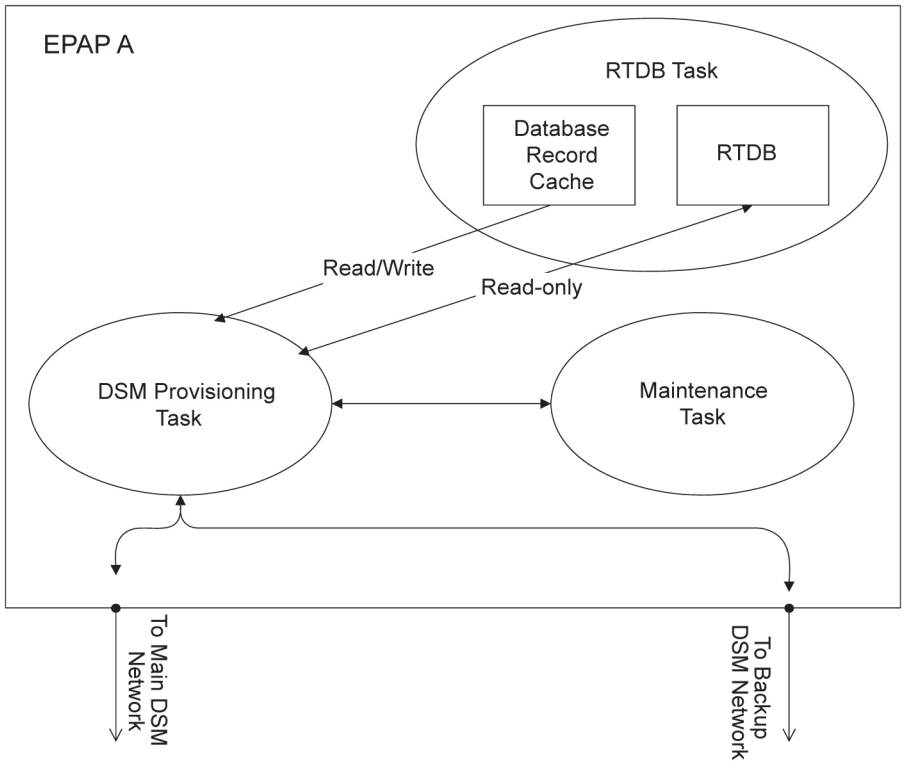

Figure 7: DSM Provisioning Task Interfaces

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 Service Module cards. Provisioning is done by database level in order to leave Service Module card tables coherent between updates.

In addition to a constant stream of current updates, it is necessary to provision back-level Service Module 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 Service Module card has missed some updates, but does not need a complete reload.

The Service Module card 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 Service Module card level.

Once an incremental loading stream is set up, the following incremental loading transaction is repeated until the Service Module cards 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 Service Module cards 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. Service Module cards accept any stream with the "next" sequential database level for that card.

Service Module Card Reload

The stages of database reload for a given Service Module card are given the following terminology:

Stage 1 loading - The database is being copied record for record from the Active EPAP to the Service Module card 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.

Service Module 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 Service Module cards with the current database. The database on the EPAP is large and may be updated constantly. The database sent to the Service Module 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 Service Module card 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 Service Module cards that do not require it.

Continuous Reload

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

Service Module Card Database Levels and Reloading

The current database level when the reload started is of special importance during reload. When a Service Module card 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 Service Module card 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 Service Module cards 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/Service Module Card 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 Service Module cards. Refer to *Figure 8: MPS Hardware Interconnection* for the MPS hardware interconnection diagram.

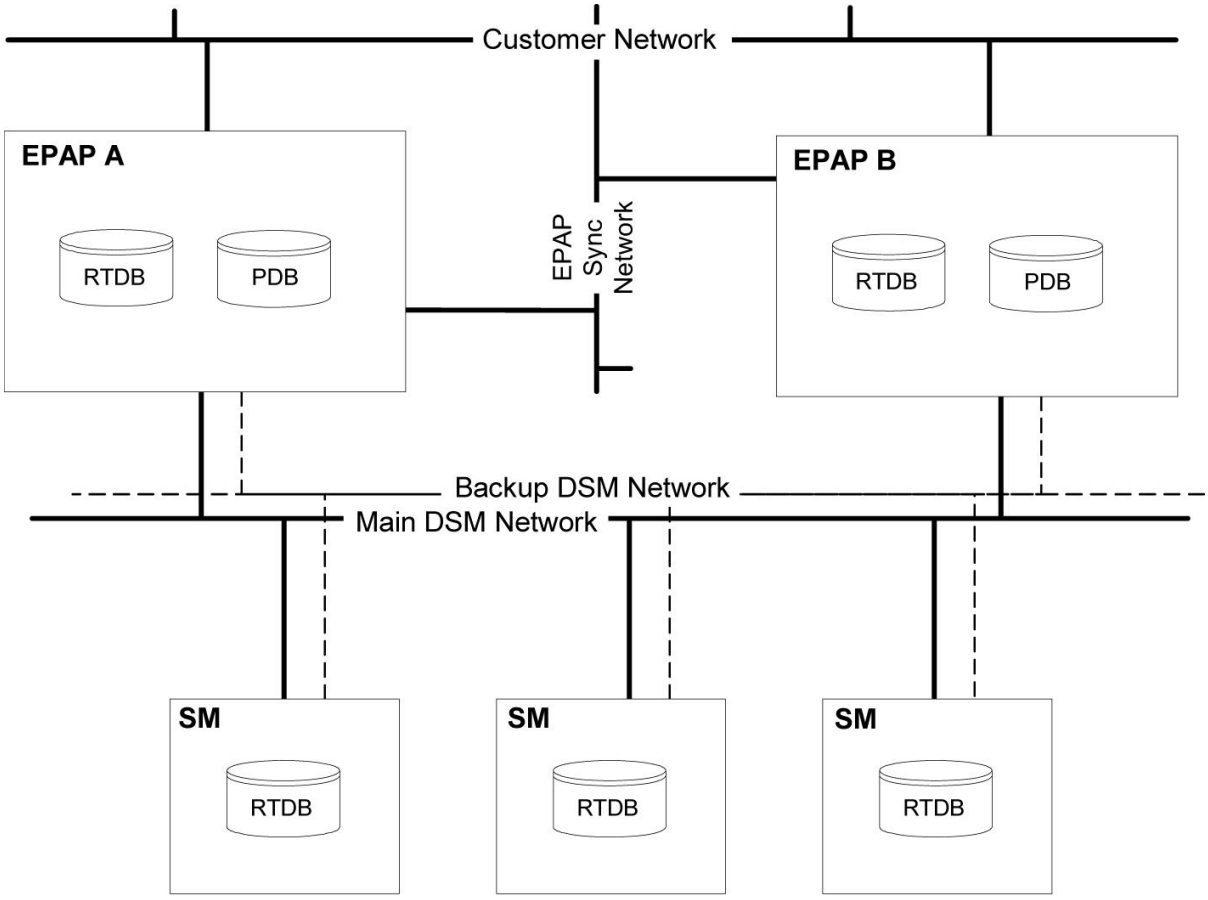

Figure 8: MPS Hardware Interconnection

MPS/Service Module Card RTDB Audit Description

MPS RTDB Audit

This audit maintains the integrity of the RTDB 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. If 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, enabled, or disabled through this control. See *Maintenance Menu*.

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

EPAP-to-DSM Network Card DB Level

Each Service Module card validates its own database level against the received EPAP database level. An inconsistent alarm is generated at the EAGLE 5 ISS for each inconsistent Service Module card. The command `rept-stat-db` displays the database on the Service Module card as *Diff* level. See *Table 12: Inconsistent Service Module Card Alarm* .

Table 12: Inconsistent Service Module 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 Service Module card. This audit cycles though the entire RTDB within a 24-hour period, reporting any anomalies in the form of alarms and may attempt to repair a corrupted record with a valid record from a mate Service Module card.

The STP Options (`chg-stpopts`) command is used to set up this audit with 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 Service Module cards is disabled from auditing the RTDB Databases. Setting the `dsmaud` parameter to `on` enables the auditing capabilities which produce an alarm if a corrupted record is detected. Setting the `dsmaud` parameter to `ccc` enables the cross correction capabilities, which provide a method for repairing a corrupt record when it is encountered.

When corruption is encountered, this sequence occurs.

1. The RTDB is set to Corrupt status.
2. A UAM (*Table 13: Corrupted RTDB Database Alarm*) is sent to the OAM
3. The corruption is logged and stored in a memory array with this information:
   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 13: 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 is 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 Reload.

Service Module 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 different events will occur based on the loading phase state. See *Table 14: Effect of Corrupted Record Received from MPS*

Table 14: 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 on any card becomes corrupted, a mate Service Module card can supply the correct data for the record. Corruption Cross Correction occurs across the IMT. For each corrupted record encountered, a single broadcast message is sent from the affected Service Module card to all mate Service Module cards. When a Service Module card receives a request for Corruption Cross Correction, the current database level and requested record are evaluated for consistency. If the request is validated, a response is sent to the original Service Module card. Otherwise, the request is discarded. This would occupy no more than 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 after being passed to the Service Module card. Subsequent messages received for the same correction are 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 Service Module card, known as the primary Service Module card. Static information is exchanged across this interface at initialization and dynamic information is exchanged on occurrence.

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 *Messages, Alarms, and Status Processing*.

The EPAP sends two types of messages to the Service Module card: EPAP Maintenance Blocks, and Service Module card 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 Service Module card in the Maintenance Block message (see *Maintenance Blocks*), which is reported on the EAGLE 5 ISS terminal by the OAM. The various alarm messages are described in *Messages, Alarms, and Status Processing*.

Status Reporting

The Active EPAP generates and sends Maintenance Blocks to the primary Service Module card. One Maintenance Block will be sent as soon as the IP link is established between the Active EPAP and the primary Service Module card. 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*).

When the EPAP desires to know the status of a Service Module card, it can send a Service Module card Status Request to that Service Module card. See *Service Module Card Status Requests*. The EPAP broadcasts the Service Module card Status Request over UDP, and all Service Module cards return their status. Service Module cards also send a Service Module card status message to the EPAP when certain events occur in the Service Module card.

EPAP status reporting is described in detail in *Messages, Alarms, and Status Processing*.

Chapter 3

EPAP Graphical User Interface

Topics:

This chapter provides a detailed description of the EPAP Graphical User Interface (GUI).

Overview of EPAP Graphical User Interface (GUI)

EPAP uses a Web-based user interface in a typical client-server paradigm. The front end appears on a Web browser. See *Compatible Browsers* for supported browsers. The back end operates on the MPS platform.

The graphical user interface display has three different sections:

- Banner header section for displaying the real-time status of the MPS servers
- Menu section for selecting desired actions
- 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. The banner applet displays current status of the EPAP, state of the alarms, and other information. The banner applet contains the EPAP A and B areas, both PDBA areas, and the busy icon.

An http or https (Hypertext Transfer Protocol) Web server starts the process of handling requests from browsers. It receives the requests and loads the document. If the document is a simple HTML file, the http or https Web server returns the document to the browser. The EPAP software may also connect with the GUI server to request actions be performed. HTML output from the script is returned to the browser and displayed.

Figure 9: Process Architecture View of the EPAP UI shows the architecture view of the EPAP user interface.

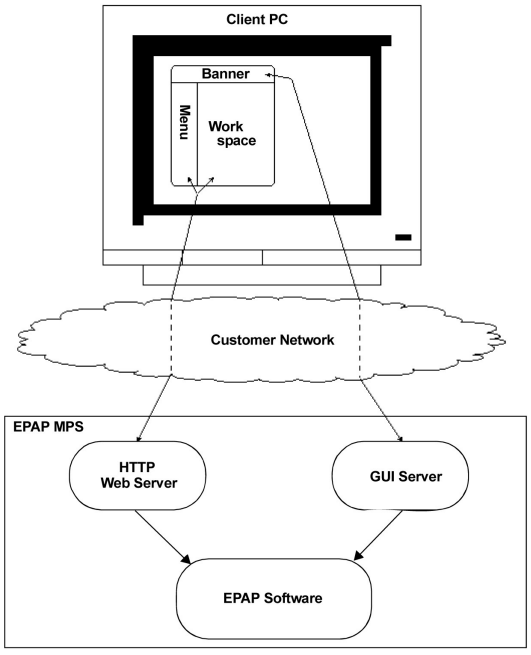

Figure 9: Process Architecture View of the EPAP UI

EPAP Support for HTTPS on GUI

The EPAP Support for HTTPS on GUI feature allows users to configure how the GUI can be accessed: by standard HTTP (Hypertext Transfer Protocol), 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.

EPAP allows admin user group members to configure 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.

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 one 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 message.

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 message.

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:

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. 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 **Security Alert** dialog is displayed.

Figure 10: Security Alert Dialog

3. Click **View Certificate**.
   The **Certificate** dialog is displayed.

Figure 11: Certificate Dialog

4. Click **Install Certificate**.
   The **Certificate Import Wizard** Welcome is displayed.

Figure 12: Certificate Import Wizard - Welcome

5. Click **Next**.
   The **Certificate Import Wizard** - Certificate Store is displayed.

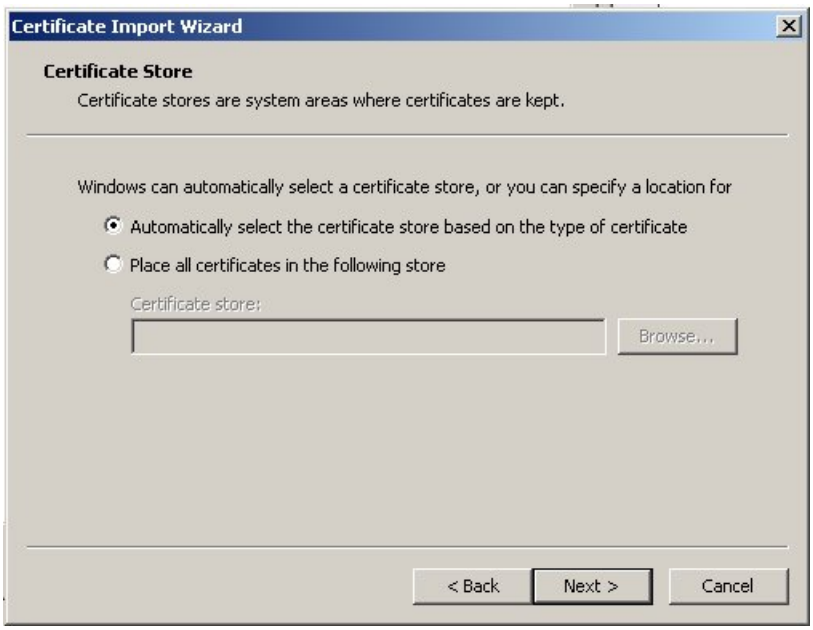

Figure 13: Certificate Import Wizard - Certificate Store

6. Ensure that the **Automatically select the certificate store based on the type of certificate** radio button is selected.
7. Click **Next**.
   The **Certificate Import Wizard** - Completing the Certificate Import is displayed.

Figure 14: Certificate Import Wizard - Completing the Certificate

8. Click **Finish**.
   The **Security Warning** dialog is displayed.

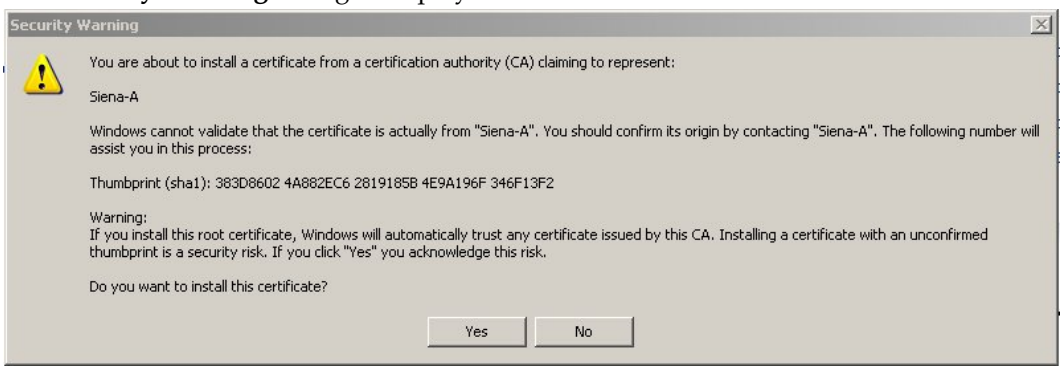

Figure 15: Security Warning Dialog

9. Click **Yes**.
   The **Certificate Import Wizard** displays a success message and you are returned to the Certificate dialog.

Figure 16: Certificate Dialog

10. Click **OK**.

Login Screen

The first screen of the EPAP User Interface (UI) 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, then click the Login button. These fields provide the user identification and verification.

When a user logs in successfully, the screen workspace indicates that the user is logged in.

When a user logs into the EPAP UI, the user does not need to log in again if the web browser session remains active and if no user in the `admin user` group changes the HTTPS configuration. Subsequent user authentication is handled with*cookies*, which are stored in the browser of the user and are retained during the browser operation. If a user in the `admin user` group changes the HTTPS configuration from only HTTP to only HTTPS, all logged -n users are disconnected. Similarly, if a user in the `admin user` group changes the HTTPS configuration from only HTTPS to only HTTP, all logged-in users are disconnected. For more information, see *EPAP Support for HTTPS on GUI* .

The user uses the Logout menu option to terminate the session. Alternatively, the user can be logged out by session inactivity (interval defined by User Administration), by disabling in the HTTP or HTTPS configuration, by administrator termination , and by selection of another window using another independent browser.

EPAP GUI Main Screen

The EPAP graphical user interface main screen is composed of three frames, or window sections. The topmost frame is the banner. The banner frame extends the entire width of the browser window. The remainder of the browser window is divided vertically into two frames of unequal width. The smaller frame on the left is the menu section. The larger frame on the right is the workspace section.

Banner Section

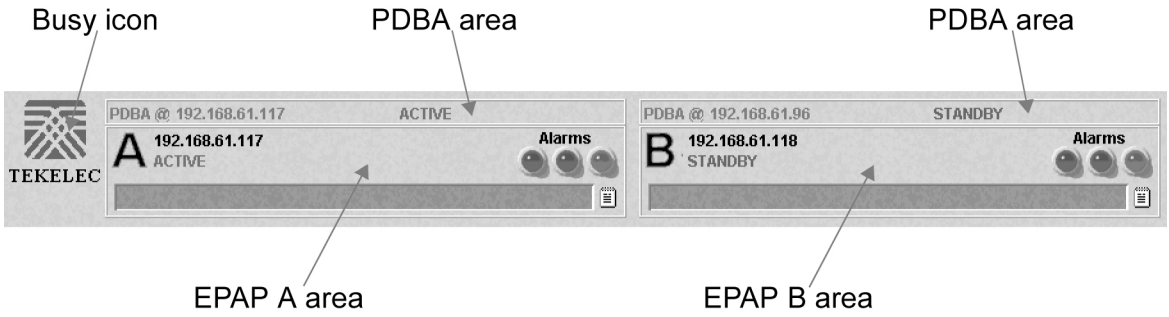

Figure 17: EPAP Banner Applet

The Tekelec logo icon 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.

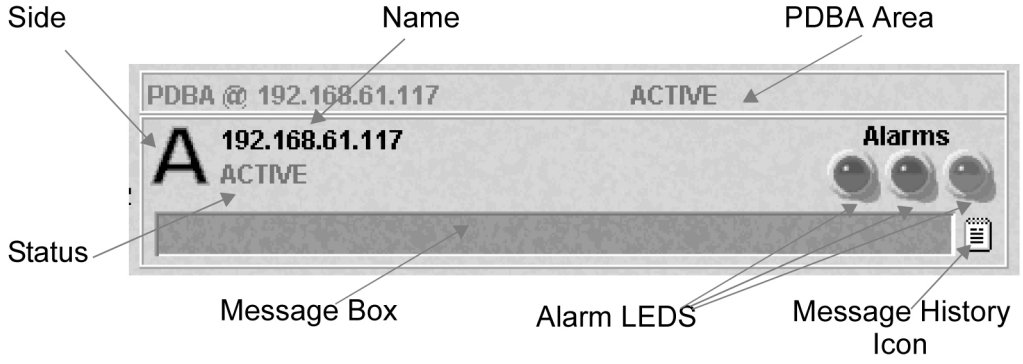

Figure 18: EPAP Area

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

- EPAP Server - This indicator shows which side of the EPAP (A or B) is represented by this area. No action is available using a mouse 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:

- 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 Service Module cards 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 Service Module cards with data. It is also the machine that has the connection to the primary Service Module card 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 *Install Java Policy File*.

- 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.

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* .

- 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.

  Below 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* 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:

PDBA Area

The PDBA areas each occupy a part of the banner applet, and have the following indicators and displays.

- 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 a 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 submenu 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.

Workspace Section

The results of 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.

The format for the workspace is a page header and footer. In the header, the left-justified letter A or B designates which MPS server this menu action affects. The right-justified menu will also display the action title. The footer consists of a bar and text with the time when the page was generated, as well as Tekelec copyright notice information.

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, a list of syntax hints can be displayed when the mouse is moved oevr the field.
- Pop-up syntax checking: When the **Submit** button is clicked, 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, the error can be corrected, and the input submitted again.

- Back-end syntax checking: When the **Submit** button has been clicked 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 Graphical User Interface Menus

The EPAP menu is the main menu of the EPAP application. It provides the functions of the EPAP User Interface. *Figure 19: EPAP Menu* shows the EPAP main menu.

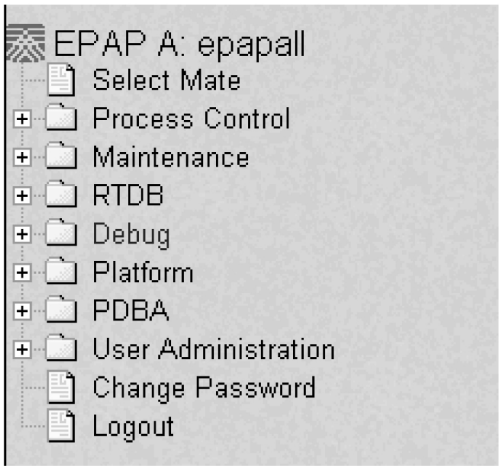

Figure 19: EPAP Menu

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 19: EPAP Menu*).

If you are 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 will be displayed.

The Select Mate action does not cause the contents of the banner to 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 provides the start and stop software actions.

Start EPAP Software

The Start EPAP Software menu option contains a button to confirm that you do want to start or stop the software processes and a checkbox to start the PDBA.

Stop EPAP Software

The Stop EPAP Software screen contains a button to confirm that the user wants to stop the software processes. It also allows a choice to automatically restart the software when the server reboots.

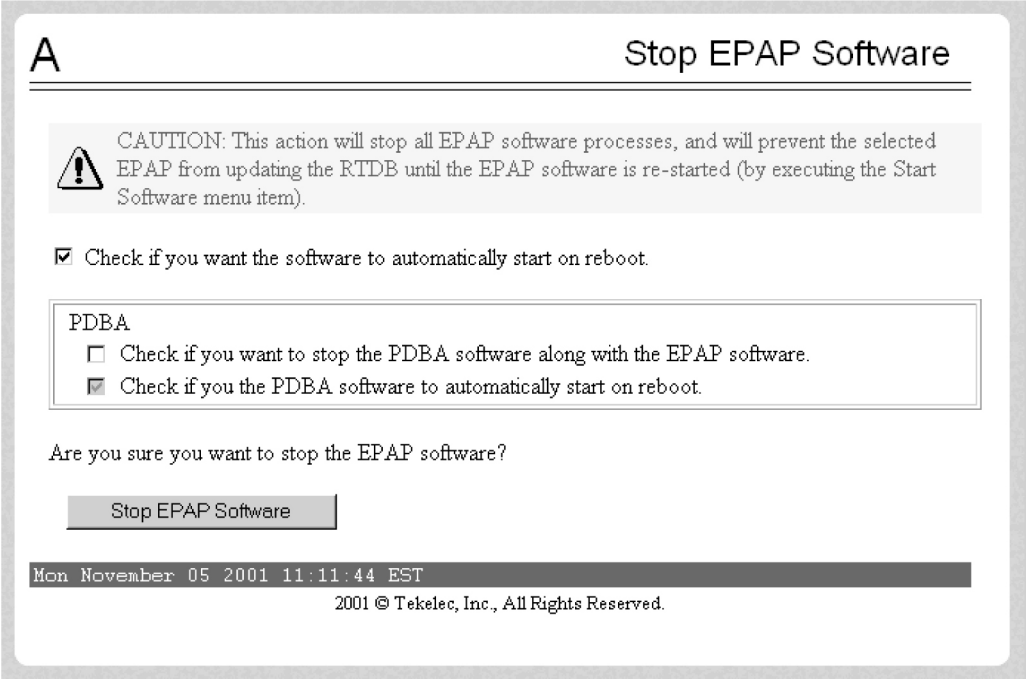

Figure 20: Stop EPAP Software Screen

Maintenance Menu

The Maintenance Menu allows the user to perform various EPAP platform tasks:

- *Force Standby*
- *Display Release Levels*
- *Decode MPS Alarm*
- *RTDB Audit*
- *Configure File Transfer*
- *Automatic PDB/RTDB Backup*

Force Standby

The Maintenance / Force Standby menu gives the user the ability to view the EPAP status and change the status.

The Force Standby menu provides the following actions:

View Status

The View Status screen displays whether or not EPAP is currently in a forced standby state.

Figure 21: View Forced Standby Status Screen

Change Status

The Change Status screen displays the current state of the selected EPAP. 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.

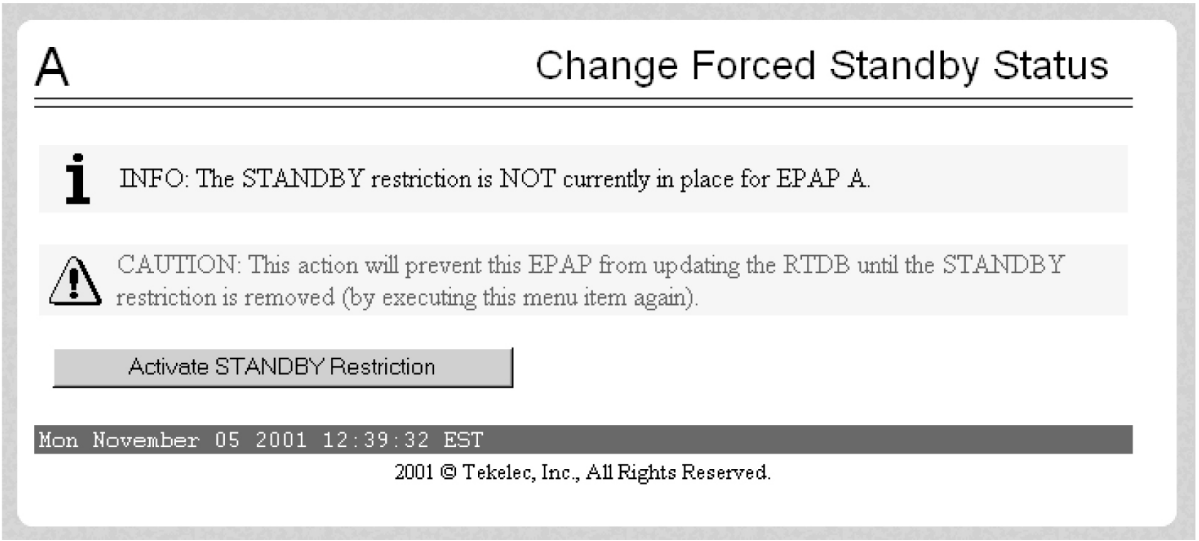

Figure 22: Change Forced Standby Status Screen

Display Release Levels

The Maintenance / Display Release Levels screen displays release information.

Transaction Log Menu

The Transaction Log menu consists of:

- Retrieve Entries
- Export to File

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 *EPAP Alarms on the T1200 Platform* manual.

RTDB Audit

The Maintenance / RTDB Audit menu lets the user view and change the auditing of the selected EPAP.

The RTDB Audit menu provides:

- *View Enabled*
- *Change Enabled*

View Enabled

The Maintenance / RTDB Audit / View Enable menu selection lets the user view the status of RTDB audit enabled:.

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.

Configure File Transfer

This screen has several different functions. This screen can be used to:

- 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 23: Configure File Transfer Screen*.

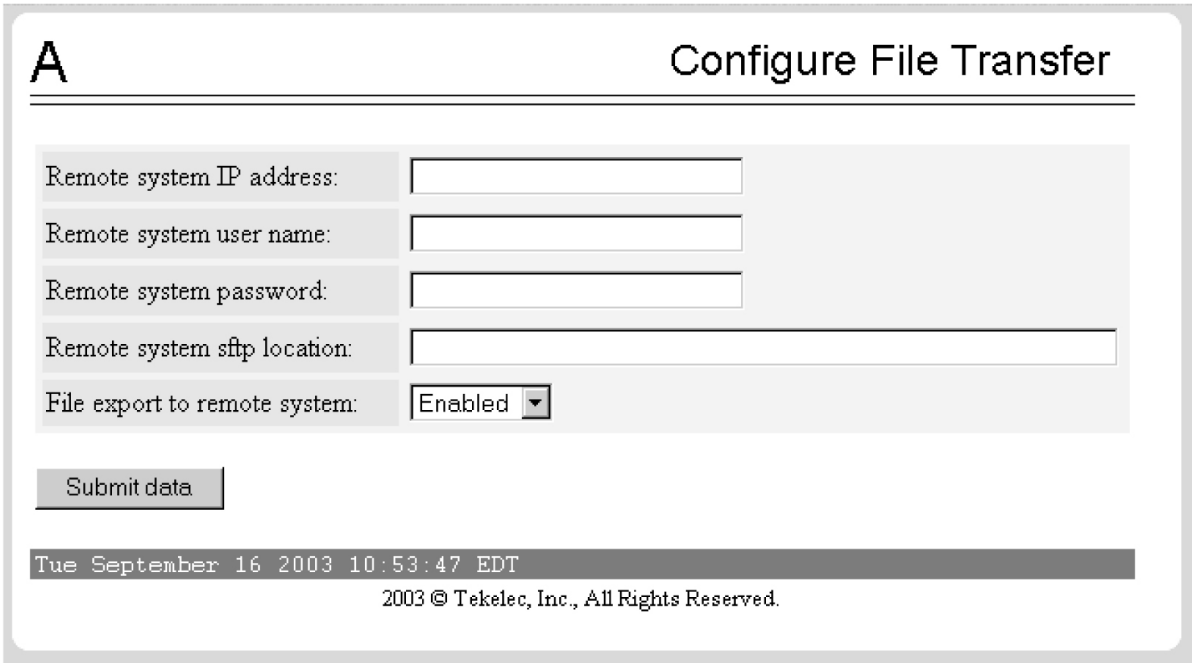

Figure 23: Configure File Transfer Screen

Automatic PDB/RTDB Backup

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

- 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 15: Mandatory and Optional Parameters* as a guide when populating the Automatic PDB/RTDB Backup screen. See *Figure 24: Automatic PDB/RTDB Backup Screen*.

Table 15: Mandatory and 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, then before scheduling:

- The 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, follow these semantic rules:

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 (*)

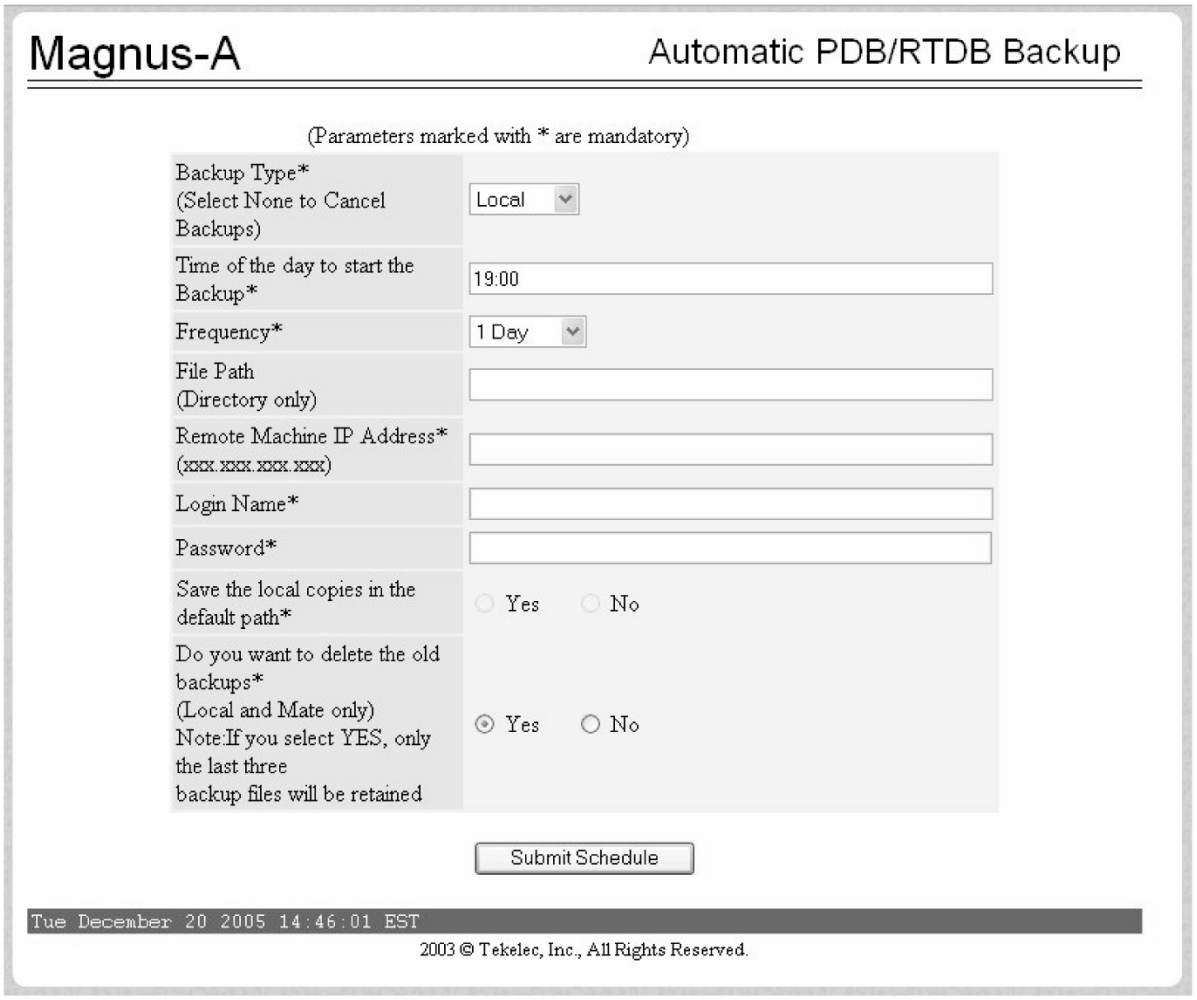

Figure 24: Automatic PDB/RTDB Backup Screen

Schedule EPAP Tasks

Maintenance /Schedule EPAP Task

This screen is used to Schedule EPAP Tasks. Through this screen the customer has a choice of what tasks to be scheduled as well as the day and time of day for the execution of the tasks.

The tasks can be scheduled at a specific time for each of the following repeat periods: at specific minute, at specific hour, every N number of days (N can be up to 30), on specific days of the week, on a specified day of the month, or on a specified day of the year.

The Schedule EPAP Tasks screen is used to display any existing tasks and to create a task by specifying the type, ID, Action, Parameters, as well as the time and repeat period. In addition, a Comment field is available to describe the task.

Figure 25: Schedule EPAP Tasks Screen is an example of the Schedule EPAP Tasks screen.

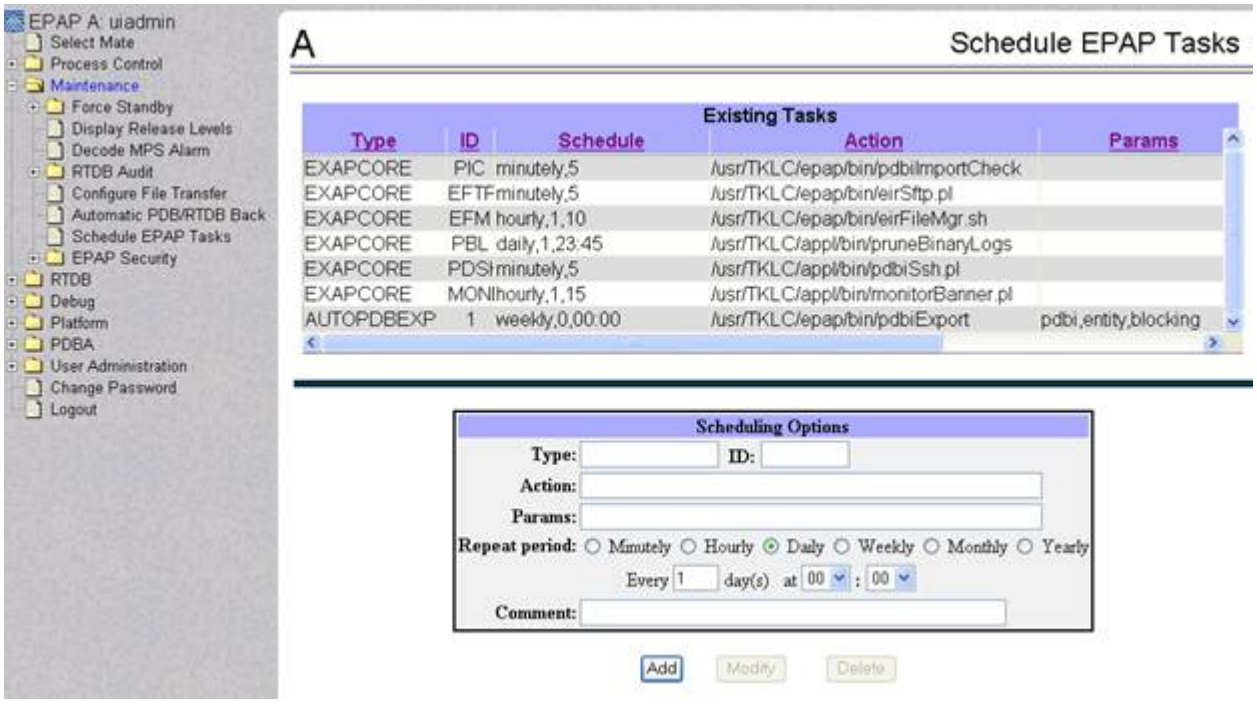

Figure 25: Schedule EPAP Tasks Screen

Existing Tasks

The Existing Tasks portion at the top of the screen displays all currently scheduled tasks 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, to view, modify or to delete the tasks.

Scheduling Options

The Scheduling Options section of the **Schedule Tasks** screen allows the user to choose how often to repeat the scheduled task and to specify the exact day and time. The appearance of this section changes depending on which **Repeat Period** radio button 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*:

Type:	Type of the task can be specified in this field.
ID:	ID of the task can be specified in this field.

Action:	Action of the task specified by adding the path for the task.
Parameters:	Parameters for the task can be specified in this field.
Comment:	Use this optional field to add comments about Tasks. 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.

Minutely Repeat Period

To schedule the task to be run minutely, select the minutely radio button, select the minute and optionally enter a comment.

Hourly Repeat Period

To schedule the task to be run hourly, select the hourly radio button, select the hour, select the minute and optionally enter a comment.

Daily Repeat Period

To schedule the task to be run every N days, select the Daily radio button, specify a number (N) to indicate that the Task should be run every N days, select the time and optionally enter a comment.

Note: Although the maximum value allowed in the day(s) field is 30.

Weekly Repeat Period

To schedule the task 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.

Monthly Repeat Period

To schedule the tasks 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.

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

Yearly Repeat Period

To schedule the tasks to be run one day each year, select the Yearly radio button, select a numeric day of the year, select the day of the month, select the time, and optionally enter a comment.

Add, Modify, and Delete Buttons

The **Add**, **Modify**, and **Delete** buttons are located at the bottom of the Schedule EPAP Tasks screen.

Add	To add a scheduled EPAP Task, enter all the data to describe the task, 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 To modify a scheduled EPAP Task, click that task in the Existing Tasks in Tasks table, change any data that describes the task, and click the **Modify** button. The **Modify** button is selectable only when an entry in the Existing Tasks table at the top of the screen has been selected and one or more fields other than Type and ID on the screen have been changed.

Delete To delete a scheduled Task, click that task in the Existing EPAP Tasks table, and click the Delete button.

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

EPAP Security

This menu allows the user to view/configure access security for EPAP server. The user can view/change the following two configurations:

- Restrict/Allow command line access to server root account.
- Restrict/Allow server access to only authorized IPs or to all.

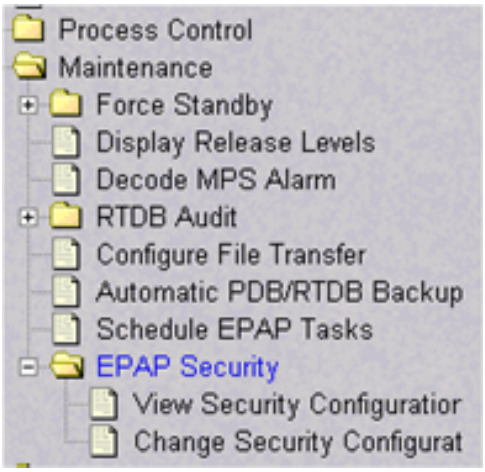

Figure 26: EPAP Security menu

View Security Configuration

This menu allows the user to view security access for EPAP server on which the GUI is open. The user can view the following two configurations:

- Restrict command line access to server root account.
- Restrict server access to only authorized IPs or to all.

Configuration may be different on mate. To view configuration on mate, select mate from GUI and select **Maintenance EPAP Security View Security Configuration** on mate to view configuration on mate server.

When the value of *Restrict remote access to server root account* is set to *No*, root can access the server using ssh. When the value of *Restrict remote access to server root account* is set to *Yes*, root cannot directly access the server using ssh. However, the user can ssh to the server as `epapdev` and then do an `su - root` to access the server as root.

When the value of *Restrict server access to authorized IPs* is set to *No*, the server can be accessed from any IP address. When the value of *Restrict server access to authorized IPs* is set to *Yes*, the server can be accessed only from the IP addresses that are added in file `/etc/hosts.allow`.

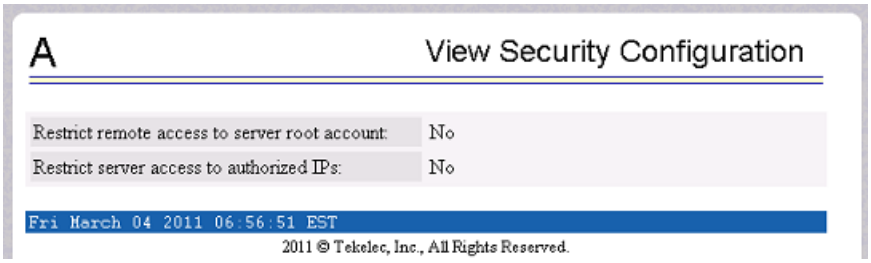

Figure 27: View Security Configuration

Change Security Configuration

This menu allows the user to change security access for EPAP server on which the GUI is open. The user can change the following two configurations:

- Restrict/Allow command line access to server root account.
- Restrict/Allow server access to only authorized IPs or to all.

Configuration will only be done on the server on which the GUI is open. To change configuration on mate, select mate from GUI and select **Maintenance EPAP Security Change Security Configuration**.

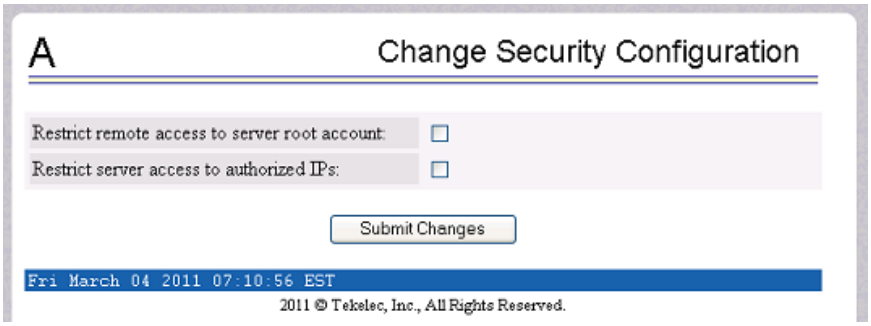

Figure 28: Change Security Configuration

RTDB Menu

The RTDB (Real-Time Database) Menu allows the user to interact with the RTDB for status, reloading, and updating.

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

- *View RTDB Status*
- *RTDB Menu - Maintenance*
- *Retrieve Records*

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.

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.

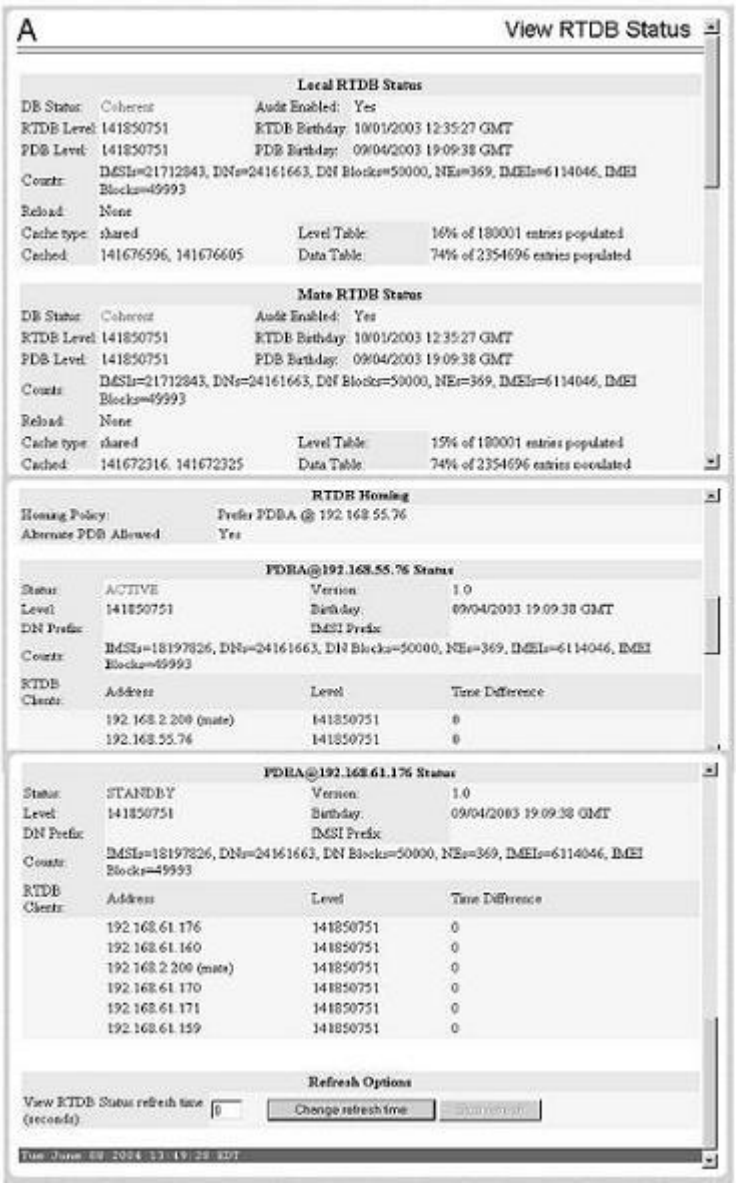

Figure 29: View RTDB Status Screen

RTDB Menu - 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.

The RTDB / Maintenance menu provides the following actions:

- *Reload RTDB from PDBA*
- *Reload RTDB from Remote*
- *Backup the RTDB*
- *Restore the RTDB*
- *PDBA / Maintenance / Configure PDBA Record Delay*

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.

Note: If the RTDBs have different birthdates (as a result of this reload), you must perform a Reload RTDB from Remote on the mate EPAP (see *Reload RTDB from Remote*). RTDBs with different birthdates may not take updates or update the Service Module cards.

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: the EPAP software must be stopped on both of the machines involved:

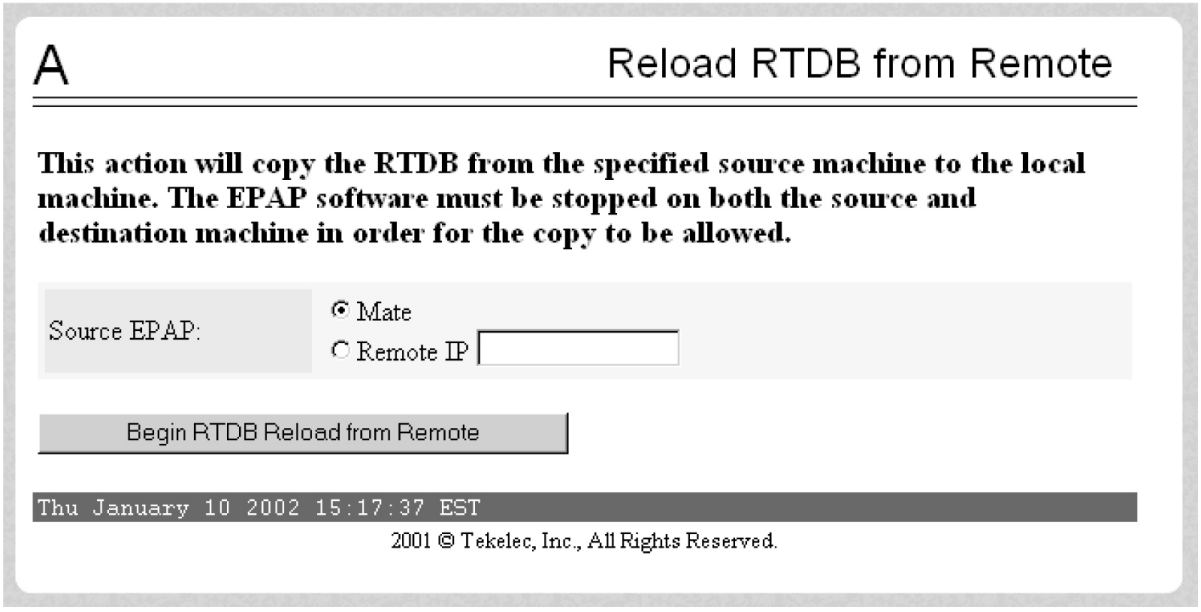

Figure 30: Reload RTDB from Remote Screen

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:

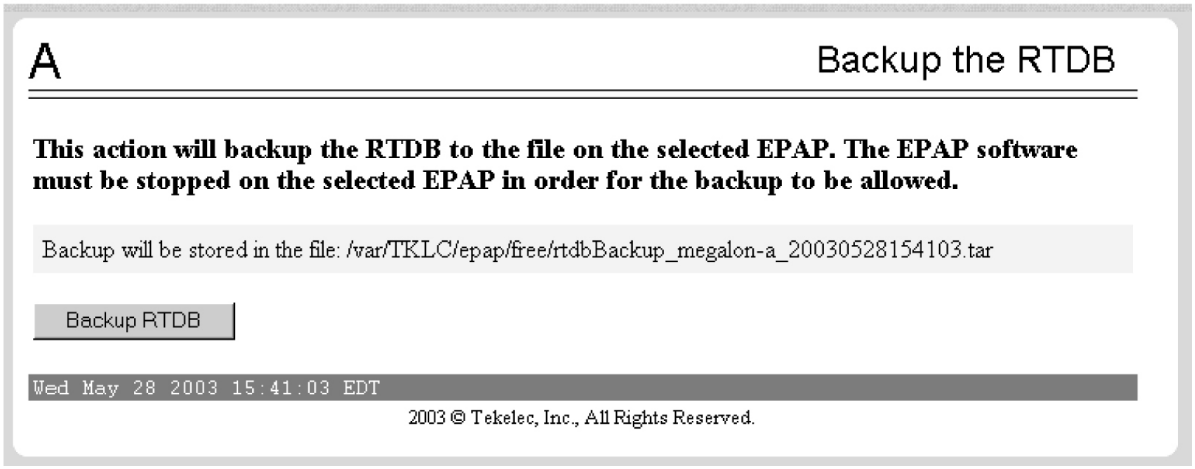

Figure 31: Backup the RTDB Screen

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.

Note: If the RTDBs have different birthdates (as a result of this restore), you must perform a Reload RTDB from Remote on the mate EPAP (see *Reload RTDB from Remote*). RTDBs with different birthdates may not take updates or update the Service Module cards.

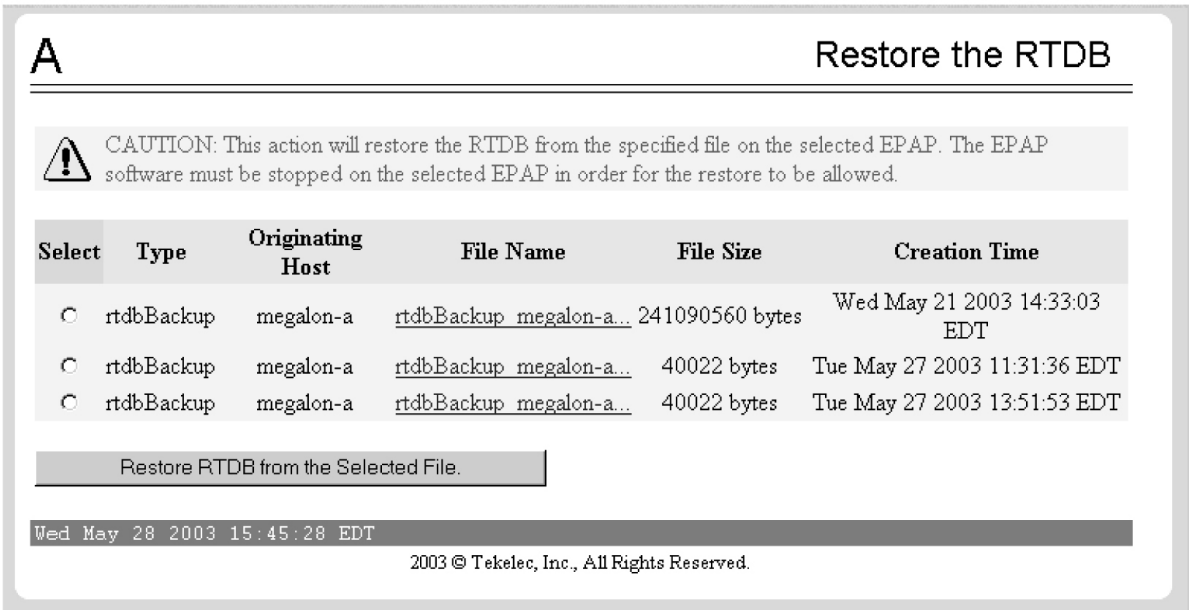

Figure 32: Restore the RTDB

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:

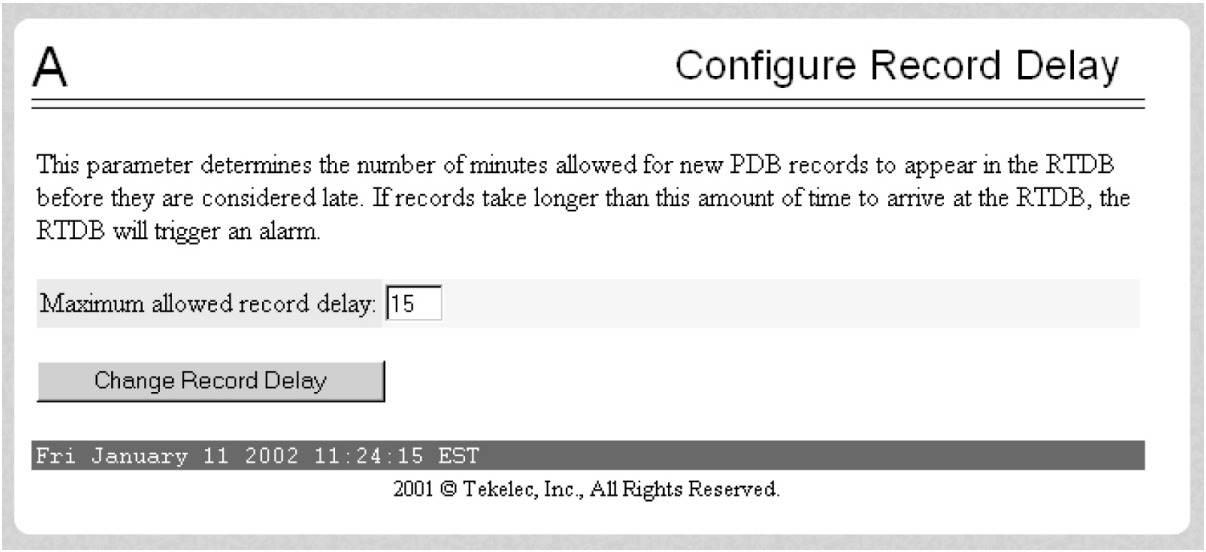

Figure 33: Configure Record Delay Screen

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:

The RTDB / Retrieve Records menu contains:

- *IMSI*
- *DN*
- *DN Block*
- *Network Entity*
- *IMEI*
- *IMEI Block*

IMSI

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

The output displays the following information about an IMSI:

- IMSI ID

- SP
- NE data for the Service Provider of the IMSI (see *Network Entity*)
- IMEI data if the IMSI being retrieved is associated with an IMEI (see *IMEI*)

DN

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

The output displays the following information about single DNs:

- ID
- Portability type (PT)
- Associated SP or RN
- Network Entity (NE) data (if the DN being retrieved is associated with up to 2 NEs)

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

DN Block

The RTDB / Retrieve Records / DN Block screen allows the user to retrieve information about about a DN block.

The output displays the following information about a block DN:

- First DN
- Last DN
- PT
- Associated SP or RN
- NE data (if the DN Block being retrieved is associated with up to 2 NEs)

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

Network Entity

The RTDB / Retrieve Records / Network Entity screen allows the user to retrieve information about a network entity:

The output displays the following information about a network entity:

- ID
- Type (RN, SP, VMS, GRN)
- 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

IMEI

The RTDB / Retrieve Records / IMSI screen allows the user to retrieve information about about an IMSI.

The output information displays:

- 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.

IMEI Block

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

The output information displays:

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

Debug Menu

The Debug Menu allows the user to view logs and list running processes.

The Debug menu actions are:

- *View Logs*
- *Capture Log Files*
- *Manage Logs and Backups*
- *View Any File*
- *List EPAP Software Processes*

View Logs

The Debug / View Logs menu allows `appuser` to view such logs as the Maintenance, RTDB, Provisioning, RTDB audit, and UI logs.

The View Logs menu options are:

- 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. Press the Open View Window button to activate the View Window viewer for the log file 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 password for the user `appuser`. 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.

Invoke the log viewer by pressing the Open View Window button. This opens the SSH User Authentication window. Only `appuser` can view logs. The `appuser` password is required to log in. The Log viewer appears in its own window. You can continue using the user interface while viewing the selected file.

Use the log viewer navigation commands in *Table 16: Log Viewer Navigation Commands* to navigate through the file displayed by the log viewer.

Table 16: 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 finished, close the Log Viewer window by clicking the Close View Window button.

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.

When you click the Capture Logs button, the copy of the log files occurs, and a successful completion message.

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 34: Manage Logs & Backups Screen* with an example of one recorded log file on the Manage Log Files screen.

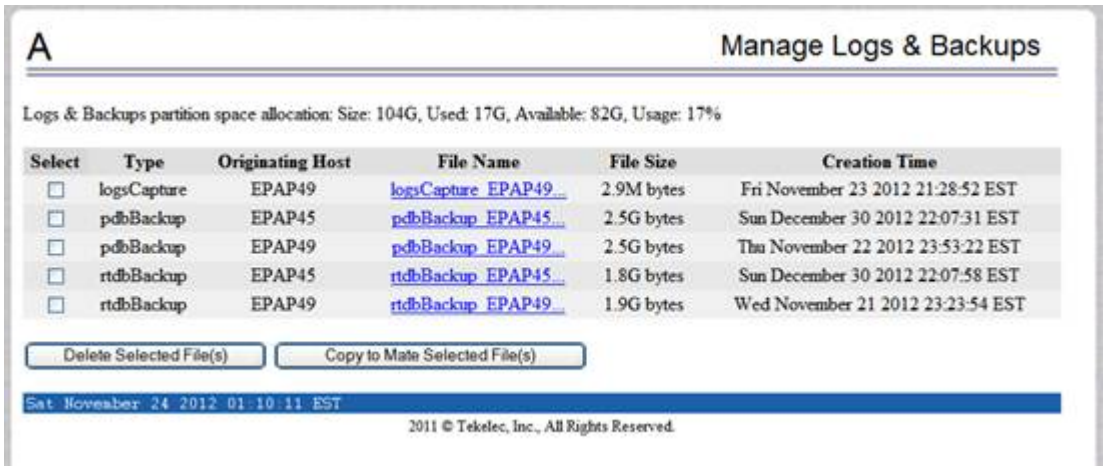

Figure 34: Manage Logs & Backups Screen

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.

View Any File

The View Any File screen allows the user to view any file on the system using the Log Viewer by entering the authorized passwoed for the user `appuser`. When the user enters a file, the Log Viewer is invoked.

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*.

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 35: Example of View Any File* shows an example of the format of the process list.

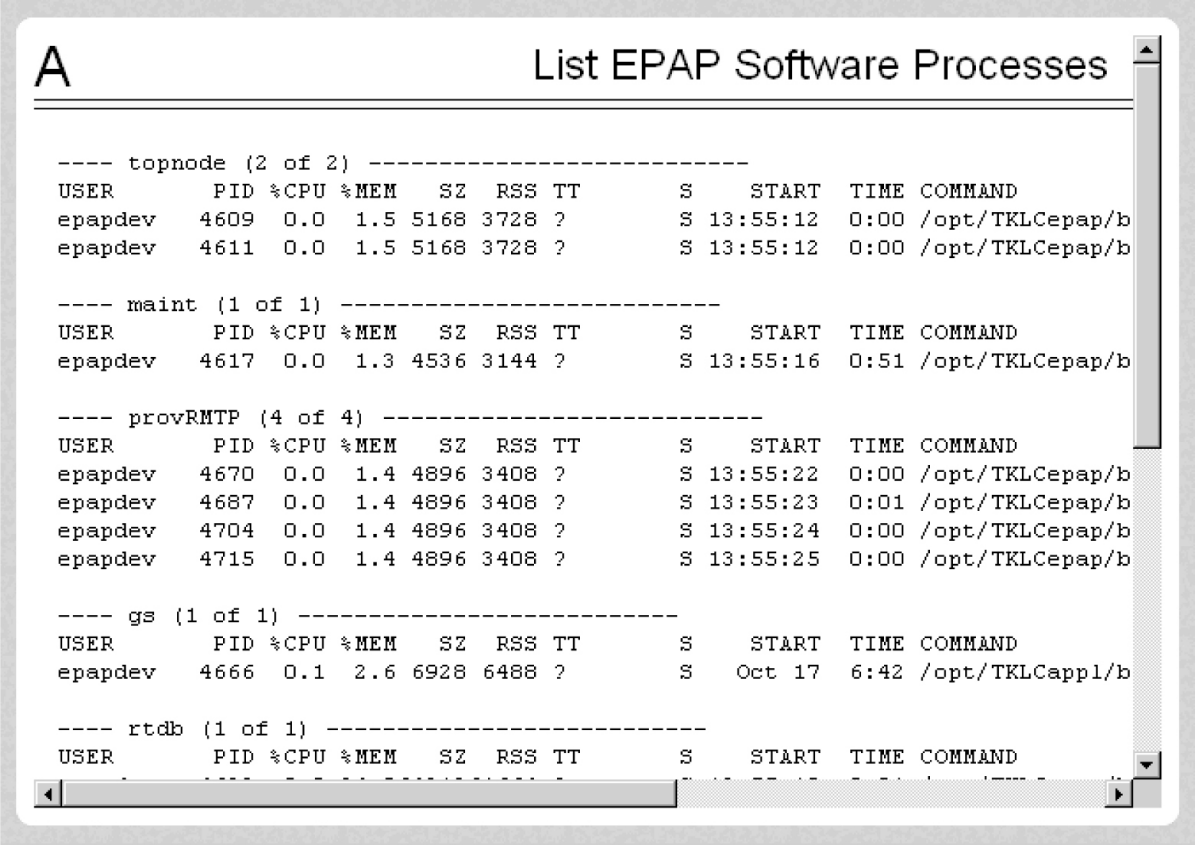

Figure 35: Example of View Any File

Platform Menu

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

The Platform menu provides these actions:

- *Run Health Check*
- *List All Running Processes*
- *View System Log*
- *Eject the CD*
- *Reboot the MPS*
- *Halt the MPS*
- *SSH to MPS*

Run Health Check

The Platform / Run Health Check screen allows the user to execute the health check routine on the selected EPAP. The *EPAP Alarms on the T1200 Platform* manual describes the health check in detail.

The first screen presented in the workspace frame lets the user select the “normal” or “verbose” mode of output detail.

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 *EPAP Alarms on the T1200 Platform* manual, System Health Check, for the functions performed and how to interpret the results of the normal outputs

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 36: List All Running Processes Screen* shows an example of the process list.

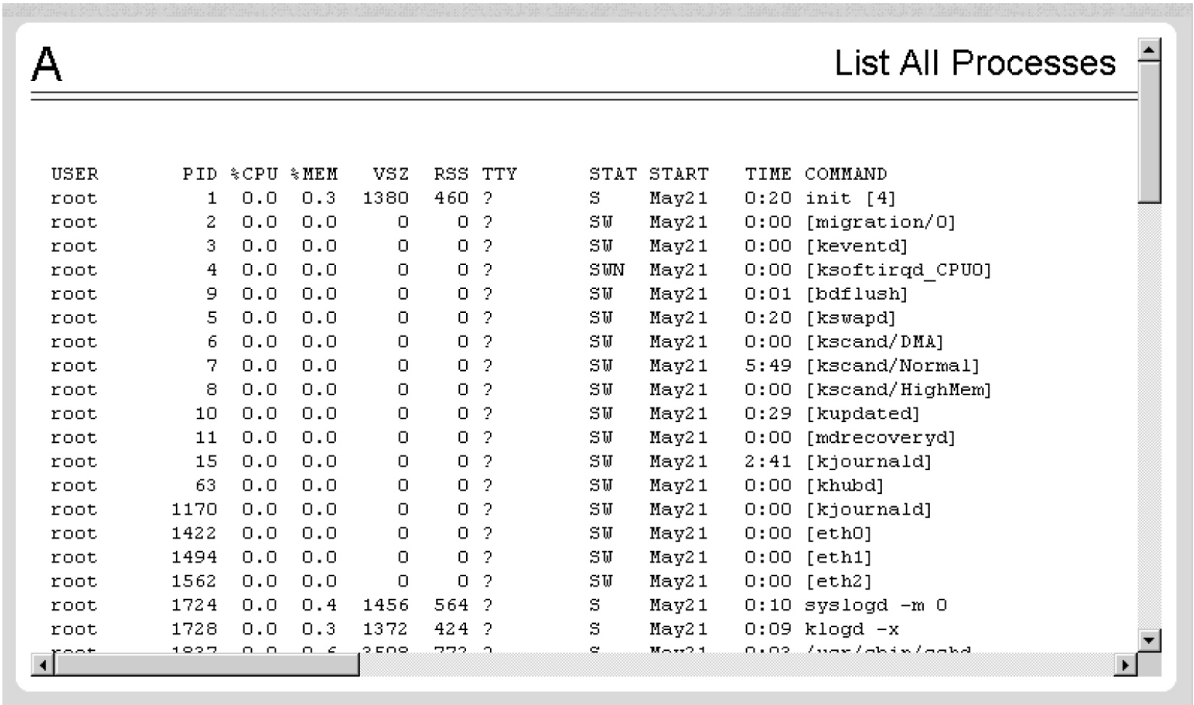

Figure 36: List All Running Processes Screen

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 is displayed. The user is required to enter the authorized password for the user `appuser`.

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*.

Eject the CD

The Platform / Eject the CD screen allows the user to eject the CD on the selected EPAP server.

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.

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.

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.

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. Initially, a Caution screen will display. Confirmation is required to halt the MPS.

To perform this action, click the halt_MPS button. A second 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 37: Caution about Halting the MPS* .

Figure 37: Caution about Halting the MPS

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. .

SSH to MPS

The Platform / SSH to MPS screen allows the user to have an SSH window to the user interface user. Clicking on the Connect button opens the SSH User Authentication window. A user name and password are required to log in. Only the IP address of the local EPAP is accepted when using SSH to MPS.

After a successful login, the SSH window opens and is used to perform SSH communications.

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.

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

- *Select Other PDBA*
- *Switchover PDBA Status*
- *Process Control*
- *View PDBA Status*
- *Manage Data*
- *Authorized IP List*
- *DSM Info*
- *PDBA / Maintenance*

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 3-190.

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 3-191.

Select Other PDBA

The PDBA / Select Other PDBA is an action performed from the PDBA menu screen. It provides access to the remote PDBA GUI.

Access the user interface on the remote PDBA. 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.

Notice that if only one PDBA is available, you are warned that the action can cause synchronization problems.

Process Control

The PDBA / Process Control menu lets you to start and stop the PDBA application.

The PDBA / Process Control menu provides these actions:

- *Start PDBA Software*
- *Stop PDBA Software*

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

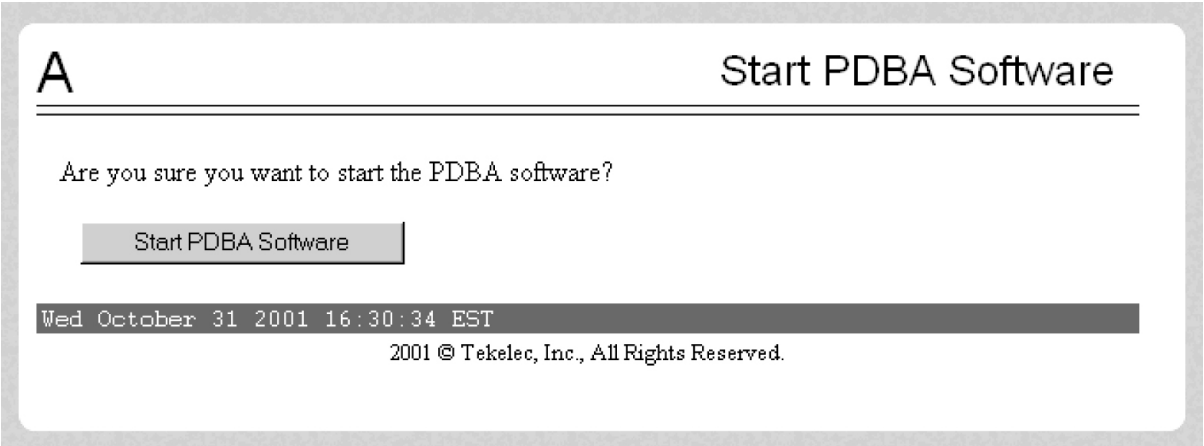

Figure 38: Start PDBA Software Screen

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.

Stop PDBA Software

The PDBA / Process Control / Stop PDBA Software screen stops the PDBA software.

The screen also has a checkbox that lets users specify whether PDBA is to be automatically restarted when the machine boots. Ifthis checkbox is selected, the software can only be restarted via the Start PDBA menu. .

The Stop PDBA Software button launches the successful stopping of the PDBA..

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.

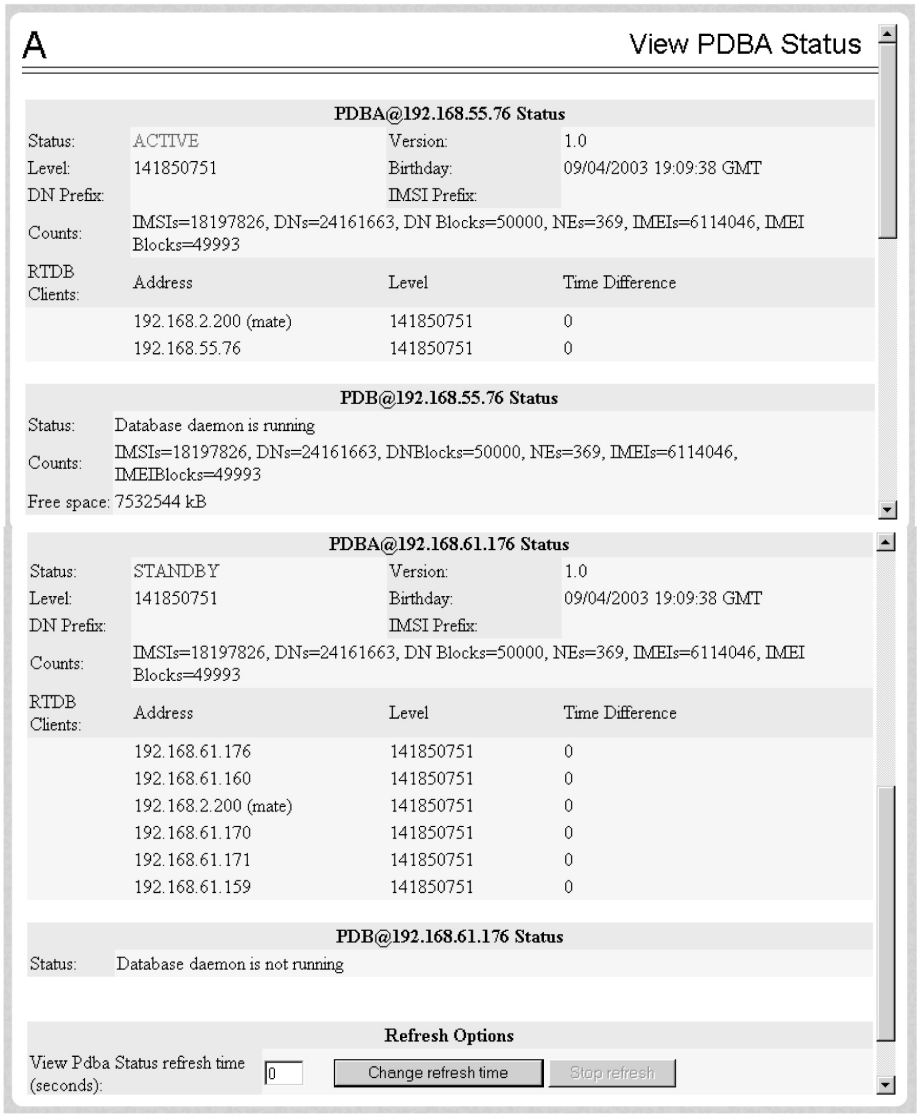

Figure 39: An Example PDBA Status Screen

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).

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*
- *IMSI Range*
- *Dialed Numbers (DN)*
- *DN Block*
- *Network Entity*
- *Individual IMEI*
- *Block IMEI*
- *Send Raw PDBI Command*
- *EPAP Provisioning Blacklist Menu*

IMSI

The PDBA / Manage Data / menu is used to add, update, delete, and view subscriptions in the Provisioning Database (PDB).

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

- *Add an IMSI*
- *Update an IMSI*
- *Delete an IMSI*
- *Retrieve an IMSI*

Add an IMSI

The PDBA / Manage Data / IMSI / Add an IMSI screen promptsthe user for the fields needed to add an IMSI to the Provisioning Database (PDB). If there is a conflicting subscription in the PDB,the user is prompted to confirm before overwriting the existing subscription.

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).

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)..

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 40: Retrieve IMSI Screen 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.

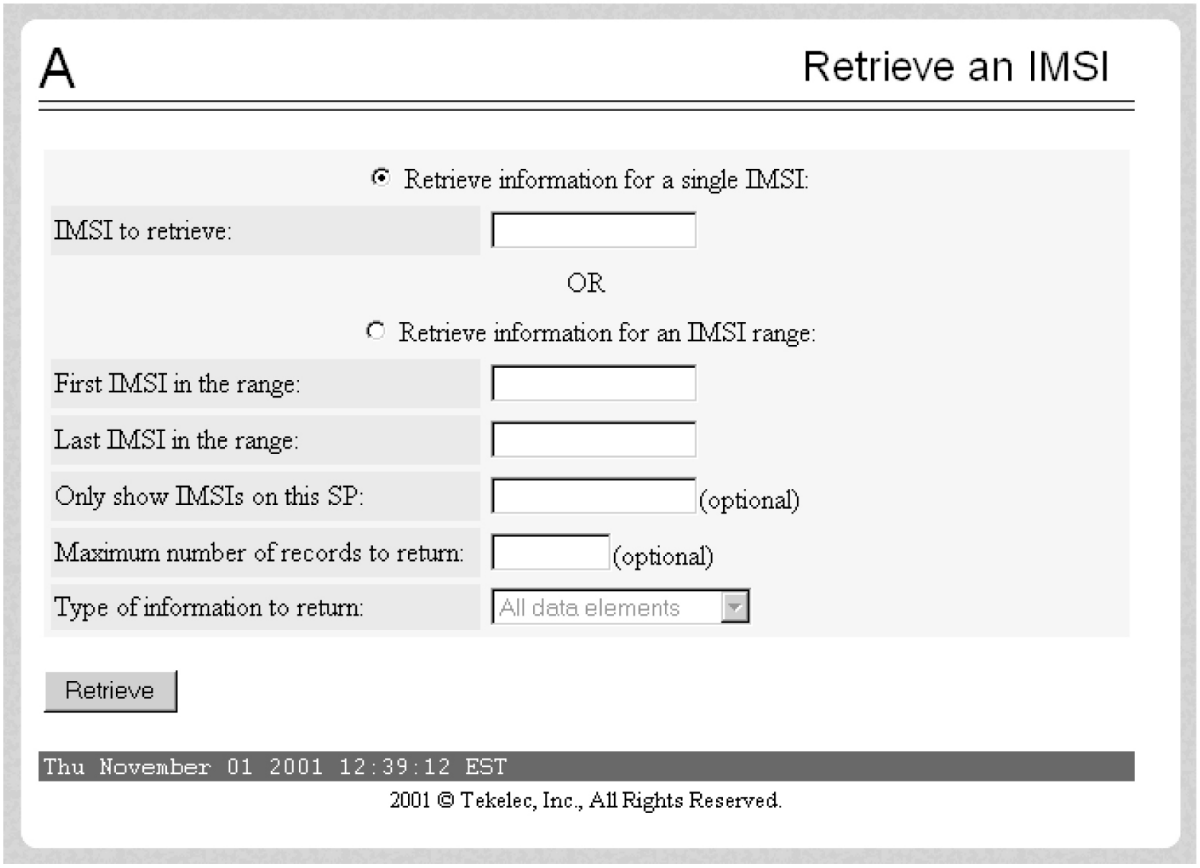

Figure 40: Retrieve IMSI Screen

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).

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

- *Add an IMSI Range*
- *Update an IMSI Range*
- *Delete an IMSI Range*
- *Retrieve an IMSI Range*

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).

Note: This screen is only operational to SOG customers.

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).

Note: This screen is only operational to SOG customers.

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).

Note: This screen is only operational to SOG customers.

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.

Note: This screen is only operational to SOG customers.

Dialed Numbers (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.

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

- *Add a DN*
- *Update a DN*
- *Delete a DN*
- *Retrieve a DN*

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 41: Add a DN Screen* for an example of the Add a DN screen.

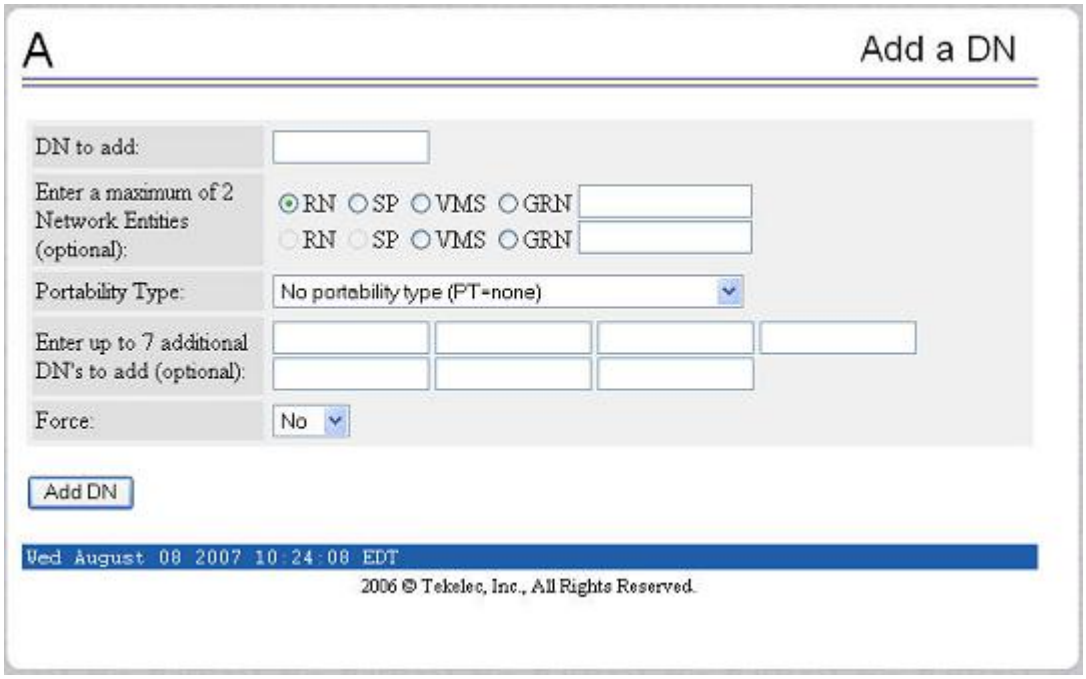

Figure 41: Add a DN Screen

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 42: Update a DN Screen* for an example of the Update a DN menu.

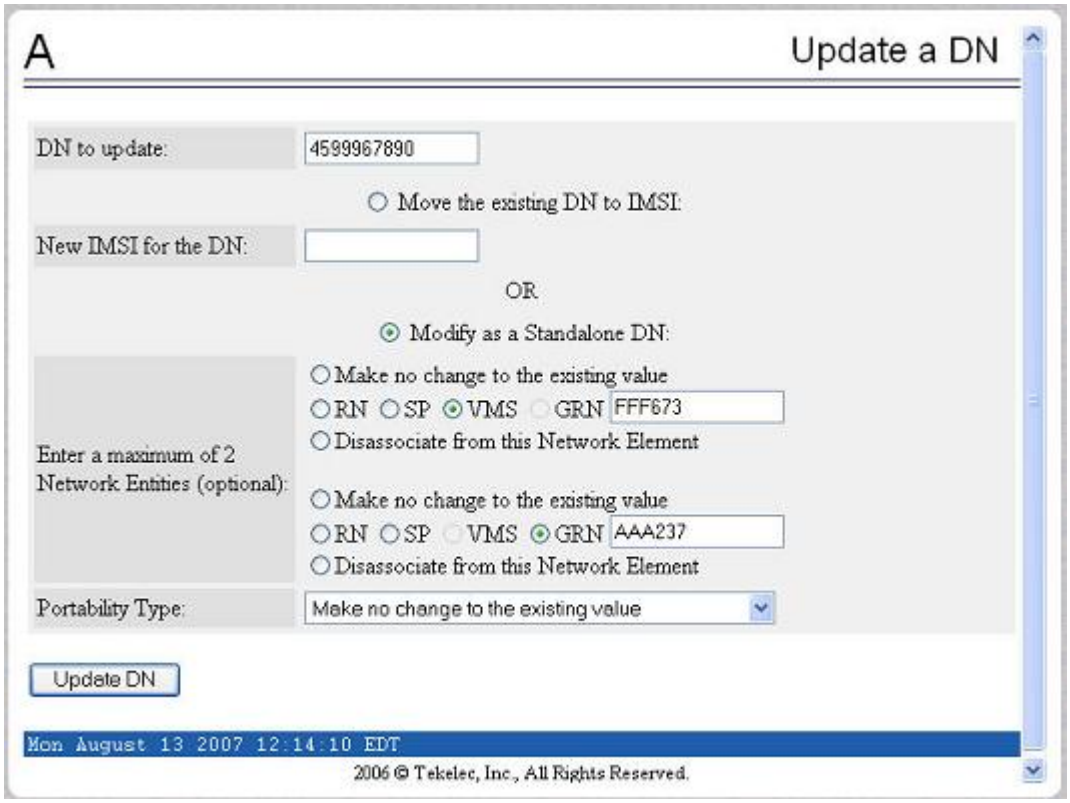

Figure 42: Update a DN Screen

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).

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.

DN Block

The PDBA / Manage Data / DNBlock 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.

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

- *Add a DN Block*
- *Update a DN Block*
- *Delete a DN Block*
- *Retrieve DN Blocks*

Add a DN Block

The PDBA / Manage Data / DNBlock / 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.

Update a DN Block

The PDBA / Manage Data / DNBlock / 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)..

Delete a DN Block

The PDBA / Manage Data / DNBlock / Delete a DN Block screen prompts the user for the fields necessary to remove a DN block from the Provisioning Database (PDB).

Retrieve DN Blocks

The PDBA / Manage Data / DNBlock / 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.

Network Entity

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

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

- *Add Network Entity*
- *Update Network Entity*
- *Delete Network Entity*
- *Retrieve Network Entity*

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 43: Add an NE Screen* for an example of the Add an NE screen.

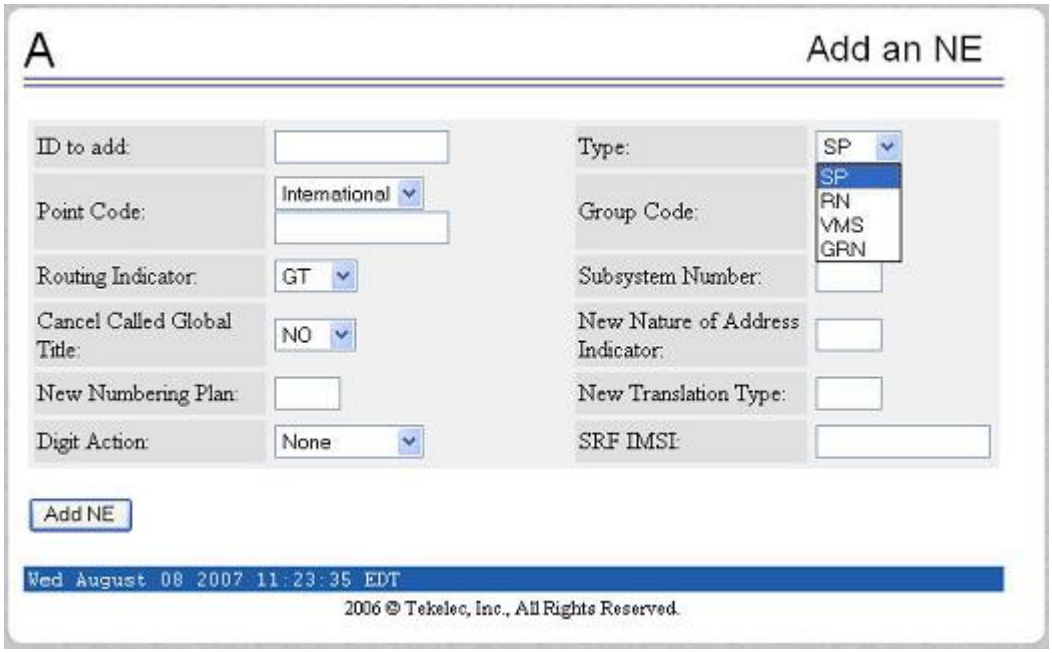

Figure 43: Add an NE Screen

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).

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).

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 44: Retrieve an NE Screen* for an example of the Retrieve an NE screen.

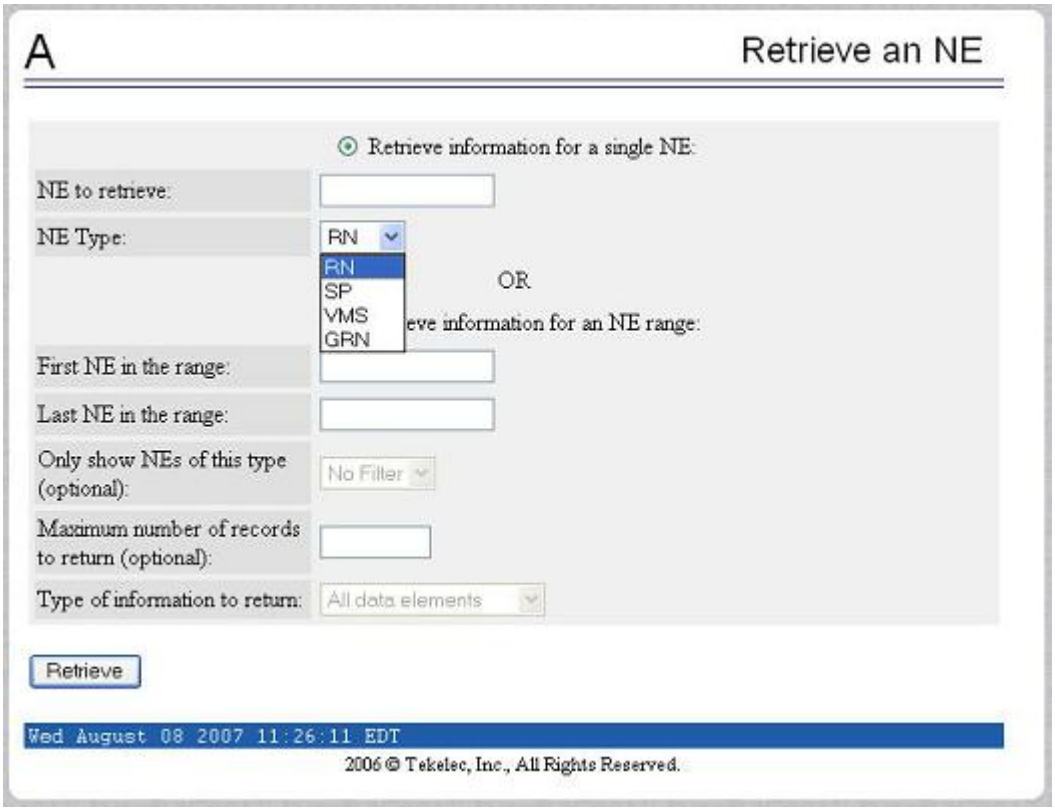

Figure 44: Retrieve an NE Screen

Individual IMEI

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

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

- *Add an IMEI*
- *Update an IMEI*
- *Delete an IMEI*
- *Retrieve an IMEI*

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 45: Add an IMEI Screen* for an example of the Add a IMEI screen.

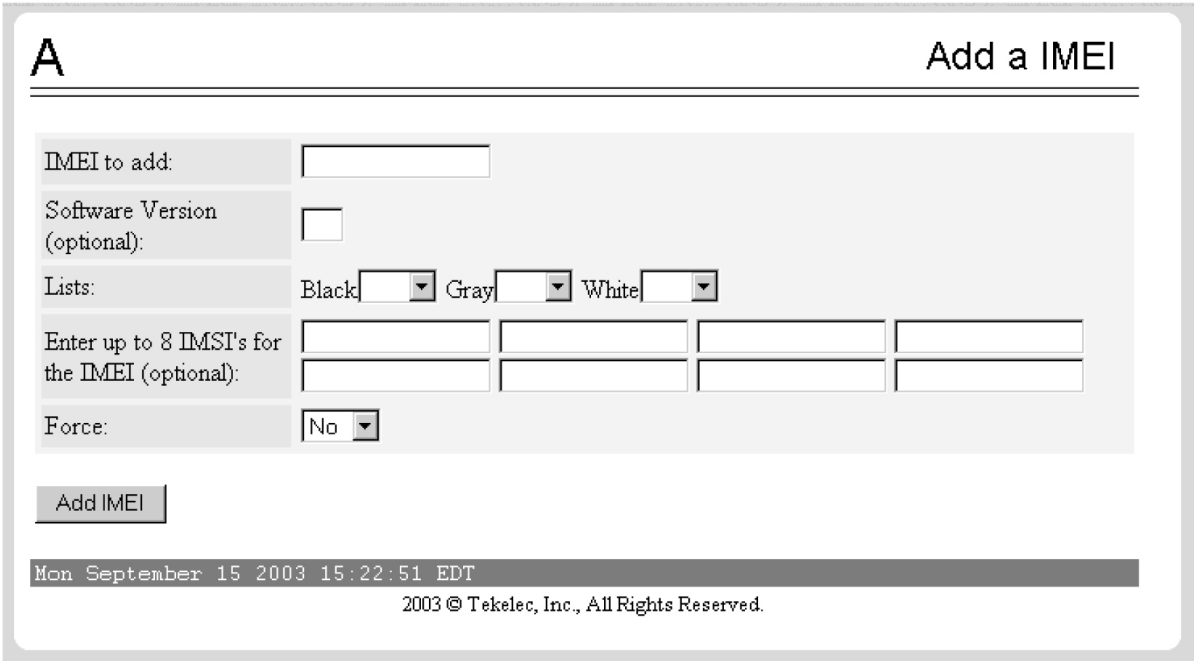

Figure 45: Add an IMEI Screen

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.

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.

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 filter:
  - 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 46: Retrieve an IMEI Screen* for an example of the Retrieve a IMEI screen.

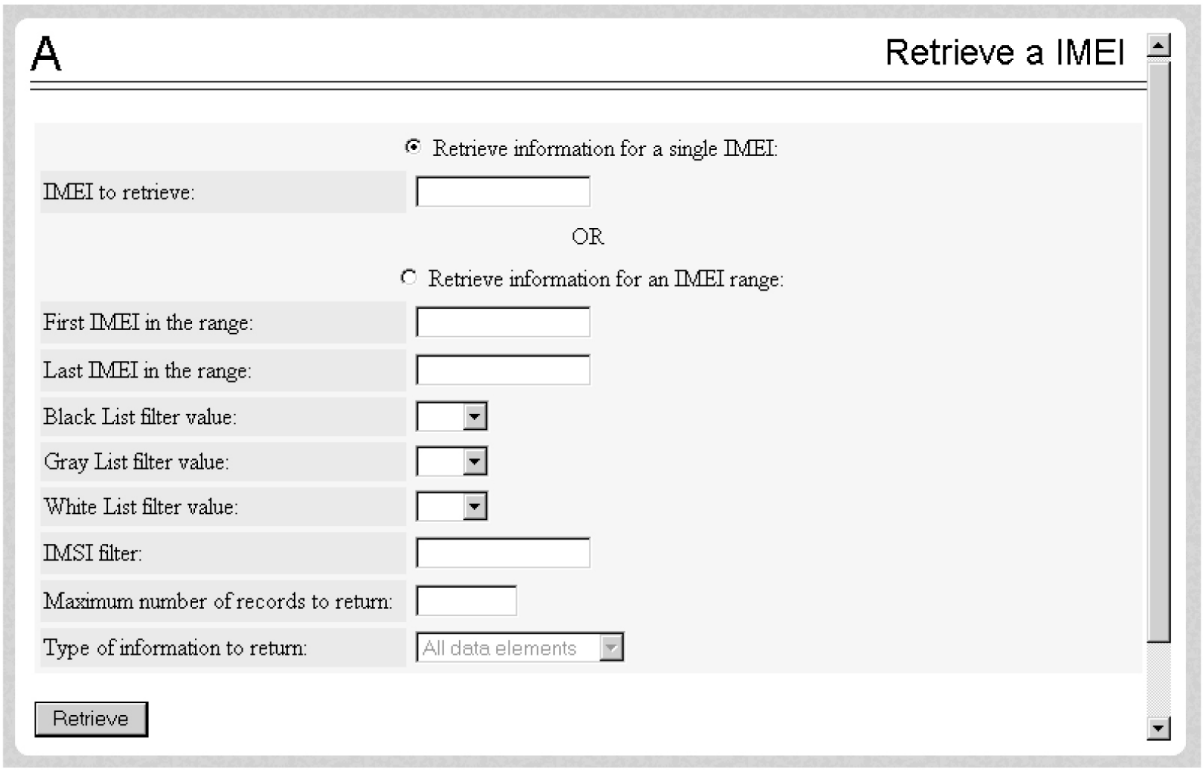

Figure 46: Retrieve an IMEI Screen

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).

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

- *Add an IMEI Block*
- *Update an IMEI Block*
- *Delete an IMEI Block*
- *Retrieve an IMEI Block*

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.

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.

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.

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:

Send Raw PDBI Command

The PDBA / Manage Data / Send Raw PDBI Command screen allows only the `epapdev` user to 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.

A socket connection to the PDBI is available; however, all other functions, including creating and ending transactions, must be entered manually. For additional information about the PDBI commands, refer to *EAGLE Provisioning Database Interface Manual*.

Press the Start PDBI Connection button, and a new window appears with the PDBI connection. The `epapdev` user password must be entered.

The session may be closed 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).

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

- *Add Provisioning Blacklist*
- *Delete Provisioning Blacklist*
- *Retrieve Provisioning Blacklist*

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. Specific 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.

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.

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.

Authorized IP List

The PDBA / Authorized IP List menu allows you add, modify, remove, and list the IP addresses authorized to connect to the PDBA through the Provisioning Database (PDB). This menu also allows 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.

For more information about SSH tunneling, refer to the Provisioning Database Interface Manual. The PDBA / Authorized IP List menu provides these actions:

- *Add Authorized IP*
- *Modify Authorized IP*
- *Remove Authorized IP*
- *List All Authorized IPs*

Add Authorized IP

The PDBA / Authorized IP List / Add Authorized PDBA Client IP screen allows you to:

- Add an IP address to the list of authorized IP addresses
- Specify a **Permission Type** of Read or Write for that IP address
- Decide if an SSH (secure shell) tunnel should be created between that IP address and the EPAP
- Specify a username, password, and port number to use on the machine represented by the IP address

.

Modify Authorized IP

The PDBA / Authorized IP List / **Modify Authorized PDBA Client IP** screen allows you to:

- Change the **Permission Type** of an authorized PDBA client IP address
- Decide to change SSH tunnel status
- Change username, password, and port number

To modify an authorized PDBA client IP address:

1. Enter an IP address in the **IP to modify** field
2. Select a **Permission Type**
3. Make a selection for the **Client User Information** checkbox
4. Enter username, password, or port number
5. Click the **Modify IP** button

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

Remove Authorized IP

The PDBA / Authorized IP List / Remove Authorized PDBA Client IP screen allows 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.

To remove an authorized PDBA client IP address, enter the desired IP address in the **IP to remove:** field, and click the **Remove IP** button.

When the removal of the IP address is accepted, a message appears indicating a successful completion of the action.

List All Authorized IPs

The PDBA / Authorized IP List / List All Authorized PDBA Client IPs screen allows you display all authorized IP addresses.

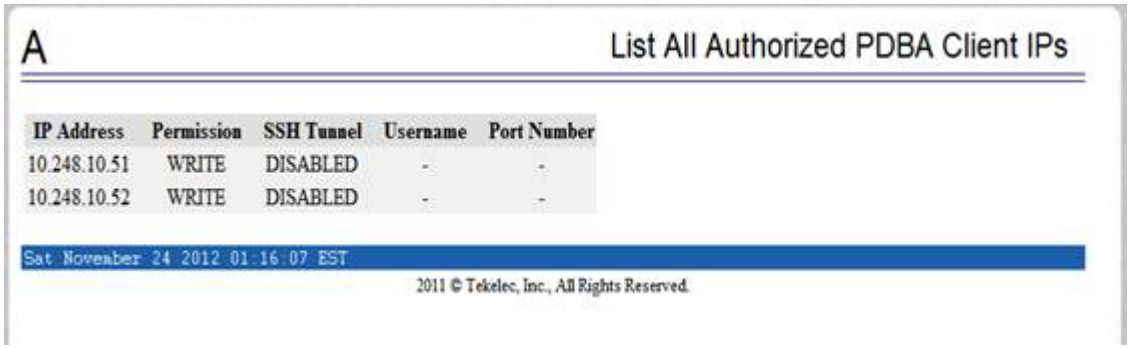

Figure 47: List All Authorized PDBA Client IPs Screen

DSM Info

The PDBA / DSM Info menu is used to request information on the Service Module cards in the network.

The PDBA / DSM Info menu provides these actions:

- *PDBA DSM Report*
- *PDBA DSM List*

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 Service Module cards. Or the user can provide a specific level to get the percentage of cards that have received that level. A list of the Service Module cards that were behind the level mentioned in the response can be provided in the report as well. See *Figure 48: PDBA DSM Report Screen* for the PDBA DSM Report screen.

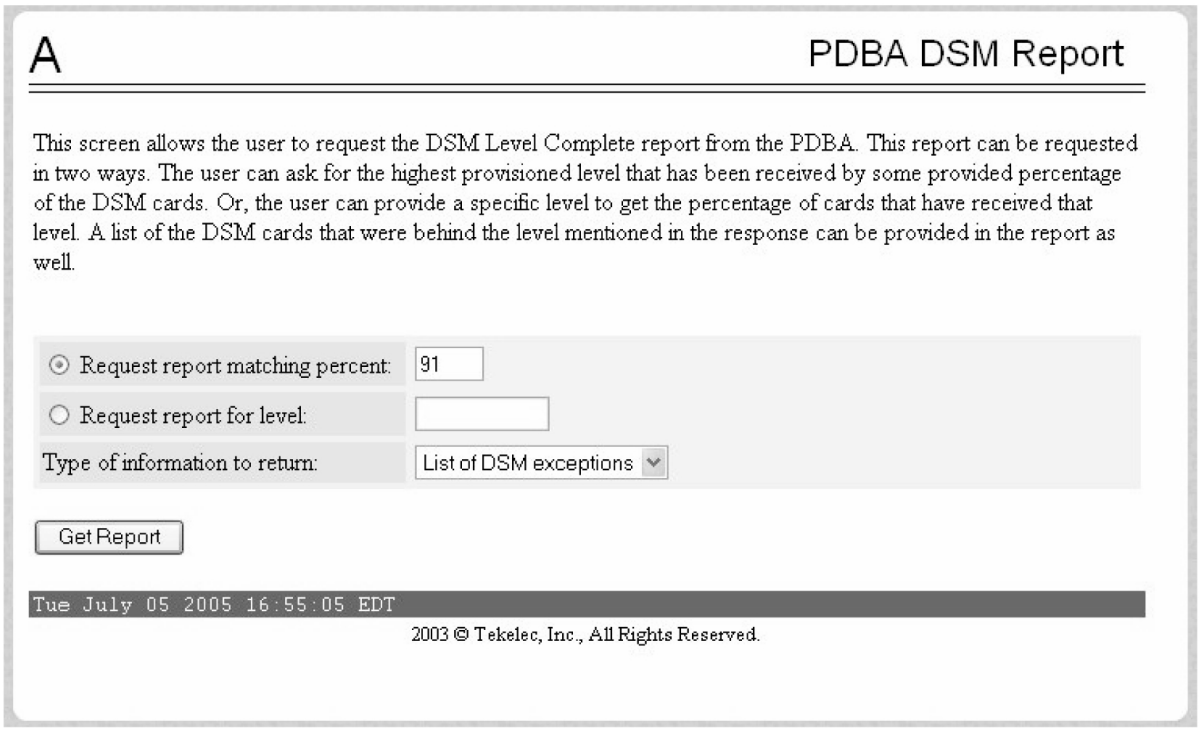

Figure 48: PDBA DSM Report Screen

PDBA DSM List

This screen retrieves all of the information that the PDBA has on all of the Service Module cards in the network. Two fields are provided to filter the list of Service Module cards returned. A third field is provided to limit the amount of information returned for each Service Module card. Refer to *Figure 49: PDBA DSM Info List Screen (with Status filter pulldown)* for an example of the PDBA DSM Info List.

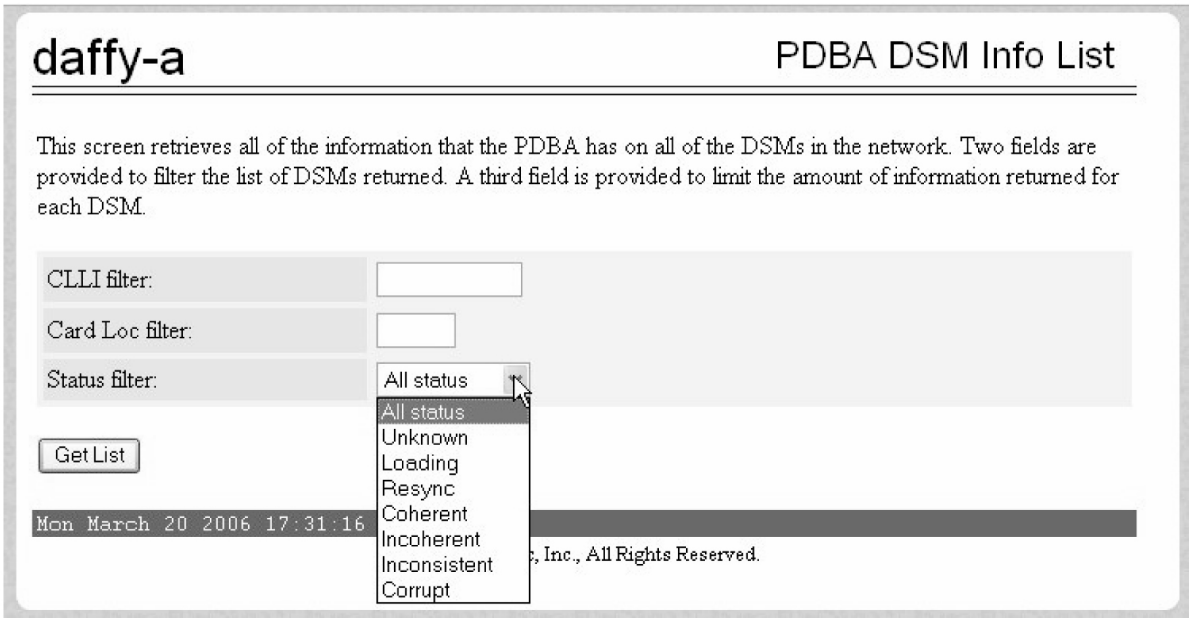

Figure 49: PDBA DSM Info List Screen (with Status filter pulldown)

PDBA / Maintenance

The PDBA / Maintenance menu lets you perform various PDB maintenance operations for the Provisioning Database (PDB).

The PDBA / Maintenance menu provides these actions:

- *PDBA / Maintenance / Backup*
- *PDBA / Maintenance / Import File to PDB*
- *PDBA / Maintenance / Export PDB to File*
- *PDBA / Maintenance / Transaction Log Params*
- *PDBA / Maintenance / Number Prefixes*
- *PDBA / Maintenance / Logs*
- *PDBA / Maintenance / Schedule PDB Export*
- *PDBA / Maintenance / Configure PDBA Record Delay*

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.

The PDBA / Maintenance / Backup menu provides these actions:

- *List Backups*
- *Backup the PDB*
- *Restore the PDB*

List Backups

The PDBA / Maintenance / Backup / List PDB Backups screen lists the details of the backup. See *Figure 50: List PDB Backups Screen* for an example of the List PDB Backups screen.

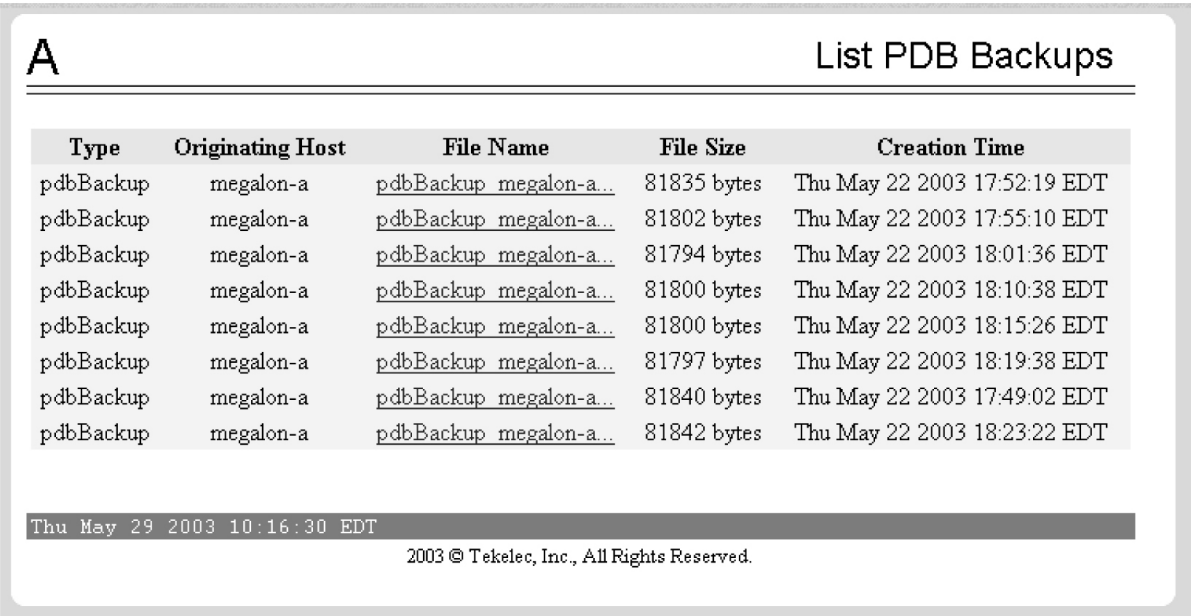

Figure 50: List PDB Backups Screen

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 completed successful backup results in the Banner Message Window.

Restore the PDB

rwb: update screen when Rhew/Rice repair it - already PRed

The PDBA / Maintenance / Backup / Restore the PDB screen lets you restore the PDB (Provisioning Database) from a previous backup.

This screen is used in the *Restoring the PDB* procedure in the *EPAP Alarms on the T1200 Platform*.

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

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

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 Technical Services for information and assistance; see *Customer Care Center* for more information.

Although the input file is normally generated by the customer's provisioning application, the *PDBA / Maintenance / Export PDB to File* action also generates a file suitable for importing with this command.

A caution screen will be displayed. Click Continue to access the Import File screen.

Specify the path and name of the file to import, and click the Import button.

For additional information on 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* .

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>`.

When you want to export a PDB to File, click the Continue button, .

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 / Transaction Log Params menu lets you view and change the parameters of the transaction log for a file to which it can export the PDB.

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

- *View Params*
- *Change Params*

View Params

The PDBA / Maintenance / Transaction 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.

Change Params

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

Parameters that control when the PDBA removes old transaction log records can be customized. (Transaction log records are the records of PDBA responses to RTDB update requests.) 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 only retrieve that information through a complete reload. Therefore, change these values only if you are certain.

Enter the maximum number of transactions log record and the maximum number of minutes to keep record. The maximum number is '-1'.

When you change either the number of records or number of minutes to keep in the Transaction Log, click the Change Parameters button. A confirmation screen will be displayed.

PDBA / Maintenance / Number Prefixes

The PDBA / Maintenance / Number Prefixes menu lets you view and change the parameters of the PDBA prefixes.

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*
- *Change Prefixes*

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

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*.

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.

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. The user is required to enter the authorized password for the user `appuser` to view the system logs.

Note: The contents of these logs are intended for the use by *Customer Care Center* in diagnosing system operation and problems. If assistance is required, contact *Customer Care Center* for more information.

The PDBA / Maintenance / Logs menu provides these actions:

- *View Command Log*
- *View Debug Log*
- *View Error Log*
- *Set Log Levels*

View Command Log

The PDBA / Maintenance / Logs / View Command Log menu selection lets you view the current PDBA Command Log. To view historic PDBA command logs, use the View Any File action. Refer to *View Any File* .

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* .

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* .

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.

Note: The levels for error, command and debug logs should be set only under the guidance of Technical Services. See *Customer Care Center* 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 toe 365) on specific 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 support 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.

Figure 51: Schedule PDB Export Screen is an example of the Schedule PDB Export screen.

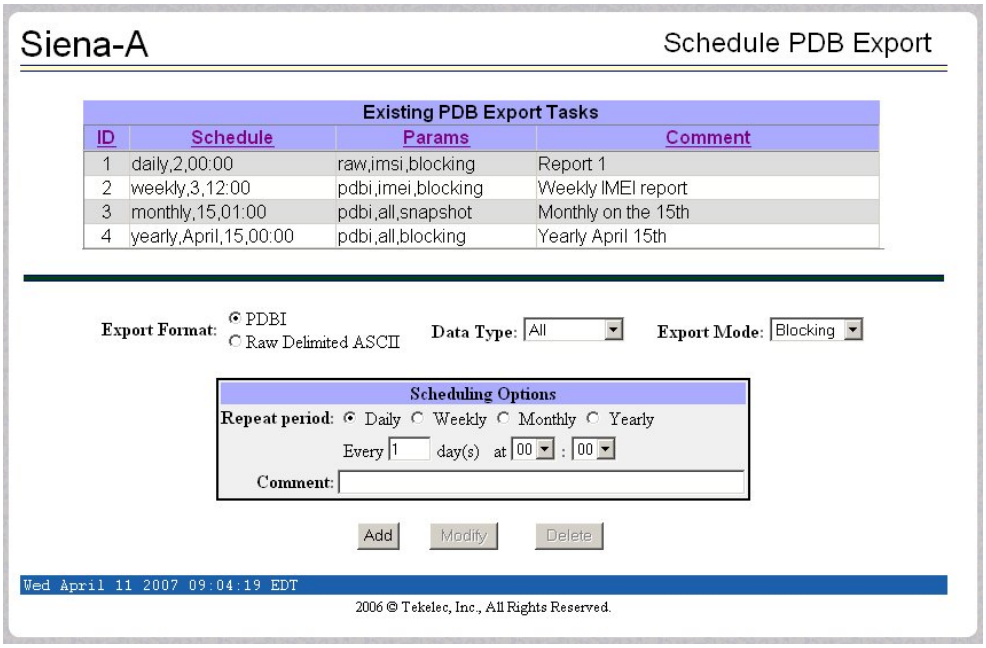

Figure 51: Schedule PDB Export Screen

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 **Repeat Period** radio button 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*):

Repeat period: 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.

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*).

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.

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.

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.)

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.

Add, Modify, and Delete Buttons

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

Add 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 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 **Modify** 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 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.

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.

A successful log into the UI provides the user with an open session. 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*
- *Groups*
- *Authorized IPs*
- *Terminate UI Sessions*
- *Modify Defaults*

Users

The User Administration / Users menu allows the system administrator to administer users functions such as add, modify, delete, retrieve, and reset user password.

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 17: EPAP UI Logins* for the current login names.

Table 17: 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 provides these capabilities:

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

Add User

The User Administration / Users / Add UI User screen is used to add a new user interface user name and a default password. A succesful entry will generate a confirmation screen.

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.

After selecting a User Name, the user permissions screen appears. 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.

After modifying any entries, click the Submit Profile Changes button. The Modify Group Membership screen appears, allowing the user to customize individual access to groups. Click Sumbit Group Membership Changes when finished. A confirmation screen will appear.

Clicking the Modify Specific Actions button displays Action Privileges to specify for the user being modified. See *Figure 52: Modify UI User's Specific Actions*.

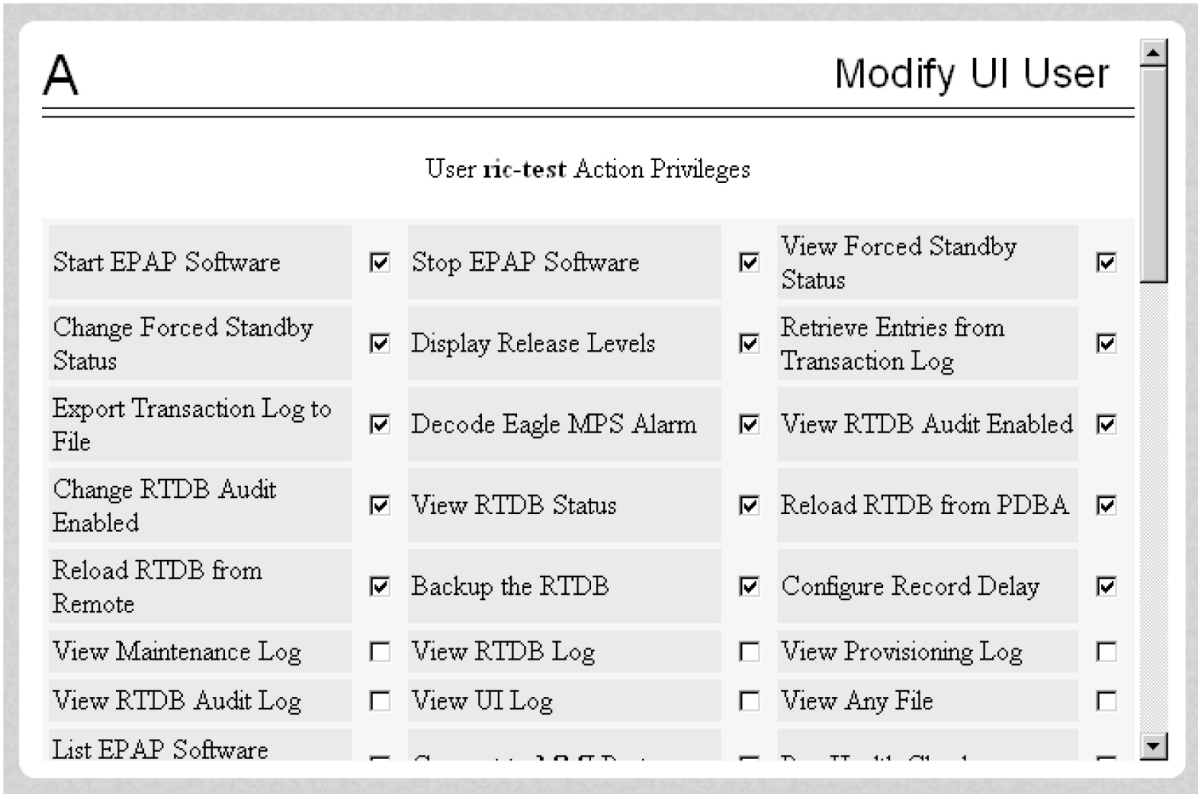

Figure 52: Modify UI User's Specific Actions

This screen contains many selections from which to choose. After customizing the settings, click the Submit Specific Action Changes at the bottom of the screen.

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.The system will generate a confirmation of the change for the user.

Delete User

The User Administration / Users / Delete UI User screen lets an administrator remove a user name from the list of user interface names. The screen is similar to Modifying UI User. First you select the user name to be deleted and click the Delete User button. A confirmation screen will appear, requesting approval of the change.

After confirmation, a success screen is generated.

Retrieve User

The User Administration / Users / Retrieve UI User screen displays the user name permission profiles from the user interface information.

The screen to view the user permissions appears, only displays the permissions allowed to that 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).

Additional information can be viewed by clicking the View Group Membership button.

Clicking the View Specific Actions in the Retrieve UI User screen displays the user privileges. This screen contains many privileges to display.

The bottom of the User Privileges screen may 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.

Reset Password

The User Administration / Users / Reset User Password screen changes the password for a user name.

A confirmation screen appears when you correctly update the user's password

Groups

The User Administration / Groups menu allows the user to administer group functions such as add, modify, delete, and retrieve.

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 allows:

- *Add Group*
- *Modify Group*
- *Delete Group*
- *Retrieve Group*

Add Group

The User Administration / Groups / Add UI Group screen lets you enter a new group and assign action privileges with the new group.

After a successful group added message, designate 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.

When the group is selected, the Modify Group Permission Profiles screen shows the current action privileges assigned to the group.

Specify the Action Privileges to assign to this group and click the Submit Specific Action Changes. A confirmation screen will be generated.

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. If a group is part of the New User Default Groups (*Modify Defaults*) , then the group cannot be deleted unless it is removed from the New User Default Groups list.

Clicking the Select Group button causes a confirmation banner and button appear. Click the Confirm Delete Group button to delete the group name and its permissions.

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.

After you select a Group Name in the screen above, the screen to view the group permissions appears. There you can view the permissions allowed to this group.

Authorized IPs

The User Administration / Authorized IP menu lets you add, remove, and list all authorized IP addresses and also change the IP address authorization status. The IP addresses are authorized for both GUI and server access.

The User Administration / Authorized IP List menu provides these actions:

- *Add Authorized IP*
- *Remove Authorized IP*
- *List All Authorized IPs*
- *Change UI IP Authorization Status*

Add Authorized IP

The User Administration / Authorized IP / Add Authorized IP screen lets you add a new individual IP address or CIDR format to the list of authorized IP addresses. Note that a pop-up syntax box appears when the cursor is positioned over the input field.

Enter the IP address you want authorized and press the Allow IP button.

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 (more than 1000) or when any internal failure is detected.

Remove Authorized IP

The User Administration / Authorized IP / Remove Authorized 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. .

When the authorized IP address is deleted, a message confirming the removal of the specified address is displayed..

List All Authorized IPs

The User Administration / Authorized IP / List All Authorized IPs screen retrieves and displays all authorized IP addresses. The screen also shows whether the authorization list is Enabled or Disabled.

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

Change UI IP Authorization Status

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

When this menu option is chosen, the current authorization state is displayed in the INFO field.

To toggle the state from not Enabled to Enabled, click the Enable IP Checking button.

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

Terminate UI Sessions

The User Administration / Terminate Active UI Sessions screen allows the administrator to selectively close individual active sessions.

Modify Defaults

The User Administration / Modify System Defaults screen allows the administrator to manage the systems defaults. The System Defaults which can be modified are:

- **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. The range is from 3 to 99. The default is 5.
- **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 the user to change the password. The range is from 1 to 180 days. The default value is 180.
- **Minimum Password Length:** This field represents the minimum password length for all users.
- **Password Expiry Warning Days:** This field represents the number of days that a user will be warned before the user's password expires. The range is from 0 to 6 days. A value of 0 disables the Password Expiry Warning. The default value is 7. The warning is displayed on the EPAP work area after a user successfully logs in to the EPAP GUI.
- **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:

  ```
  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:

  ```
  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). The refresh time is set to 5 if a value of 1 through 4 is entered.

When you complete the changes to the Modify System Defaults, click the Submit Defaults button.

Change Password

The Change Password screen provides EPAP users the capability to change their passwordsd. This basic action is available to all users and is accessible from the main menu (*Figure 19: EPAP Menu*).

To change the password, the current password must be entered, then the new password is entered. The new password is confirmed by retyping the new password and clicking the **Set Password** button.

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. A password is required to log in to the user interface.

These rules govern EPAP passwords.

- **Complexity**: Passwords complexity rules are defined as follows.
  - The user password must be at least eight characters in length.
  - The user password must not exceed 100 characters in length.
  - The user password must include at least one alpha character.
  - The user password must include at least one numeric character.
  - The user password must include at least one special punctuation character: question mark (?), period (.), exclamation point (!), comma (,), or semicolon (;).
  - The user password must not contain three or more of the same alphanumeric or special punctuation character in a row.
  - The user password must not contain three or more consecutive ascending alphanumeric characters in a row.
  - The user password must not contain three or more consecutive descending alphanumeric characters in a row.
  - The user password must not contain the user account name (login name).
  - The user password must not contain the user account name in reverse character order.
  - The user password must not be blank or null.
  - The user password must not be a default password.
- **Aging:** Users can be forced to change their passwords after a certain number of days. The administrator can set a maximum password age of up to 180 days as a default for the system. The administrator can also specify a different maximum password age for any individual user.
- **Force Change on Initial Login:** Users can be forced to change their password the first time that they log in. The administrator can assign a password to a user, either when the user is first created or when the password of an existing user is reset; the user must change the password the first time that the user 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 from 3 to 99, with a default value of 5.

Logout

The Logout menu selection confirms logging out of the current session. This basic action is available to all users and is accessible from the main menu (*Figure 19: EPAP Menu*).

On logout, you are notified by the screen notifies that this terminates your current session and ofers the opportunity to continue or not. Click the Logout button to complete the logout.

After logout, the screen returns to the screen showing the Tekelec EPAP User Interface login.

Chapter 4

Messages, Alarms, and Status Processing

Topics:

This chapter provides a description of EPAP messages, alarms, and status processing.

EPAP Messages

This section includes *Table 18: EPAP Error Messages* and *Table 19: EPAP Informational Banner Messages* .

For alarm-related banner messages that appear on the UI browser screen in the Message Box described in *EPAP GUI Main Screen*, refer to *EPAP Alarms on the T1200 Platform* for alarm recovery procedures.

EPAP Error Messages

Table 18: EPAP Error Messages lists the error codes and associated text that are generated by the EPAP user interface. The <> fields indicate values that are different for each error; the fields are filled at run time.

Table 18: EPAP Error Messages

E0047	Cmd Rej: RTDB returned error code RTDB_RET_DB_ENTRY_NOT_FOUND
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*>
E1017	PDBI error: <*error text*>
E1021	IP address <*address*> is not authorized for PDB access.
E1023	Invalid value for <*prompt* >: <*value*>: Valid values are <*range*>. Hit the Escape key to abort the command.

E1028	IP address <*IP address*> is already authorized for PDBI access.
E1029	IP address <*IP address*> is not authorized for PDBI access.
E1032	Operation aborted by user.
E1035	Script <*script name*> failed: status=<*status*>
E1037	One or more EPAP software processes did not start
E1038	One or more EPAP software processes did not stop
E1043	The specified EPAP was not available.
E1044	Remote EPAP software is running. You must stop the remote EPAP software before performing this operation.
E1049	Could not connect to <*device or process*>: <*error text*>
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.
E1066	The requested user <*user*> 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.
E1075	This action must be done on the Active PDBA.
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.
E1088	Attempt to access the PDBA was not successful.
E1092	The range would overlap the existing range 232323 to 232324 (applicable for Both IMSI range and Blacklist Range).
E1093	The <*Provisioning Blacklist or IMSI range*> does not exist.
E1097	The maximum capacity for this provisioning has been reached.
E1098	Unable to establish SSH tunnel to <*machine Identifier*> machine.
E1099	Invalid IP Address/Username/Password combination
E1100	Task Scheduler error: <*error text*>
E1101	IP address <*IP Address*> is not authorized to perform this action: <*action text*>
E1102	This backup is incompatible: <*backup identifier*> Reason: <*reason text*>
E1103	This action cannot be performed as <*action text*> is in progress.

EPAP Banner Messages

Table 19: EPAP Informational Banner Messages lists the banner informational banner messages that appear on the user interface (UI) browser screen in the Message Box described in *EPAP GUI Main Screen*. These messages, sometimes referred to as *scroll by messages*, indicate the status of the EPAPs.

Table 19: EPAP Informational Banner Messages

Another user has already started the EPAP Software
Attempt to restart MySQL replication failed
Auto FTP: Failed transfer of file <*filename*> error
Auto FTP: Failed transfer of file <*filename*> error
Auto FTP: Successful transfer of file <*filename*>
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
HTTP interface disabled
HTTPS interface disabled
Import of <*file name*> in progress - <*xx.xx%*>
Import of <*file name*> completed
Import of <*file name*> failed (<*reason*>)
Import of <*file name*> postponed (<*reason*>)
Import PDB completed successfully
Import PDB failed
Import PDB in progress
MPS Reboot in Progress
MySQL data replication error detected; Attempting to restart
MySQL data replication restarted: <*reason*>
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
SSH Tunnel down for IP(s): <*IP1*>, <*IP2*>, <*IP3*> (display maximum 5 IPs)
SSH Tunnel down for more than 5 IPs
The EPAP software could not 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

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* and refer to the *EPAP Alarms on the T1200 Platform* 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 Service Module card.

The Active EPAP generates and sends Maintenance Blocks to the primary Service Module card. One Maintenance Block is sent as soon as the IP link is established between the Active EPAP and the primary Service Module card. 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 the *EPAP Alarms on the T1200 Platform* 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 a ppear 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.

Service Module Card Status Requests

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

Service Module Card Status Reporting to the EPAP

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

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

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

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

Service Module Card Status Message Fields

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

- Service Module card Memory Size

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

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

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

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

System Hardware Verification

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

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

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

Service Module Card Motherboard Verification

An AMD-K6 (or better) motherboard is required to support the G-Flex/ G-Port/INP/EIR VSCCP application on the Service Module card. EAGLE 5 ISS maintenance stores the validity status of the Service Module card motherboard configuration. The system does not allow the G-Flex, G-Port, INP/AINPQ, EIR, A-Port, V-Flex, and Migration 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 Service Module 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/AINPQ/EIR/A-Port/V-Flex/Migration application, loading of the Service Module card is automatically inhibited and the card is booted via PMTC. Booting the card in this manner suppresses any obituary.

Service Module Card Daughterboard Memory Verification

The VSCCP application performs two types of memory validation to determine whether or not a Service Module card has sufficient memory to run G-Flex/G-Port/INP/AINPQ/EIR/A-Port/Migration/V-Flex: Local Memory validation and Continual Memory validation.

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

The VSCCP application performs two types of memory validation to determine whether or not a Service Module card has sufficient memory to run G-Flex/G-Port/INP/AINPQ/EIR/A-Port/Migration/V-Flex: Local Memory validation and Real-Time Memory validation.

Local Memory Validation

When the G-Flex or INP feature bit is first enabled (a Feature Access Key is used for the EIR, AINPQ, G-Port, Migration, and V-Flex features), or any time the G-Flex, G-Port, INP/AINPQ, EIR, A-Port, V-Flex or Migration feature is enabled and the Service Module card is initializing, VSCCP checks to see if the Service Module card has at least one D1G daughterboard. G-Flex, G-Port or INP feature bit cannot be enabled if any of the Service Module cards have less than 1 GB of memory installed.

Real-Time Memory Validation

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

Actions Taken When Hardware Determined to be Invalid

When the hardware configuration for a Service Module card is determined to be invalid for the G-Flex, G-Port, INP/AINPQ, EIR, A-Port, V-Flex, and Migrationapplication, SCM automatically inhibits loading for that specific Service Module card. A major alarm is generated indicating that card loading for that Service Module 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 Service Module card determined to be invalid:

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

The `rept-stat-sccp` command supports the Service Module cards running the VSCCP application and reports G-Flex, G-Port, INP/AINPQ, EIR, A-Port, V-Flex, and Migration statistics. See *Commands* for more details on the `rept-stat-sccp` command.

Unstable Loading Mode

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

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

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

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

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

  It is possible for LIMs or Service Module cards to be inhibited or to have problems that prevent them from operating normally. If enough Service Module cards are out of service, it may not be possible for the remaining IS-NR Service Module cards to service at least 80% of the number of IS-NR LIMs. This is called "insufficient SCCP service." When this occurs, some of the LIMs are 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*).
- If LIM cards are being denied SCCP service and any Service Module 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 reports the existence of the unstable loading mode and the specific trigger that caused it.
- When in an unstable Loading Mode, the EAGLE 5 ISS w does not accept database updates. When updates are rejected, the reason is given as:

  ```
  E3112 Cmd Rej: Loading Mode unstable due to SCCP service is deficient.
  ```

  The `inh-card` and `alw-card` commands can be used to alter SCCP service levels to achieve the 80% threshold. This can be repeated for each card until the system is able to supply SCCP services to at least 80% of the IS-NR LIMs. The remaining 20% LIM or supporting Service Module cards may remain out of service until the stream of 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 EAGLE 5 ISS database has been loaded, that database can be updated (as long as the system is not in an unstable Loading Mode). However, if an EAGLE 5 ISS update comes in during EAGLE 5 ISS database loading, the Service Module card aborts the current loading, issue a class 01D7 obit message (*Figure 53: Obit Message for Abort of Card Loading*), and reboot.

```
tekelecstp 97-04-08 12:29:04 EST EAGLE 35.0.0

------------------------------------------------------------------------
    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
```

Figure 53: Obit Message for Abort of Card Loading

- If executing the `ent-card` or `inh-card` command would cause the system to enter an unstable Loading Mode, it is 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/AINPQ status
- EIR status
- A-Port status
- Migration status
- V-Flex status
- Service Module card memory capacity status
- Loading mode support status

System Status Reporting

The rept-stat-sccp command supports the Service Module cards running the VSCCP application, and reports G-Flex, G-Port, INP/AINPQ, EIR, A-Port, V-Flex, and Migration statistics. See *rept-stat-sccp* for details on the `rept-stat-sccp` command.

G-Flex/G-Port/INP/AINPQ/EIR/A-Port/V-Flex/Migration Status Reporting

The `rept-stat-mps` command reports the status of the G-Flex/G-Port/INP/AINPQ/EIR/A-Port/V-Flex/Migration provisioning system. The `rept-stat-sccp` command reports separately the statistics for G-Flex, G-Port, INP/AINPQ, EIR, A-Port, V-Flex, and Migration. See *Commands* for details on the `rept-stat-mps` and `rept-stat-sccp` commands.

Service Module Card Memory Capacity Status Reporting

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

When the EPAP sends database updates to the Service Module cards, the update messages includes a field that contains the new database memory requirements. Each Service Module card monitors the DB size requirements, and 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 Service Module card memory, a major alarm is issued.

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

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 Service Module cards in the system. When the loading mode is unstable, the `rept-stat-sys`command reports the existence of the unstable Loading Mode and the specific conditions which caused it. See *Unstable Loading Mode* 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 Service Module 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 54: rept-stat-sccp Command Report Examples*:

```
    Command entered at terminal #3.
;

     tekelecstp 00-06-23 13:34:22 EST EAGLE 35.0.0
    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 USA
    ------------------------------------------------------------------------
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%  GPLEX =  5%  GPORT = 10%
      INPMR =  2%  INPQS =  3%

    TOTAL SERVICE STATISTICS:
      SERVICE    SUCCESS    ERRORS    WARNINGS    FORWARD TO GTT    TOTAL
      GTT:          1995         5           -                 -     2000
      GPLEX:         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 35.0.0
    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%
      GPLEX: 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
      GPLEX:         500         1           4                10      515
      GPORT:         500         1           4                10      515
      INPMR:          50         2           3                15       70
      INPQS:         499         1           -                 -      500

   Command Completed.
;
```

Figure 54: `rept-stat-sccp` Command Report Examples

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.

```
   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        -
;
```

Figure 55: `rept-stat-db` Command Report Example

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 Service Module card.
- `rept-stat-mps:loc=xxxx` – This produces a more detailed report showing the G-Flex/G-Port/INP/EIR status of a specific Service Module card.

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

  Each Service Module card monitors the 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 Service Module card memory, a major alarm is issued.

Samples of the reports produced by these commands are shown in *Figure 56: rept-stat-mps Command Report Examples*:

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

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

                      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 35.0.0
    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.
;
```

Figure 56: rept-stat-mps Command Report Examples

rept-stat-trbl

This command includes the G-Flex/G-Port/A-Port /Migration Subsystem, INP/AINQP Subsystem, EIR Subsystem, V-Flex Subsystem, and Service Module card/EPAP IP link alarms.

```
    rept-stat-trbl
    Command entered at terminal #10.
;
    eagle10605 99-06-24 14:34:08 EST EAGLE 35.0.0
    Searching devices for alarms...
;
    eagle10605 99-06-24 14:34:09 EST EAGLE 35.0.0
    SEQN UAM  AL DEVICE   ELEMENT      TROUBLE TEXT
    0002.0143  * CARD 1113 OAM         System release GPL(s) not approved
    0011.0176  * SECULOG 1116          Stdby security log -- upload required
    3540.0203 ** SLK 1201,A lsn1       REPT-LKF: lost data
    3541.0203 ** SLK 1201,B lsn4       REPT-LKF: lost data
    3542.0203 ** SLK 1202,A lsn2       REPT-LKF: lost data
    3544.0202 ** SLK 1203,A lsn3       REPT-LKF: HWP - too many link interrupts
    0021.0318 ** LSN lsn1              REPT-LKSTO: link set prohibited
    0022.0318 ** LSN lsn2              REPT-LKSTO: link set prohibited
    0023.0318 ** LSN lsn3              REPT-LKSTO: link set prohibited
    0010.0318 ** LSN lsn4              REPT-LKSTO: link set prohibited
    3537.0084 ** DSM A   1215          IP Connection Unavailable
    3536.0084 ** 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.
```

Figure 57: `rept-stat-trbl` Command Output Example

rept-stat-alm

This command includes the alarm totals for the G-Flex/G-Port Subsystem, INP Subsystem, EIR Subsystem, and Service Module card/EPAP IP links.

```
    rept-stat-alm
    Command entered at terminal #10.
;

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

Figure 58: `rept-stat-alm` Command Report Example

pass: cmd="Ping"

The 'ping' command allows for troubleshooting of the private EPAP-Service Module card IP network.

```
eagle10506 99-08-11 08:43:45 EST EAGLE 35.0.0
    pass:loc=1215:cmd="ping     -h"
    Command entered at terminal #2.
;

    eagle10506 99-08-11 08:43:45 EST EAGLE 35.0.0
    PASS: Command sent to card
;

    eagle10506 99-08-11 08:43:45 EST EAGLE 35.0.0

    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)

;
```

Figure 59: `pass: cmd="Ping"` Command Output Example

pass: cmd="netstat"

The '`pass: cmd="netstat"` command allows troubleshooting of network interface and routing configuration problems within the private EPAP-Service Module card IP network.

```
eagle10506 99-08-11 08:43:00 EST EAGLE 35.0.0
    pass:loc=1215:cmd="netstat  -h"
    Command entered at terminal #2.;
    eagle10506 99-08-11 08:43:00 EST EAGLE 35.0.0
    PASS: Command sent to card;
    eagle10506 99-08-11 08:43:00 EST EAGLE 35.0.0

    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
;
```

Figure 60: `pass: cmd="netstat"` Command Output Example

Hourly Maintenance Report

The hourly maintenance report includes the alarm totals for the G-Flex/G-Port/A-Port/Migration Subsystem, INP/AINQP Subsystem, V-Flex Subsystem, and DSM/EPAP IP links.

```
    eagle10506 99-10-10 16:00:01 EST EAGLE 35.0.0
    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 35.0.0
    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 35.0.0
    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 35.0.0
    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 35.0.0
    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"
;
```

Figure 61: Hourly Maintenance Report Output Example

Unsolicited Alarm and 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*EPAP Alarms on the T1200 Platform* manual 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 the *EPAP Alarms on the T1200 Platform*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 20: EAGLE 5 ISS MPS Platform and Application Alarms 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*). 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 the *EPAP Alarms on the T1200 Platform*manual.

Table 20: 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

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

Figure 62: Alarm Output Example

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

Figure 63: MPS Available Alarm

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

EPAP-to-Service Module Card Connection Status

The EPAP and the Service Module cards are connected over two Ethernet networks and use TCP/IP. If connection is inoperative, the Service Module card 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-Service Module Card UAMs

Maintenance Blocks EPAP have a field to identify error message requests. (See *Maintenance Blocks*). The Service Module card processes incoming Maintenance Blocks and generates the requested UAM. The Service Module card acts only as a delivery agent. The recovery actions for the EPAP-Service Module card UAMs are defined in *Unsolicited Alarm and Information Messages*.

Service Module Card-EPAP Link Status Alarms

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

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

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

Figure 64: Service Module Card-EPAP Link Alarm Example

RTDB Audit Alarms

During an audit of the Service Module 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 *Unsolicited Alarm and Information Messages*.

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

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

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

- 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.

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

    station1234 00-04-30 16:28:08 EST EAGLE 35.0.0
*   0012.0444 * CARD 1108 VSCCP        RTDB Database is inconsistent
```

- 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.

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

    station1234 00-04-30 16:28:08 EST EAGLE 35.0.0
    0012.0445 CARD 1108 VSCCP          RTDB Database has been corrected
```

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

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

    station1234 99-09-30 16:28:08 EST EAGLE 35.0.0
*   0012.0448 * CARD 1108 VSCCP        RTDB Database is incoherent
```

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

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

    station1234 99-09-30 16:28:08 EST EAGLE 35.0.0
**  0012.0449** CARD 1108 VSCCP        RTDB resynchronization in progress
```

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

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

    station1234 99-09-30 16:28:08 EST EAGLE 35.0.0
    0012.0450   CARD 1108 VSCCP        RTDB resynchronization complete
```

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

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

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

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

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

    station1234 99-09-30 16:28:08 EST EAGLE 35.0.0
    0012.0452   CARD 1108 VSCCP        RTDB reload complete
```

Chapter 5

EPAP Software Configuration

Topics:

This chapter describes how to configure the EPAP software.

Setting Up an EPAP Workstation

The customer workstation serving as a client PC, shown in *Figure 9: Process Architecture View of the EPAP UI* must meet the criteria described below.

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

Microsoft Internet Explorer® version 5.0 or later is supported and certified for use with the EPAP Graphical User Interface (GUI). Mozilla Firefox® version 3.0.0 is partially supported for use with the EPAP GUI. If using Firefox, this message is displayed when logging in to the EPAP GUI:

```
CAUTION: The User Interface may not function correctly with the browser you are
using.
```

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. The EPAP GUI supports Java 1.5 and 1.6 clients.

The Java installation must be performed in the sequence shown:

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

Install Java Plug-In

Because the Java applet is required for the EPAP GUI to operate, perform this procedure to install the Java plug-in after completing the EPAP configuration.

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

1. Using the selected browser, enter the IP address for your EPAP A machine. You will see the login screen.
2. Attempt to log in to the EPAP User Interface screen. If using a browser other than a certified browser (*Compatible Browsers*), this message is displayed when logging in to the EPAP GUI:

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

   After you successfully enter the Username and Password, the login process checks for the required Java plug-in. If the Java plug-in not present and a previous version of Java is installed, the system displays a **Security Warning** window as shown in *Figure 65: Security Warning Window*.

Figure 65: Security Warning Window

3. Click the **Install** button to begin the process of loading the Java plug-in.
4. The Java installation presents a **License Agreement** screen as shown in *Figure 66: License Agreement*.

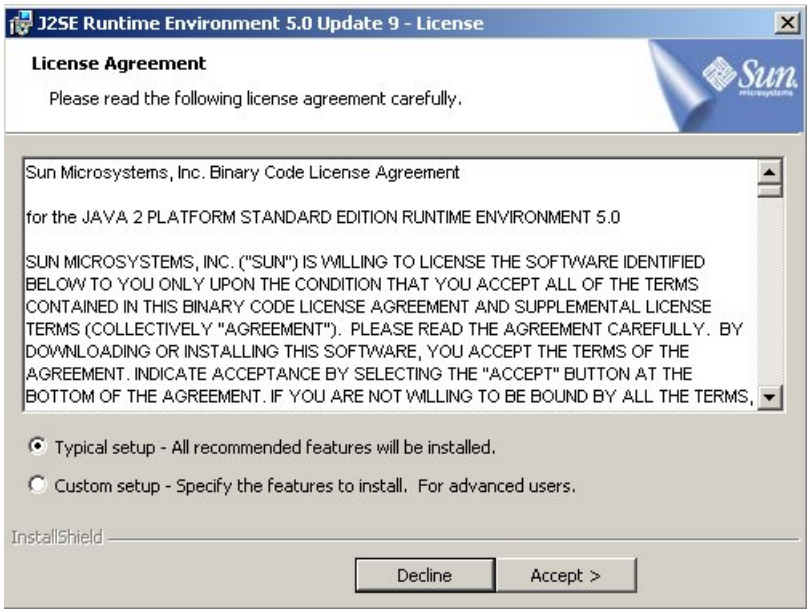

Figure 66: License Agreement

5. Ensure that the **Typical Setup** radio button is selected. Click the **Accept** button to accept the Sun Microsystems agreement.
6. After the installation process starts, a progress window is displayed as shown in *Figure 67: Java Installation Progress Window*.

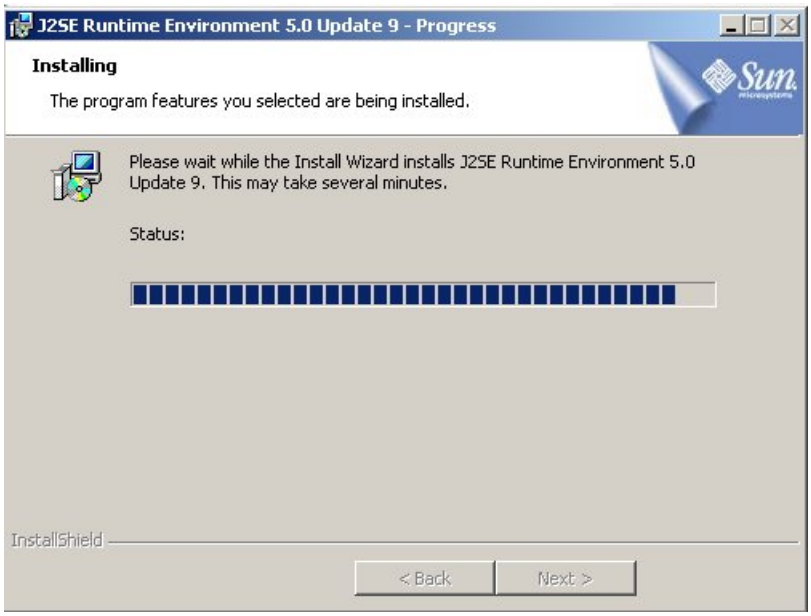

Figure 67: Java Installation Progress Window

7. When the installation is complete, the Installation Complete window appears as shown in *Figure 68: Java Installation Complete Window*.

Figure 68: Java Installation Complete Window

8. The installation is complete. Click the **Finish** button. Return to the browser screen displaying the EPAP login screen.

Install Java Policy File

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

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

Add Security Parameters to an Existing Java Policy File

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

1. From the Windows **Start** menu, select **Control Panel**.
2. Select the **Java Control Panel**. After the **Java Control Panel** appears, click the **Java** tab as shown in *Figure 69: Java Control Panel, Java Tab*.

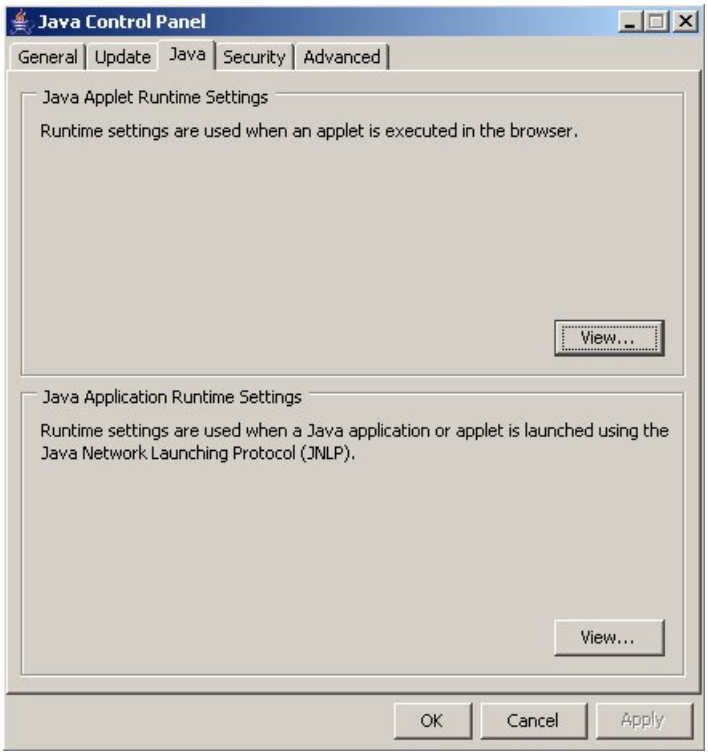

Figure 69: Java Control Panel, Java Tab

3. Click **View** in the **Java Applet Runtime Settings** pane. The Java Runtime Settings dialog box appears as shown in *Figure 70: Java Runtime Settings Dialog Box*.

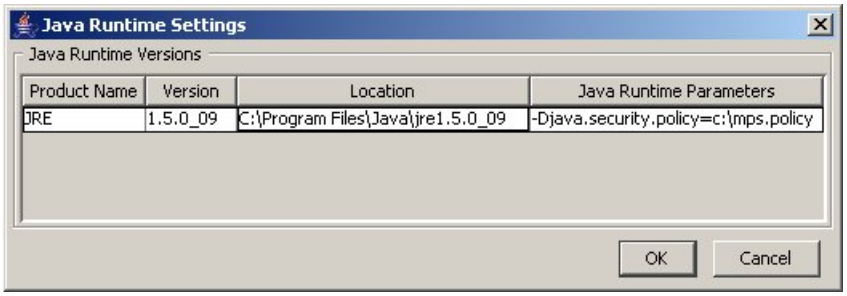

Figure 70: Java Runtime Settings Dialog Box

4. Adjust the width of the columns until you can read the contents of the Java Runtime Parameters column at the far right.
5. Open the policy file indicated in the Java Runtime Parameters column. Insert the following text.

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

Create a New Java Policy File

To create a Java policy file:

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

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

2. Follow steps 2 through 4 in the procedure described in *Add Security Parameters to an Existing Java Policy File*.
3. In the Java Runtime Parameters column of the Java Runtime Settings Diaglog Box, type the path to the file created in step 1 of this procedure. An example is shown below. If the path name to your system contains spaces, enclose the path name in double quotes (").

```
-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* . That data will be used in the configuration procedure.

Required Network Address Information

This information is needed to configure the MPSs at EAGLE 5 ISS A, EAGLE 5 ISS B, and non-provisionable MPSs. Fill in the tables for reference during the installation procedure.

Table 21: 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)*	

Common Information		
	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 22: Information for Provisionable MPSs at EAGLE 5 ISS B*)		. . .
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 22: Information for Provisionable MPSs at EAGLE 5 ISS B*)		. . .

Table 22: Information for Provisionable MPSs at EAGLE 5 ISS B

Common Information	
MPS A Provisioning Network Address	. . .

Common Information		
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 21: Information for Provisionable MPSs at EAGLE 5 ISS A*)		. . .
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		

Common Information	
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 21: Information for Provisionable MPSs at EAGLE 5 ISS A*)	. . .

Table 23: 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	. . .

Common Information	
	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 21: Information for Provisionable MPSs at EAGLE 5 ISS A*)	. . .
MPS A Provisioning Network Address for MPS at EAGLE 5 ISS B (copy from *Table 22: Information for Provisionable MPSs at EAGLE 5 ISS B*)	. . .
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 24: Information for Non-Provisionable MPSs at EAGLE 5 ISS #2

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

Common Information		
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 21: Information for Provisionable MPSs at EAGLE 5 ISS A*)		. . .
MPS A Provisioning Network Address for MPS at EAGLE 5 ISS B (copy from *Table 22: Information for Provisionable MPSs at EAGLE 5 ISS B*)		. . .
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		

Common Information	
MPS A Forwarded Banner Port	
MPS B Forwarded Banner Port	
MPS A Provisioning Static NAT Addr.	. . .
MPS B Provisioning Static NAT Addr.	. . .

EPAP Firewall Port Assignments

If a firewall is installed in the provisioning network between the MPS systems or between the MPS system(s) and the provisioning system, it must be configured to allow selected traffic to pass. Firewall protocol filtering for the various interfaces is defined in this table (from the perspective of each MPS).

Note: Use the information in this table for both internal customer network configuration and VPN access for support.

Table 25: Firewall Requirements

Server Interface	TCP/IP Port	Inbound	Outbound	Application	Use/Comments
EPAP Application Firewall Requirements:					
Port 1	22	Yes	Yes	EPAP	SSH/SCP/SFTP
Port 1	123	Yes	Yes	EPAP	NTP - Needed for time-sync.
Port 1	80	Yes	No	EPAP	APACHE - Needed for EPAP Web-based GUI.
Port 1	8001-8002	Yes	No	EPAP	SUXEC (process) - Needed by EPAP Web-based GUI.
Port 1	8473	Yes	Yes	EPAP	GUI server (process) - Needed by EPAP Web-based GUI.

Server Interface	TCP/IP Port	Inbound	Outbound	Application	Use/Comments
EPAP Application Firewall Requirements:					
Port 1	5871-5873	Yes	No	EPAP	Used to send Provisioning data to the EPAP.
Port 1	5874	Yes	Yes	EPAP	Used to send Provisioning data to the EPAP
Port 1	5019	Yes	Yes	EPAP	Versant Fault Tolerant Server: EPAP database mgmt system.
Port 1	9696	Yes	Yes	EPAP	PDBA (process) - PDB application manages the provisioning data.
RMM Firewall Requirements:					
RMM Port	22	Yes	Yes	RMM	SSH/SCP/SFTP
RMM Port	80	Yes	No	RMM	HTTP - Needed for RMM Web-based GUI.
RMM Port	443	Yes	No	RMM	SSL (https) - Needed for RMM Web-based GUI secure connection (REQUIRED)
RMM Port	623	Yes	Yes	RMM	RMCP

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 71: Configuration Menu Header Format* shows a sample configuration header format.

```
MPS Side A:  hostname: mpsa-d1a8f8  hostid: 80d1a8f8
             Platform Version: 5.0.0-22.0.0
             Software Version: EPAP 5.0.0-30.1.0
             Wed Jul 13 09:51:47 EST 2005
```

Figure 71: Configuration Menu Header Format

When you are shown a menu, 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. Press **Return** to enter your choice.

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*. 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:

```
E
        XXXX
      :
        Error text
```

```
Press return to continue
```

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

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

Note: 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 *Procedure for Configuring EPAPs*. 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 72: 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...
```

Figure 72: Initial Configuration Text Screen

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 73: Initial Configuration Continues* shows the continuation of the screen information. The installer enters **y** if the installation is to continue.

```
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
```

Figure 73: Initial Configuration Continues

Note:

Review the information required for the following section in *Required Network Address Information* . Make certain all required information is obtained and recorded in the tables provided.

Next, the installer declares the MPS to be provisionable or non-provisionable, as shown in *Figure 74: Designating Provisionable or Non-Provisionable MPS*. The example illustrates this MPS as a 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
```

Figure 74: Designating Provisionable or Non-Provisionable MPS

Next, the installer is prompted for the `epapdev` user password on the mate MPS server. *Figure 75: Entering the epapdev Password* shows sample output that is generated after the correct password is entered.

```
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.
```

Figure 75: Entering the `epapdev` Password

The **Configuration Menu** appears for the first time.

EPAP Configuration Menu

As shown in *Figure 76: EPAP Configuration Menu*, a report and the test-based **EPAP Configuration Menu** appear. The `epapconfig` user can now begin configuring the MPS local and remote servers.

Figure 76: 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              |
|----|-----------------------------------|
|  8 | PDB Configuration Menu            |
|----|-----------------------------------|
|  9 | Security                          |
|----|-----------------------------------|
|  e | Exit                              |
\--------------------------------------/
Enter Choice:
```

To choose a menu item, enter the number or letter of the menu item at the `Enter Choice` prompt and press **Return**.

Display Configuration

The Display Configuration option **1** displays a configuration of the EPAP. See an example of the Configuration Report in *Figure 77: Example of Configuration Report*.

```
MPS Side A:  hostname: mpsa-d1a8f8  hostid: 80d1a8f8
             Platform Version: 5.0.0-22.0.0
             Software Version: EPAP 5.0.0-30.1.0
             Wed Nov 28 09:51:47 EST 2001

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…
```

Figure 77: Example of Configuration Report

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 26: Sample IP Addresses Used in Configuration* shows an example of IP addresses that could be used in the configuration process.

Table 26: 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 78: Configure Network Interfaces Menu*. It supports the configuration of all the network interfaces for the EPAP.

```
MPS Side A:  hostname: mpsa-f0ad77  hostid: 80f0ad77
             Platform Version: 5.0.0
             Software Version: EPAP 5.0.0-20.18.0
             Thu Jan 17 10:18:27 EST 2002

 /-----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:
```

Figure 78: Configure Network Interfaces Menu

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: 127.0.0.1 is not a valid IP address for this operation.

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*.

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 79: Configure Provisioning Network Output* for the option 1 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 ...
```

Figure 79: Configure Provisioning Network Output

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 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: 127.0.0.1 is not a valid IP address for this operation.

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* for a description of EPAP network IP address assignments. See *Figure 80: Configure DSM Network* for the option 3 output.

```
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 ...
```

Figure 80: Configure DSM Network

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* for a description of EPAP network IP address assignments. See *Figure 81: Configure Backup Provisioning Network* for the option 4 output.

```
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 ...
```

Figure 81: Configure Backup Provisioning Network

Note: 127.0.0.1 is not a valid IP address for this operation.

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.

Note: 127.0.0.1 is not a valid IP address for this operation.

Each numbered item of the Configure Forwarded Ports menu allows the user to specify a port number used for remote access to the MPS.

This information should be received from the customer for the MPS and recorded in *Table 21: Information for Provisionable MPSs at EAGLE 5 ISS A* and *Table 22: Information for Provisionable MPSs at EAGLE 5 ISS B* .

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 82: Configuring NAT Addresses Prompt* shows an example of a resulting prompt.

Note: 127.0.0.1 is not a valid IP address for this operation.

```
EPAP A Static NAT Address:
```

Figure 82: Configuring NAT Addresses Prompt

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 83: Configure Provisioning VIP Addresses Output* for the option 7 output.

Note: 127.0.0.1 is not a valid IP address for this operation.

```
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...
```

Figure 83: Configure Provisioning VIP Addresses Output

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 84: Select Time Zone Menu* for the option 3 output.

```
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:
```

Figure 84: Select Time Zone Menu

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 *Time Zone File Names* for the list that appears when you press the Return key or enter invalid time zone file name.

The time zone change does not take effect until the next time the MPS is rebooted. The **Reboot MPS** menu is described in *Reboot the MPS* .

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 85: Exchange Secure Shell Keys Menu* for the option 4 output.

```
MPS Side A:  hostname: tortola-a  hostid: a8c0883d
             Platform Version: 2.0.2-4.0.0_50.26.0
             Software Version: EPAP 1.0.1-4.0.0_50.34.0
             Fri Sep 16 07:37:32 EDT 2005

 /-----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:
```

Figure 85: Exchange Secure Shell Keys Menu

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 86: Exchange Secure Shell Keys Output* for the Option **1** output.

```
MPS Side A:  hostname: tortola-a  hostid: a8c0883d
             Platform Version: 2.0.2-4.0.0_50.26.0
             Software Version: EPAP 1.0.1-4.0.0_50.34.0
             Fri Sep 16 07:37:32 EDT 2005

 /-----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:
```

Figure 86: Exchange Secure Shell Keys Output

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 87: Change Password* for the option `5` output.

```
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...
```

Figure 87: Change Password

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 88: Platform Menu Output* for the option 6 output.

```
 /-----EPAP Platform Menu-\
/--------------------------\
|  1 | Initiate Upgrade    |
|----|---------------------|
|  2 | Eject CD            |
|----|---------------------|
|  3 | Reboot MPS          |
|----|---------------------|
|  4 | Halt MPS            |
|----|---------------------|
|  5 | MySQL Backup        |
|----|---------------------|
|  6 | RTDB Backup         |
|----|---------------------|
|  7 | PDB Backup          |
|----|---------------------|
|  e | Exit                |
\--------------------------/

Enter Choice:
```

Figure 88: Platform Menu Output

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 Technical Services; refer to .*Customer Care Center* .

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.

MySQL Backup

The MySQL Backup option `5` 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 the NPDB...
```

RTDB Backup

The RTDB Backup option `6` 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

Successfully started backup of RTDB.
Status will be displayed on the GUI banner.
```

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 `7` 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_20030530144717GMT_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 89: Configure NTP Server Menu* for the option 9 output.

```
 /----EPAP Configure NTP Server Menu-\
/-------------------------------------\
|  1 | Display External NTP Server     |
|----|---------------------------------|
|  2 | Add External NTP Server         |
|----|---------------------------------|
|  3 | Remove External NTP Server      |
|----|---------------------------------|
|  e | Exit                            |
\-------------------------------------/

Enter Choice:
```

Figure 89: Configure NTP Server Menu

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 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 enabling the Automated Database Recovery and PDBA Proxy features. See *Figure 90: Configure PDB Menu* for the option **8** output.

```
 /-----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:
```

Figure 90: Configure PDB Menu

Configure PDB Network

The Configure PDB Network option **1** of the Configure PDB Menu identifies the provisioning network interface addresses of the remote PDBs. 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 91: Configure PDB Network for Provisionable MPS shows the provisionable MPS configuration, and *Figure 92: Configure PDB Network for Non-Provisionable MPS* shows the non-provisionable MPS configuration.

```
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 91: Configure PDB Network for 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...
```

Figure 92: Configure PDB Network for Non-Provisionable MPS

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* . *Figure 93: RTDB Homing Menu* shows the option **2** output.

```
/-------RTDB Homing Menu------------\
/-------------------------------------\
|  1 | Configure Specific RTDB Homing |
|----|--------------------------------|
|  2 | Configure Active RTDB Homing   |
|----|--------------------------------|
|  3 | Configure Standby RTDB Homing  |
|----|--------------------------------|
|  e | Exit                           |
\-------------------------------------/

Enter Choice:
```

Figure 93: RTDB Homing Menu

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*. 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 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 PDB of the standby MPS.

```
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 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 PDB of the active MPS.

```
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 about these states, refer to *Provisioning Multiple EPAPs Support*. This command toggles the states between provisionable and non-provisionable.

See *EPAP Configuration Menu* for the prompt that is displayed for 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 User Interface 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 this 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 this 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 *EPAP Configuration Menu*.

Security

Figure 94: 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            |
|--------------------------------------|
|  8 | PDB Configuration Menu          |
|--------------------------------------|
|  9 | Security                        |
|--------------------------------------|
|  e | Exit                            |
\--------------------------------------/

Enter Choice: 5
Are you sure you wish to change the text UI password on MPS A [N]: Y
Enter new password for text ui user:
```

The Security Menu, option 9, of the *Figure 94: EPAP Configuration Menu*, provides access to configure the Idle Terminal Timeout and the password restrictions for the EPAP system users. See *Figure 95: EPAP Configure Security Menu* for the option 9 output.

```
 /-----EPAP Configure Security Menu-\
/-----------------------------------\
|  1 | Idle Terminal Timeout        |
|----|------------------------------|
|  2 | Password Restriction         |
|----|------------------------------|
|  e | Exit                         |
\-----------------------------------/
```

Figure 95: EPAP Configure Security Menu

Idle Terminal Timeout

The Idle Terminal Timeout, option 1 of the *Figure 95: EPAP Configure Security Menu* displays the subment shown in *Figure 96: Configure Idle Terminal Timeout Menu*. This menu provides access to configure the Idle Terminal Timeout Security options. Option 1 of the menu displays the configured idle terminal timeout. Option 2 of the menu provides the interface to set the Idle Terminal Timeout.

The EPAP terminal will logout the user if the terminal remains idle for the configured amount of time. The Idle Terminal Timeout limit will be within the range of **0 - 9999** (seconds), both inclusive, where **0** specifies no timeout. If the idle terminal timeout is not set, then the system default shall apply i.e. no timeout.

Note: The idle terminal timeout is not applicable to the system users who either have restricted shell or do not have their own shell. This behavior is valid for system users like **appuser**, **platcfg**, and **epapconfig**.

```
 /-----Configure Idle Terminal Timeout Security Menu-\
/-------------------------------------------------\
|  1 | Display Idle Terminal Timeout              |
|----|--------------------------------------------|
```

```
|  2 | Configure Idle Terminal Timeout                |
|----|------------------------------------------------|
|  e | Exit                                           |
\-------------------------------------------------------/
```

Figure 96: Configure Idle Terminal Timeout Menu

Password Restriction

The Password Restriction, option 2 of the *Figure 95: EPAP Configure Security Menu* displays the submenu shown in *Figure 97: Configure Password Restriction Menu*. Option 1, System Default, provides the interface to configure password restrictions for the System Default, i.e. the restrictions shall apply for all new system users only. Option 2, Per User, provides the interface to configure password restrictions per user basis.

```
 /-----Configure Password Restriction Menu-\
/------------------------------------------ \
|  1 | System Default                       |
|----|--------------------------------------|
|  2 | Per User                             |
|----|--------------------------------------|
|  e | Exit                                 |
\-----------------------------------------/
```

Figure 97: Configure Password Restriction Menu

System Default

Option 1 of the *Figure 97: Configure Password Restriction Menu*, displays the submenu shown in *Figure 98: Configure Password Restriction Menu*. Option 1 displays the password restrictions configured for the new system users. Options 2 to 5 provide interface to set the password restrictions for the new system users.

If the password restrictions are not configured, then the default password restrictions is applied to the existing and new system users.

```
 /-----Configure Password Restriction Menu----------------------------------\
/-------------------------------------------------------------------------------\
|  1 | Display Password Restriction Configuration                               |
|----|--------------------------------------------------------------------------|
|  2 | Min no of days allowed between password changes                          |
|----|--------------------------------------------------------------------------|
|  3 | Max no of days a password may be used                                    |
|-------------------------------------------------------------------------------|
|  4 | Minimum acceptable Password size                                         |
|-------------------------------------------------------------------------------|
|  5 | Number of days that a user will be warned before his password expires    |
|--- |--------------------------------------------------------------------------|
|  e | Exit                                                                     |
\-------------------------------------------------------------------------------/
```

Figure 98: Configure Password Restriction Menu

Per User

If password restrictions are configured per user basis, then the user is required to enter the username and password of the user for which password restriction is to be applied, as shown in *Figure 99: Configure Password Restriction per User*.

Figure 99: Configure Password Restriction per User

```
 /-----Configure Password Restriction Menu-\
/------------------------------------------ \
|  1 | System Default                       |
|----|--------------------------------------|
|  2 | Per User                             |
|----|--------------------------------------|
|  e | Exit                                 |
\-----------------------------------------/

Enter Choice: 2
Enter username:
Enter password for user:
```

After the successful authorization of the entered username, the submenu shown in *Figure 100: Configure Password Restriction Menu* is displayed.

Option 1, Display Password Restriction Configuration, displays the password restrictions configured for the specified system user. Options 2 to 4 provide the interface to set the password restrictions for the specified system user.

Figure 100: Configure Password Restriction Menu

```
 /-----Configure Password Restriction Menu----------------------------------\
/-------------------------------------------------------------------------- \
|  1 | Display Password Restriction Configuration                           |
|----|--------------------------------------------------------------------- |
|  2 | Min no of days allowed between password changes                      |
|----|--------------------------------------------------------------------- |
|  3 | Max no of days a password may be used                                |
|----------------------------------------------------------------------------|
|  4 | Number of days that a user will be warned before his password expires  |
                                    |
|----------------------------------------------------------------------------|
|  e | Exit                                                                 |
\-----------------------------------------------------------------------------/
```

Password Restriction Parameters

Min no of days allowed between password changes	The min no. of days allowed between password changes parameter prevents the system user from changing the password before the configured time. If the value is not set, then the system default of **0** days is used. the value must be within the range of **1 - 180**, both inclusive. The value must be less than or equal to the maximum number of days a password may be used.
Max no of days a password may be used (Password Aging)	The maximum no of days a password may be used (password aging) determines the number of days for which the current password of the system user works. Once the password expires, the user is required to change to a new password. The user cannot login with the expired password. If the value is not set, then the system default of **99999** days is used. If configured, the EPAP system password aging must be within the

	range of **1 - 180**, both inclusive. When configuring password aging, only a value greater than or equal to the current value of minimum no. of days a password may be used, is acceptable.
Number of days that a user will be warned before his password expires	System users are warned N days before their passwords expire. The N value is configured using the Number of days that a user will be warned before his password expires parameter. If the password warning days is not set, then the system default of **7** days is used. A value of **0** means warning is given only on the day of password expiration. A value of **-1** means no warning is given. When configuring the password warning days for EPAP system users, only a value less than or equal to the difference between current password aging and minimum no. of days allowed between password changes settings, is acceptable.
Minimum acceptable Password size	The minimum password length configured is applicable for all existing and new system users. The allowed minimum length for password is in the range of 8 to 80, both inclusive. If minimum password length is not set, then the system default of 5 is used.

Password change for system users

All system users can change their own passwords. The **epapdev** and **appuser** users use the `passwd` command provided by the Operating System. If changing a password using the `passwd` command, then the Linux PAM credit rules are used.

The system user **epapconfig** uses the option provided in the *Figure 94: EPAP Configuration Menu*. Linux PAM rules are not applicable while changing the password for **epapconfig** user. Only the configured minimum password length applies.

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 that 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* and defined in *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 notations to indicate individual instructions to be performed for those specific MPSs.

Table 27: Configuration Notations

Notation	Notation Description
A: MPS on EAGLE 5 ISS A:	This notation indicates installation instructions to be performed specifically for the MPSs (MPS A and MPS B) on EAGLE 5 ISS A.

B: MPS on EAGLE 5 ISS B:	This notation indicates installation instructions to be performed specifically for the MPSs (MPS A and MPS B) on EAGLE 5 ISS B.
N: Non-Provisionable MPS:	This notationl 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 thecorrect 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* , 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, connect to an MPS to perform configuration. In a typical installation, connect directly to the MPS at EAGLE 5 ISS A to configure it, then use `ssh` to connect to the MPS at EAGLE 5 ISS B and configure it.

After connecting to the MPS on EAGLE 5 ISS A, you are prompted to log in.

1. Log in as `epapconfig`.

   A Caution notice is displayed. Evaluate the conditions listed.

```
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. After all conditions of the Caution notice are satisfied, press **Return** to continue.

   After pressing **Return** to continue, you can abort or proceed with the initial configuration.

Note: Pressing**Return** accepts the default valuen. .

```
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
```

3. To continue with the configuration, enter `y`

   B: MPS on EAGLE 5 ISS 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', the configuration software now considers the same MPS pair now to be 'local'. For more information, refer to .

4. Declare whether the MPS is provisionable or non-provisionable.
   (This example shows this MPS as a provisionable MPS.)

   A: MPS on EAGLE 5 ISS A:

   Answer `y` in this step.

   B: MPS on EAGLE 5 ISS B:

   Answer `y` in this step.

   N: Non-Provisionable MPS:

   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
```

5. When prompted, enter the `epapdev` user password on the mate MPS server in order to confirm the secure shell keys are successfully exchanged.
   This 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.
```

Upon successful configuration file setup, the **EPAP Configuration Menu** appears (for the first time) with 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:
5.0.0
-22.0.0
             Software Version: EPAP 5.0.0-30.1.0
             Wed Jul 16 09:51:47 EST 2003
 /-------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              |
|----|-----------------------------------|
|  8 | PDB Configuration Menu            |
|----|-----------------------------------|
|  9 | Security                          |
|----|-----------------------------------|
|  e | Exit                              |
\----------------------------------------/
Enter Choice:
```

6. Choose option `1`, Display Configuration.

   This option 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                      = No

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              |
|----|-----------------------------------|
|  8 | PDB Configuration Menu            |
|----|-----------------------------------|
|  9 | Security                          |
|----|-----------------------------------|
|  e | Exit                              |
\----------------------------------------/
Enter Choice: 2
```

9. Choose option 1, Configure Provisioning Network.

```
MPS Side A:  hostname: dakar  hostid: a8c03c42
             Platform Version: 2.0.4-0.19570
             Software Version: EPAP 1.0.8-0.19570
             Tue Dec  6 11:06:52 EST 2005

 /-----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
```

The **Configure Provisioning Network Menu** allows you to accept the default IP address values presented by the configuration software for EPAP A and EPAP B provisioning network and network netmask, or enter specific IP values previously received from the customer for the MPS.

Note: 127.0.0.1 is not a valid IP address for this operation.

Refer to the information recorded in *Table 21: Information for Provisionable MPSs at EAGLE 5 ISS A* through *Table 24: Information for Non-Provisionable MPSs at EAGLE 5 ISS #2* 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 appears.

```
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…
```

10. Press the **Return** , to return to the **Configure Network Interfaces Menu**.

11.

```
 /-----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
```

```
Verifying connectivity with mate...
Enter the first 3 octets for the EPAP MPS sync Network [192.168.4]
Press return to continue...
```

- Press **Return** to accept the default Sync Network IP address octet values presented by the configuration software.
- Change the default Sync Network IP address octet values presented by the configuration software by entering an IP address octet.

Upon accepting the default value or entering a specific EPAP Sync IP address octet value, the **Configure Network Interfaces Menu** appears.

Note: Unless a known network address conflict exists, skip *Step 12* and *Step 13*r elated to option 3, Configure DSM Network.

12. Choose option 3, Configure DSM Network.

```
 /-----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
```

The Configure DSM Network choice automatically adds the DSM network IP address to the list of known hosts.

13. Accept the 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]:
```

Upon accepting the default value or entering a specific EPAP backup DSM network octet IP address value, the **Configure Network Interface Menu** appears.

Note: If you do not want to configure a backup provisioning network interface, skip *Step 14* and *Step 15*. Proceed to *Step 16*.

14. Choose option 4, Configure Backup Provisioning Network.

```
 /-----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
```

This menu selection prompts you for all information necessary to set up a second interface for the customer's Provisioning Network.

Note: 127.0.0.1 is not a valid IP address for this operation.

The address information should be received from the customer for the MPS. Refer to the information recorded in *Table 21: Information for Provisionable MPSs at EAGLE 5 ISS A* through *Table 24: Information for Non-Provisionable MPSs at EAGLE 5 ISS #2* for the correct addresses.

The IP address for this interface must be on a different class C subnet than the primary Provisioning Network address. You must set up a second default router address to coincide with the Backup Provisioning Network. There are no default values for any of these fields. The customer must supply all the information. The Backup Provisioning Network cannot be configured using the `platcfg` utility.

```
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 ...
```

15. Press **Return** 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, skip *Step 16* through *Step 19* and proceed to *Step 20*.

16. Choose option 5, Configure Forwarded Ports.

```
 /-----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
```

The **Configure Forwarded Ports Menu** appears.

```
 /-----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:
```

17. Enter the correct option number for the port information to be entered.

    Refer to the information recorded in *Table 21: Information for Provisionable MPSs at EAGLE 5 ISS A* and *Table 22: Information for Provisionable MPSs at EAGLE 5 ISS B* for the correct information.

    A: MPS on EAGLE 5 ISS A:

    Options 1, 3, 5, and 7 are valid.

    B: MPS on EAGLE 5 ISS B:

    Options 2, 4, and 6 are valid.

18. Enter the appropriate port information.

    Press return to return to the **Configure Forwarded Ports Menu**.

```
EPAP A HTTP Port [80]:
```

19. Enter an 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, skip *Step 20* through *Step 23* for configuring static NAT and continue with *Step 24*.

20. Choose option `6`, Configure Static NAT Addresses.

```
 /-----Configure Network Interfaces Menu----\
/--------------------------------------------\
|  1 | Configure Provisioning Network        |
|----|---------------------------------------|
|  2 | Configure Sync Network                |
|----|---------------------------------------|
|  3 | Configure DSM Network                 |
|----|---------------------------------------|
|  4 | Configure Backup Provisioning Network |
|----|---------------------------------------|0
|  5 | Configure Forwarded Ports             |
|----|---------------------------------------|
|  6 | Configure Static NAT Addresses        |
|----|---------------------------------------|
|  7 | Configure Provisioning VIP Addresses  |
|----|---------------------------------------|
|  e | Exit                                  |
\--------------------------------------------/
Enter choice: 6
```

    The **Configure Static NAT Addresses Menu** appears.

```
/-----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                                  |
\--------------------------------------------/
```

21. Enter the appropriate option to configure the Static NAT Address.

    Each numbered item of the **Configure Static NAT Addresses Menu** allows you to specify an IP Address used outside of the firewall for remote access to the MPS

    A: MPS on EAGLE 5 ISS A:

    Options 1 and 3 are valid.

    B: MPS on EAGLE 5 ISS B:

    Option 2 is valid.

22. Enter a valid NAT IP address from *Table 21: Information for Provisionable MPSs at EAGLE 5 ISS A* or *Table 22: Information for Provisionable MPSs at EAGLE 5 ISS B*.

    Note: 127.0.0.1 is not a valid IP address for this operation.

```
EPAP A Static NAT Address:
```

23. Choose option `e` on the**Configure Static NAT Addresses Menu** to return to the **Configure Network Interfaces Menu**.

Note: If you are not configuring VIP provisioning addresses at this time, skip *Step 24* through *Step 26* and proceed to *Step 27*.

24. Choose option 7, Configure Provisioning VIP Addresses.

```
 /-----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
```

25. Enter the local and remote provisioning VIP addresses.

Note: 127.0.0.1 is not a valid IP address for this operation.

```
EPAP local provisioning Virtual IP Address [192.168.66.80]:
EPAP remote provisioning Virtual IP Address [192.168.66.78]:
```

26. 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*), skip menu option 3. Proceed to *Step 30*.

27. Choose option 3, Set Time Zone.

```
 /-------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               |
|----|------------------------------------|
|  8 | PDB Configuration Menu             |
|----|------------------------------------|
|  9 | Security                           |
```

```
|----|-----------------------------------|
|  e | Exit                              |
\-------------------------------------/
Enter Choice: 3
```

A Caution statement appears:

```
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...
```

28. After noting the caution, press **Return** to continue.

    You are prompted to confirm the time zone setting for MPS A and MPS B at this site.

```
Are you sure you wish to change the timezone for MPS A and B? [N]: y
```

29. Enter `y` to confirm the change.

    Pressing **Return** accepts the default of 'N' (or no) and the action is aborted. In this case, you are returned to the **EPAP Configuration Menu**.

    When the affirmative response `y` is given to change the time zone, the following prompt appears.

```
Enter a time zone:
```

    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, press **Return**, and a list of the valid names appears.

    A list of valid time zones is provided in Appendix A, *Time Zone File Names*.

    If an incorrect time zone is entered or if only **Return** is pressed, a list of all available time zone values appears. Select a value from this table. The time zone change does not take effect until the the MPS is rebooted.

    After setting the time zone successfully, you are returned to the **EPAP Configuration Menu**.

    Note: Option 4, ExchangeSecure Shell Keys, is 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). If you do not want to exchange secure shell keys, skip this step and proceed to *Step 34*.

30. Choose option 4, Exchange Secure Shell Keys.

```
 /-------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              |
|----|-----------------------------------|
|  8 | PDB Configuration Menu            |
|----|-----------------------------------|
|  9 | Security                          |
|----|-----------------------------------|
|  e | Exit                              |
\-----------------------------------------/
Enter Choice: 4
```

The **Exchange Secure Shell Keys Menu** appears.

```
MPS Side A:  hostname: tortola-a  hostid: a8c0883d
             Platform Version: 2.0.2-4.0.0_50.26.0
             Software Version: EPAP 1.0.1-4.0.0_50.34.0
             Fri Sep 16 07:37:32 EDT 2005
 /-----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
```

31. Select Option `1` to Exchange Keys with the mate.

    A prompt appears.

```
Are you sure you wish to exchange keys? [N]: y
```

32. Enter `y`.

    You are notified that secure shell keys have 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...
```

33. Press **Return** to confirm and continue with the exchange.

    A confirmation prompt appears.

```
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.
```

- Press **Return** ('N' or 'no') to abort the exchange action.
- Enter `Y` to confirm the exchange.

If you enter `y`, you are prompted for the password of the mate. Contact *Customer Care Center* for the password.

After entering the appropriate password, a verification of the exchange appears and you are returned to the **EPAP Configuration Menu**.

Note: If you want do not want to change the text-based UI password for the MPSs at this site, skip option5 and proceed to *Step 36*.

34. Enter option `5`, Change Password, 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               |
|----|------------------------------------|
|  8 | PDB Configuration Menu             |
|----|------------------------------------|
|  9 | Security                           |
|----|------------------------------------|
|  e | Exit                               |
\---------------------------------------/
Enter Choice: 5
```

You are prompted to confirm the action of changing the password for both servers (MPS A and MPS B) at this site.

```
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 ...
```

- Press **Return** to accept the default ('N' or 'no') and abort the action to change the password.
- Enter `y` invokes a prompt for the new password and re-entry of the password to confirm the entry.

35. Enter the new password, confirm, and press **Return** to return to the **EPAP Configuration Menu**.

Note: If you do not want to add anNTP server at this time, skip all steps related to option7 and proceed to *Step 42*.

36. Enter option 7, **Configure NTP Server**, 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             |
|----|----------------------------------|
|  8 | PDB Configuration Menu           |
|----|----------------------------------|
|  9 | Security                         |
|----|----------------------------------|
|  e | Exit                             |
\------------------------------------/
Enter Choice: 7
```

37. Enter option 2, Add External 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: 2
```

You are prompted to confirm the action of adding a new NTP Server.

- Press **Return** to accept the default ('N' or 'no') and abort the action to add an external NTP server.
- Enter y to add an external NTP server.

A prompt appears allowing you to add the IP address of the 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...
```

Note: 127.0.0.1 is not a valid IP address for this operation.

B: MPS on EAGLE 5 ISS B:

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.

N: Non-Provisionable MPS:

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.

Note: All NTP Server IP addresses shown are only examples.

The display shows the server verification occurring. A confirmation of a successful addition of the NTP server also appears.

38. Press **Return** to return to the **EPAP Configure NTP Server Menu**.
39. Enter option `1`, Display External NTP Server, 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
```

The IP address of the NTP S appears.

```
ntpserver1 192.168.61.157

Press return to continue...
```

40. If the External NTP Server IP address is correct, press **Return** to return to the **EPAP Configure NTP Server Menu**.
41. 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
```

42. Enter option `8`, **PDB 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               |
|----|------------------------------------|
|  8 | PDB Configuration Menu             |
```

```
|----|-----------------------------------|
|  9 | Security                          |
|----|-----------------------------------|
|  e | Exit                              |
\-----------------------------------------/
Enter Choice: 8
```

43. Enter option `1`, Configure PDB Network.

    Note: The procedure for configuring the PDB Network will be different for provisionable MPSs and non-provisionable MPSs, as described in the following choices.

```
 /-----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
```

    Refer to *Table 21: Information for Provisionable MPSs at EAGLE 5 ISS A* through *Table 24: Information for Non-Provisionable MPSs at EAGLE 5 ISS #2* for the information required to configure the PDB Network.

    Note: 127.0.0.1 is not a valid IP address for this operation.

    - **Only for provisionable MPSs (MPS of EAGLE 5 ISS A or MPS of EAGLE 5 ISS B):**

      A: MPS on EAGLE 5 ISS A:

      You must have the IP address for the MPS A of EAGLE 5 ISS B (recorded in *Table 22: Information for Provisionable MPSs at EAGLE 5 ISS B*).

      B: MPS on EAGLE 5 ISS B:

      You must have the IP address for the MPS A of EAGLE 5 ISS A (recorded in *Table 21: Information for Provisionable MPSs at EAGLE 5 ISS A*).

      Option `1` requires you to provide the IP address of the MPS A on EAGLE 5 ISS A and 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'.)

      You must 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 exchanged.

      If you configure the PDBA Proxy feature, the IP address for MPS B (mate non-provisionable MPS) on EAGLE 5 ISS B is required.

      Note: References to 'local' and 'remote,' by the software configuration, are relative to the MPS that is actively executing the configuration software.

```
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...
```

Upon pressing **Return**, you are returned to the **Configure PDB Menu**. If you are configuring only provisionable MPSs, proceed to *Step 44*.

- **Only for non-provisionable MPSs:**

  N: Non-Provisionable MPS:

  You 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 21: Information for Provisionable MPSs at EAGLE 5 ISS A* and *Table 22: Information for Provisionable MPSs at EAGLE 5 ISS B*).

  Option 1 requires you 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...
```

Upon pressing **Return**, you are returned to the **Configure PDB Menu**.

Note: The default homing policy for a pair of provisionable MPSs is specific homing to the local PDB. If you do not want to configure active/standby homing, skip option2,**RTDB Homing Menu**, and proceed with *Step 47*.

44. Enter option 2, **RTDB Homing 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
```

45. Enter option 1, 2, or 3 from the **RTDB Homing Menu**.

You 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* .

```
 /-------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)
```

- Option 1 for specific homing:

  Select one of the two IP addresses on the list, as shown in the 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:

  Choose whether to allow updates from the standby PDB. If updates from the standby PDB are not allowed, the choice must be confirmed, as shown in the 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:

  Choose 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 the 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.
  ```

Upon making a selection, you are returned to the **RTDB Homing Menu**.

46. Enter option e to exit the **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: e
```

47. Enter option 5, Change Auto DB Recovery, to enable the Automated Database Recovery feature.

Note: This step 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
```

The following output appears.

```
Auto DB Recovery is currently DISABLED.
Do you want to ENABLE Auto DB Recovery? [N]: y
```

48. Enter option 6, Change PDBA Proxy State, to enable the PDBA Proxy feature.

Note: You must perform this step on both provisionable MPS A of a mated pair if this feature is utilized.

```
 /-----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
```

The following output appears.

```
PDBA PROXY is currently DISABLED.
Do you want to ENABLE PDBA Proxy? [N]: y
```

Note:

The next action depends on 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.

A: MPS on EAGLE 5 ISS A:

Proceed to *Step 49*.

N: Non-Provisionable MPS:

Proceed to *Step 52*.

B: MPS on EAGLE 5 ISS B:

Proceed to *Step 55*.

A: MPS on EAGLE 5 ISS A:

Perform *Step 49* through *Step 52* only for MPS A and B on EAGLE 5 ISS A.

49. Enter option e to exit 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: e
```

50. 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               |
|----|------------------------------------|
|  8 | PDB Configuration Menu             |
|----|------------------------------------|
|  e | Exit                               |
\------------------------------------/
Enter Choice: e
```

A Caution statement appears.

```
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...
```

51. Press **Return** in response to the cautionary message stating that the current MPS is not completely configured.

    A: MPS on EAGLE 5 ISS A:

    The configuration of the MPSs on EAGLE 5 ISS A is not complete until its PDB is created. The MPSs on the EAGLE 5 ISS A PDB are created during the initial configuration of the MPS A on EAGLE 5 ISS B, which automatically replicates the PDB on the MPS on EAGLE 5 ISS A at the same time.

    You have completed the initial configuration of MPSs on EAGLE 5 ISS A. You can begin the configuration of the MPSs on EAGLE 5 ISS B.

    

    CAUTION: Do not attempt to reboot the MPSs on EAGLE 5 ISS A at this point in the configuration. Rebooting the MPSs at EAGLE 5 ISS A and EAGLE 5 ISS B is performed concurrently when the configuration of the MPSs at EAGLE 5 ISS B is completed.

    N: Non-Provisionable MPS:

    Perform *Step 52* and *Step 54* only for a non-provisionable MPS

52. 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
```

53. Enter option 6, **Platform 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              |
|----|-----------------------------------|
|  8 | PDB Configuration Menu            |
|----|-----------------------------------|
|  9 | Security                          |
|----|-----------------------------------|
|  e | Exit                              |
\----------------------------------------/
Enter Choice: 6
```

54. Proceed to *Step 57*.

B: MPS on EAGLE 5 ISS BA:

Perform *Step 55* only for MPS A and B on EAGLE 5 ISS B.

55. Enter option 4, Create PDB.

```
 /-----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
```

This action creates the PDB on the present EPAP, and automatically replicates it on the former EPAP.

After you receive an output indicating successful creation of the PDBs, you are returned to the **EPAP Configuration Menu**.

- During configuration of MPSs on EAGLE 5 ISS B, if the time zone was not changed (*Step 27*) the EPAP initial configuration of MPSs on EAGLE 5 ISS B is now complete.

- During configuration of MPSs on EAGLE 5 ISS B, if the Backup Provisioning Network (*Step 14*) was not configured on either MPS, the EPAP initial configuration of MPSs on EAGLE 5 ISS B is now complete.
- Otherwise continue with *Step 56* to reboot both MPS pairs on EAGLE 5 ISS A and on EAGLE 5 ISS B.

56. Enter option 6, **Platform 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              |
|----|-----------------------------------|
|  8 | PDB Configuration Menu            |
|----|-----------------------------------|
|  9 | Security                          |
|----|-----------------------------------|
|  e | Exit                              |
\---------------------------------------/
Enter Choice: 6
```

57. Enter option 3, Reboot MPS.

```
 /-----EPAP Platform Menu-\
/-------------------------\
|  1 | Initiate Upgrade   |
|----|--------------------|
|  2 | Eject CD           |
|----|--------------------|
|  3 | Reboot MPS         |
|----|--------------------|
|  4 | Halt MPS           |
|----|--------------------|
|  5 | MySQL Backup       |
|----|--------------------|
|  6 | RTDB Backup        |
|----|--------------------|
|  7 | PDB Backup         |
|----|--------------------|
|  e | Exit               |
\-------------------------/
Enter Choice: 3
```

An output appears requiring you to select the MPSs to reboot.

```
Reboot MPS A, MPS B or [BOTH]:
```

58. Enter `BOTH` (the default value) when prompted on whether MPS A, MPS B or `BOTH` sides are to be rebooted.

The reboot of both MPS A and MPS B begins when you press **Return**.

When the MPS server pair on EAGLE 5 ISS B is rebooted, the **Platform Menu** may re-appear; however, the connection to the MPS server is closed, and you are returned to the system prompt.

When a ssh session is closed, you are returned to the previous ssh session. You are back at the system prompt of MPS A of EAGLE 5 ISS A.

59. Log in as `epapconfig` to invoke the EPAP Configuration. Type the following command and the password.

```
$su epapconfig

Password:
```

The **EPAP Configuration Menu** appears.

60. Enter option 6, **Platform 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               |
|----|------------------------------------|
|  8 | PDB Configuration Menu             |
|----|------------------------------------|
|  9 | Security                           |
|----|------------------------------------|
|  e | Exit                               |
\---------------------------------------/
Enter Choice: 6
```

61. Enter option 3, Reboot MPS.

```
 /-----EPAP Platform Menu-\
/-------------------------\
|  1 | Initiate Upgrade    |
|----|---------------------|
|  2 | Eject CD            |
|----|---------------------|
|  3 | Reboot MPS          |
|----|---------------------|
|  4 | Halt MPS            |
|----|---------------------|
|  5 | MySQL Backup        |
|----|---------------------|
|  6 | RTDB Backup         |
|----|---------------------|
|  7 | PDB Backup          |
|----|---------------------|
|  e | Exit                |
```

```
\-------------------------/
Enter Choice: 3
```

62. 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 you press **Return**.

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.

B: MPS on EAGLE 5 ISS B:

The initial configuration of MPSs on EAGLE 5 ISS B is complete. Both MPSs on EAGLE 5 ISS A and MPSs on B are configured and rebooted.

Configure the non-provisionable MPSs, if appropriate.

N: Non-Provisionable MPS:

The initial configuration of the non-provisionable MPSs is complete.

The non-provisionable MPS A and B, for the current site, are configured and rebooted. Repeat this procedure, if necessary, until all remaining non-provisionable MPSs are configured.

Appendix A

Time Zone File Names

Topics:

This appendix provides a listing of valid time zone file names.

Time Zone File Names

This appendix lists the valid UNIX file names, from the /usr/share/lib/zoneinfo /directory, for setting the time zone in EPAP software configuration. The initial default value for the time zone is "US/Eastern".

The Select Time Zone menu (refer to *Set Time Zone*) 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.

Table 28: Time Zone File Names

Enter a time zone file (relative to /usr/share/lib/zoneinfo):		
Valid time zone files are:		
Australia/Broken_Hill	Australia/LH	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* .

Glossary

A

A-Port	ANSI-41 Mobile Number Portability A feature that enables IS-41 subscribers to change their service provider while retaining the same Mobile Dialed Number (MDN).
ACK	Data Acknowledgement
ASCII	American Standard Code for Information Interchange

B

Blacklist	Provisioning Blacklist. An indication that a call from the calling party is not valid.

C

CD	Carrier Detect Compact Disk
CSV	Comma-separated value The comma-separated value file format is a delimited data format that has fields separated by the comma character and records separated by newlines (a newline is a special character or sequence of characters signifying the end of a line of text).

D

Database	All data that can be administered by the user, including cards, destination point codes, gateway screening tables, global title translation tables, links, LNP services, LNP service

D

	providers, location routing numbers, routes, shelves, subsystem applications, and 10 digit telephone numbers.
DB	Database
DN	Directory number A DN can refer to any mobile or wireline subscriber number, and can include MSISDN, MDN, MIN, or the wireline Dialed Number.
DSM	Database Service Module. The DSM provides large capacity SCCP/database functionality. The DSM is an application card that supports network specific functions such as EAGLE Provisioning Application Processor (EPAP), Global System for Mobile Communications (GSM), EAGLE Local Number Portability (ELAP), and interface to Local Service Management System (LSMS).

E

EIR	Equipment Identity Register A network entity used in GSM networks, as defined in the 3GPP Specifications for mobile networks. The entity stores lists of International Mobile Equipment Identity (IMEI) numbers, which correspond to physical handsets (not subscribers). Use of the EIR can prevent the use of stolen handsets because the network operator can enter the IMEI of these handsets into a 'blacklist' and prevent them from being registered on the network, thus making them useless.

E

EPAP	EAGLE Provisioning Application Processor
EPAP-related features	Features that require EPAP connection and use the Real Time Database (RTDB) for lookup of subscriber information. • ANSI Number Portability Query (AINPQ) • ANSI-41 AnalyzedInformation Query – no EPAP/ELAP (ANSI41 AIQ) • Anytime Interrogation Number Portability (ATI Number Portability, ATINP) • AINPQ, INP, G-Port SRI Query for Prepaid, GSM MAP SRI Redirect, IGM, and ATINP Support for ROP • A-Port Circular Route Prevention (A-Port CRP) • Equipment Identity Register (EIR) • G-Flex C7 Relay (G-Flex) • G-Flex MAP Layer Routing (G-Flex MLR) • G-Port SRI Query for Prepaid • GSM MAP SRI Redirect to Serving HLR (GSM MAP SRI Redirect) • GSM Number Portability (G-Port) • IDP A-Party Blacklist • IDP A-Party Routing • IDP Relay Additional Subscriber Data (IDPR ASD) • IDP Relay Generic Routing Number (IDPR GRN) • IDP Service Key Routing (IDP SK Routing) • IDP Screening for Prepaid • INAP-based Number Portability (INP) • Info Analyzed Relay Additional Subscriber Data (IAR ASD)

E

- Info Analyzed Relay Base (IAR Base)
- Info Analyzed Relay Generic Routing Number (IAR GRN)
- Info Analyzed Relay Number Portability (IAR NP)
- INP Circular Route Prevention (INP CRP)
- IS41 Mobile Number Portability (A-Port)
- IS41 GSM Migration (IGM)
- MNP Circular Route Prevention (MNPCRP)
- MO-based GSM SMS NP
- MO-based IS41 SMS NP
- MO SMS Generic Routing Number (MO SMS GRN)
- MO- SMS B-Party Routing
- MO SMS IS41-to-GSM Migration
- MT-based GSM SMS NP
- MT-based GSM MMS NP
- MT-based IS41 SMS NP
- MTP Routed Messages for SCCP Applications (MTP Msgs for SCCP Apps)
- MTP Routed Gateway Screening Stop Action (MTPRTD GWS Stop Action)
- Portability Check for MO SMS
- Prepaid IDP Query Relay (IDP Relay, IDPR)
- Prepaid SMS Intercept Phase 1 (PPSMS)
- Service Portability (S-Port)
- S-Port Subscriber Differentiation
- Triggerless ISUP Framework Additional Subscriber Data (TIF ASD)
- Triggerless ISUP Framework Generic Routing Number (TIF GRN)
- Triggerless ISUP Number Portability (TIF NP)
- Triggerless ISUP Framework Number Substitution (TIF NS)

E

- Triggerless ISUP Framework SCS Forwarding (TIF SCS Forwarding)
- Triggerless ISUP Framework Simple Number Substitution (TIF SNS)
- Voice Mail Router (V-Flex)

G

GB	Gigabyte — 1,073,741,824 bytes
G-Flex	GSM Flexible numbering A feature that allows the operator to flexibly assign individual subscribers across multiple HLRs and route signaling messages, based on subscriber numbering, accordingly.
GMT	Greenwich Mean Time
G-Port	GSM Mobile Number Portability A feature that provides mobile subscribers the ability to change the GSM subscription network within a portability cluster, while retaining their original MSISDN(s).
GPS	Global Positioning System
GS	Gateway Switch
GUI	Graphical User Interface The term given to that set of items and facilities which provide the user with a graphic means for manipulating screen data rather than being limited to character based commands.

I

I

IMEI	International Mobile Equipment Identifier
IMSI	International Mobile Subscriber Identity
IMT	Inter-Module-Transport The communication software that operates the inter-module-transport bus on all cards except the LIMATM, DCM, DSM, and HMUX.
INP	INAP-based Number Portability Tekelec's INP can be deployed as a stand-alone or an integrated signal transfer point/number portability solution. With Tekelec's stand-alone NP server, no network reconfiguration is required to implement number portability. The NP server delivers a much greater signaling capability than the conventional SCP-based approach. Intelligent Network (IN) Portability
IP	Internet Protocol IP specifies the format of packets, also called datagrams, and the addressing scheme. The network layer for the TCP/IP protocol suite widely used on Ethernet networks, defined in STD 5, RFC 791. IP is a connectionless, best-effort packet switching protocol. It provides packet routing, fragmentation and re-assembly through the data link layer.
IP Address	The location of a device on a TCP/IP network. The IP Address is a number in dotted decimal notation

I

	which looks something like [192.168.1.1].
IPM	Initial Product Manufacture
IS-ANR	In Service - Abnormal The entity is in service but only able to perform a limited subset of its normal service functions.
IS-NR	In Service - Normal
ISS	Integrated Signaling System

L

LAN	Local Area Network A private data network in which serial transmission is used for direct data communication among data stations located in the same proximate location. LAN uses coax cable, twisted pair, or multimode fiber. See also STP LAN.
LED	Light Emitting Diode An electrical device that glows a particular color when a specified voltage is applied to it.
LIM	Link Interface Module Provides access to remote SS7, IP and other network elements, such as a Signaling Control Point (SCP) through a variety of signaling interfaces (DS0, MPL, E1/T1 MIM, LIM-ATM, E1-ATM, IPLIMx, IPGWx). The LIMs consist of a main assembly and possibly, an interface

L

	appliqué board. These appliqués provide level one and some level two functionality on SS7 signaling links.
Load Sharing	A type of routing used by global title translation to route MSUs This type of routing is used when a second point code and subsystem is defined for the primary point code and subsystem. Traffic is shared equally between the replicated point codes and subsystems.

M

MDN	Mobile Dialed Number Mobile Directory Number
MEA	Mismatch of Equipment and Attributes
MIN	Mobile Identification Number
MPS	Multi-Purpose Server The Multi-Purpose Server provides database/reload functionality and a variety of high capacity/high speed offboard database functions for applications. The MPS resides in the General Purpose Frame. Messages Per Second A measure of a message processor's performance capacity. A message is any Diameter message (Request or Answer) which is received and processed by a message processor.
MSISDN	Mobile Station International Subscriber Directory Number

M

The MSISDN is the network specific subscriber number of a mobile communications subscriber. This is normally the phone number that is used to reach the subscriber.

MSU — Message Signal Unit

The SS7 message that is sent between signaling points in the SS7 network with the necessary information to get the message to its destination and allow the signaling points in the network to set up either a voice or data connection between themselves. The message contains the following information:

- The forward and backward sequence numbers assigned to the message which indicate the position of the message in the traffic stream in relation to the other messages.
- The length indicator which indicates the number of bytes the message contains.
- The type of message and the priority of the message in the signaling information octet of the message.
- The routing information for the message, shown in the routing label of the message, with the identification of the node that sent message (originating point code), the identification of the node receiving the message (destination point code), and the signaling link selector which the EAGLE 5 ISS uses to pick which link set and signaling link to use to route the message.

N

NAK — Negative Acknowledgment

N

NAT	Network Address Translation
NE	Network Element An independent and identifiable piece of equipment closely associated with at least one processor, and within a single location. Network Entity
NTP	Network Time Protocol

O

OAM	Operations, Administration, and Maintenance The application that operates the Maintenance and Administration Subsystem which controls the operation of the EAGLE 5 ISS.
OOS-MT	Out of Service - Maintenance The entity is out of service and is not available to perform its normal service function. The maintenance system is actively working to restore the entity to service.
OS	Operations Systems

P

PC	Point Code The identifier of a signaling point or service control point in a network. The format of the point code can be one of the following types: • ANSI point codes in the format network indicator-network cluster-network cluster member (**ni-nc-ncm**).

P

	• Non-ANSI domestic point codes in the format network indicator-network cluster-network cluster member (**ni-nc-ncm**). • Cluster point codes in the format network indicator-network cluster-* or network indicator-*-*. • ITU international point codes in the format **zone-area-id**. • ITU national point codes in the format of a 5-digit number (**nnnnn**), or 2, 3, or 4 numbers (members) separated by dashes (**m1-m2-m3-m4**) as defined by the Flexible Point Code system option. A group code is required (**m1-m2-m3-m4-gc**) when the ITUDUPPC feature is turned on. • 24-bit ITU national point codes in the format main signaling area-subsignaling area-service point (**msa-ssa-sp**).
PCI	Peripheral Component Interface
PDB	Provisioning Database
PDBA	Provisioning Database Application There are two Provisioning Database Applications (PDBAs), one in EPAP A on each EAGLE 5 ISS. They follow an Active/Standby model. These processes are responsible for updating and maintaining the Provisioning Database (PDB).
PDBI	Provisioning Database Interface The interface consists of the definition of provisioning messages only. The customer must write a client application that uses the PDBI

P

	request/response messages to communicate with the PDBA.
PMTC	Peripheral Maintenance
PPP	Point-to-Point Protocol
Provisioning Blacklist	A list of ranges that are prohibited from being used as DNs, DN Blocks, and IMSI address strings.
PT	Portability Type

R

Restricted	The network management state of a route, link set, or signaling link that is not operating properly and cannot carry all of its traffic. This condition only allows the highest priority messages to sent to the database entity first, and if space allows, followed by the other traffic. Traffic that cannot be sent on the restricted database entity must be rerouted or the traffic is discarded.
RFC	Request for Comment RFCs are standards-track documents, which are official specifications of the Internet protocol suite defined by the Internet Engineering Task Force (IETF) and its steering group the IESG.
RMTP	Reliable Multicast Transport Protocol
RN	Routing Number
RTDB	Real Time Database

S

SCCP	Signaling Connection Control Part
SCM	System Configuration Manager
SCP	Service Control Point Service Control Points (SCP) are network intelligence centers where databases or call processing information is stored. The primary function of SCPs is to respond to queries from other SPs by retrieving the requested information from the appropriate database, and sending it back to the originator of the request.
	Secure Copy
Service Module card	DSM card or E5-SM4G card that contains the Real Time Database (RTDB) downloaded from an EPAP or ELAP system.
SFTP	SSH File Transfer Protocol (sometimes also called Secure File Transfer Protocol) A client-server protocol that allows a user on one computer to transfer files to and from another computer over a TCP/IP network over any reliable data stream. It is typically used over typically used with version two of the SSH protocol.
SOG	Service Order Gateway
SP	Signaling Point A set of signaling equipment represented by a unique point code within an SS7 domain.

S

SSH	Secure Shell A protocol for secure remote login and other network services over an insecure network. SSH encrypts and authenticates all EAGLE 5 ISS IPUI and MCP traffic, incoming and outgoing (including passwords) to effectively eliminate eavesdropping, connection hijacking, and other network-level attacks.
STP	Signal Transfer Point The STP is a special high-speed switch for signaling messages in SS7 networks. The STP routes core INAP communication between the Service Switching Point (SSP) and the Service Control Point (SCP) over the network.

T

TCP	Transfer Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol

U

UAM	Unsolicited Alarm Message A message sent to a user interface whenever there is a fault that is service-affecting or when a previous problem is corrected. Each message has a trouble code and text associated with the trouble condition.
UDP	User Datagram Protocol
UI	User Interface

U

UTC	Coordinated Universal TIme

V

V-Flex	Voicemail Flexible Routing An advanced database application based on the industry proven EAGLE 5 ISS. Deployed as a local subsystem on the EAGLE platform, V-Flex centralizes voicemail routing.
VSCCP	VxWorks Signaling Connection Control Part The application used by the Service Module card to support EPAP-related features and LNP features. If an EPAP-related or LNP feature is not turned on, and a Service Module card is present, the VSCCP application processes normal GTT traffic.

W

WAN	Wide Area Network