Oracle® Communications

EAGLE Application Processor Administration Guide

Release 17.1
G35524-01
June 2025

Oracle Communications EAGLE Application Processor Administration Guide, Release 17.1

G35524-01

Copyright © 2000, 2025, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

B Time Zones

My Oracle Support

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support can assist you with My Oracle Support registration.

Call the Customer Access Support main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

- For Technical issues such as creating a new Service Request (SR), select **1**.
- For Non-technical issues such as registration or assistance with My Oracle Support, select **2**.
- For Hardware, Networking and Solaris Operating System Support, select **3**.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Acronyms

The following table provides information about the acronyms used in the document:

Table Acronyms

Acronym	Definition
STP	Signal Transfer Point
ADR	Automated Database Recovery
CGI	Common Gateway Interface
EDLM	EPAP Service Module Database Levels Monitor
EPAP	EAGLE Application Processor
GMT	Greenwich Mean Time
GPS	Global Positioning System
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
IMSI	International Mobile Subscriber Identity
LAN	Local Area Network
MPS	Multi Purpose Server
NTP	Network Time Protocol
PDB	Provisioning Database
PDBA	Provisioning Database Application
PDBI	Provisioning Database Interface
RMTP	Reliable Multicast Transport Protocol
RTDB	Real Time Database
SOG	Service Order Gateway
SR	Service Request
UTP	Universal Time Coordinated
WAN	Wide Area Network

What's New in This Guide

This section introduces the documentation updates for Release 17.1 in Oracle Communications EAGLE Application Processor Administration Guide.

Release 17.1 - G35524-01, June 2025

Updated the supported data capacities in step 2 in the Standalone PDB Capacity Configuration section.

1 Introduction

This chapter provides a brief overview of the Oracle Communications EAGLE Application Processor which includes Oracle Communications EAGLE Application Processor Provisioning (EPAP) and Oracle Communications EAGLE Application Processor Non-provisioning (EPAP). The chapter also includes the scope, audience, and organization of the manual; how to find related publications; and how to contact Oracle for assistance.

1.1 Overview

This manual describes the administration of the Oracle Communications EAGLE Application Processor which includes Oracle Communications EAGLE Application Processor Provisioning (**EPAP**) and Oracle Communications EAGLE Application Processor Non-provisioning (EPAP).

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 Oracle Communications EAGLE. EPAP supports the **EPAP-related features**, which are listed in the Glossary.

2
Functional Description

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

2.1 General Description

The EAGLE Application Processor (EPAP) 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:

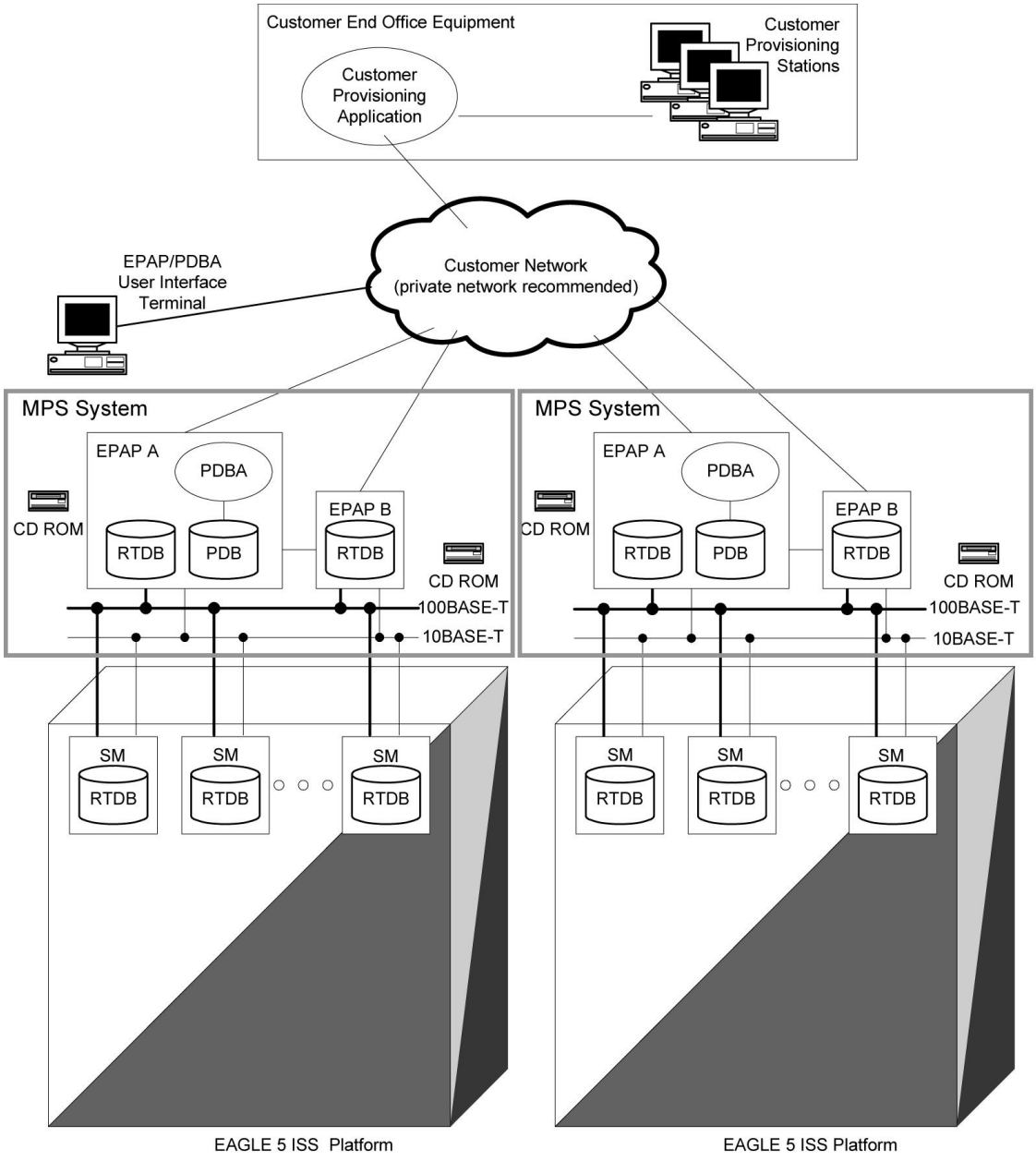
- Accept and store data provisioned by the customer
- Update customer provisioning data and reload databases on the **Service Module** cards in the Multi Purpose Server (MPS)

Operational Flow

The Multi Purpose Server (MPS) hardware platform supports high speed provisioning of large databases for the EAGLE. 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 2-1 Mated EAGLE Platform Example



EPAP Types

Each EPAP can be configured as one of three types:

- Mixed EPAP - This configuration supports the Real Time Database (RTDB) and the Provisioning Database (PDB), along with the associated processes for both. Mixed EPAP is identified as an Oracle Communications EAGLE Application Processor Provisioning (EPAP). Mixed EPAP is described in Mixed EPAP. The majority of the content in this chapter and subsequent chapters applies to Mixed EPAP. EAGLE interfaces, Service Module cards, and Mate Servers are supported by Mixed EPAP.
- Non-Provisioning EPAP - This configuration is similar to Mixed EPAP, but supports only the Real Time Database (RTDB) and its associated processes. The Provisioning Database (PDB) is not supported by this configuration. Non-Provisioning EPAP is identified as an

Oracle Communications EAGLE Application Processor Non-provisioning (EPAP). Content in this chapter and subsequent chapters which is PDB-related does not apply to the Non-Provisioning EPAP configuration.

- Standalone PDB EPAP - This configuration supports only the Provisioning Database (PDB) and its associated processes. The Real Time Database (RTDB), EAGLE interfaces, Service Module cards, Mate Servers, and associated processes are not supported by this configuration. Standalone PDB EPAP is identified as an Oracle Communications EAGLE Application Processor Provisioning (EPAP). Content in this chapter and subsequent chapters which is RTDB-related or requires a Mate server or EAGLE interface does not apply to this configuration. Refer to Standalone PDB EPAP for specific information about the Standalone PDB EPAP configuration.

Mixed EPAP

An **EPAP** system consists of two mated EPAP processors (A and B) installed as part of an EAGLE. A set of **Service Module** cards is part of the EAGLE. 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 2-2 shows the network layout and examples of typical IP addresses of the network elements. The shaded portion represents a second EAGLE and mated EPAPs deployed as a mated EAGLE.

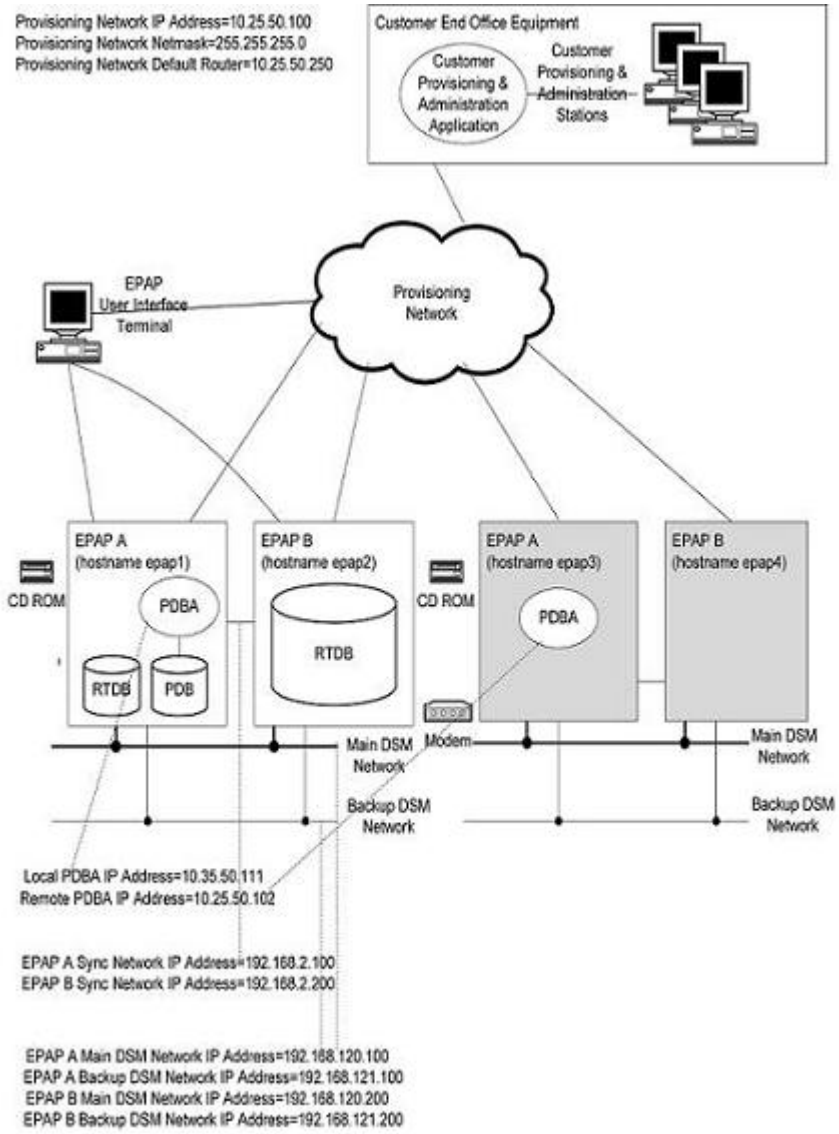
The EPAP system maintains the Real Time Database (RTDB) required to provision the EAGLE Service Module cards, and maintains redundant copies of both databases on each mated EPAP.

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 2-2 Example of EPAP Network IP Addresses



2.1.1 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. 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.
   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 2-1 lists the possible combinations.

> **Note:**
>
> In the absence of Switch 1B (i.e., when switch 1B is down), the EPAP Sync network will not be available. In this scenario, if the EPAP software is restarted, it may cause both EPAPs (A and B) to go in 'Active' state, causing problems with EAGLE SM cards provisioning.

Table 2-1 EPAP Switchover Matrix

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

The following are exceptions to the switchover matrix:

1. If the mate maintenance component cannot be contacted and the mate EPAP is not visible on the DSM networks, the EPAP assumes an Active role if any DSMs are visible on the DSM networks.
2. If the EPAP GUI menu item is used to force an EPAP to Standby role, no condition will cause it to become Active until the user removes the interface restriction with another menu item. See Force Standby 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 .

2.1.2 EPAP Component Overview

The major components that run on the Oracle Communications EAGLE Application Processor Provisioning (**EPAP**) and Oracle Communications EAGLE Application Processor Non-provisioning (**EPAP**) are shown in the following table.

Table 2-2 Major Component Tasks

Task	EPAP Provisioning	EPAP Non-provisioning	Standalone PDB EPAP
Provisioning Database Application (**PDBA**)	X		X
Provisioning Database (**PDB**)	X		X
Maintenance task	X	X	X
Real Time Database (**RTDB**)	X	X	
RTDB Audit	X	X	
DSM Provisioning	X	X	
EPAP Service Module Database Levels Monitor (EDLM)	X	X	

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 User's Guide*.

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.

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 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.

The EPAP SM Database Levels Monitor (EDLM) continuously monitors the current database level of all active (in-service) Service Module Cards on EAGLE. If all of the Service Module Cards stop receiving database updates from the Active EPAP server, EDLM automatically resets the RMTP channels at the EPAP end. This results in a re-established connection with the Service Module Cards on EAGLE.

2.1.3 Provisioning Database Interface

Provisioning clients connect to the **EPAPs** through the **Provisioning Database Interface** (**PDBI**). The PDBI provides commands that communicate provisioning information from the customer database to the Provisioning Database (PDB) in the Active PDBA on EAGLE. 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 User's Guide*.

2.1.4 Network Connections

This section describes the four types of **EPAP** network connections.

- SM Networks
- EPAP Sync Network
- Customer Network

SM Networks

The **SM** networks carry provisioning data from the Real Time Databases (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 platform.

The EAGLE 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, the term *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 Reference*.

Network speeds when installed Service Module cards are a mix of E5-SM4G cards and E5-SM8G-B cards:

- Main SM network - 1 Gbps (1000 Mbps), full duplex
- Backup SM network - 1 Gbps (1000 Mbps), full duplex

Refer to the "Switch Configuration" procedure in *Upgrade/Installation Procedure* for EPAP.

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 2-3 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 2-3 IP Addresses on the SM Network

Octet	Derivation
1	192

Table 2-3 (Cont.) IP Addresses on the SM Network

Octet	Derivation
2	168
3	Usually configured as: 120 for SM main network 121 for SM backup network
4	100 for EPAP A 200 for EPAP B 1 - 32 for SM 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.

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 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.

2.1.5 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

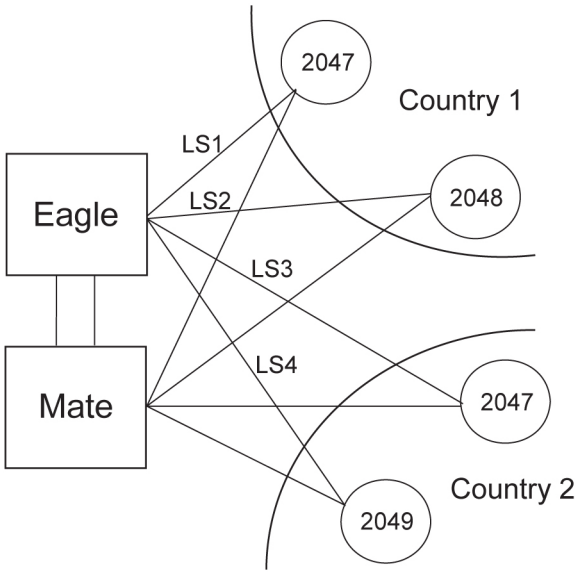
The EPAP Support of EAGLE ITU Duplicate Point Code feature allows point codes to be provisioned in the PDB using a two-character group code. This feature works with the EAGLE ITU Duplicate Point Code feature, which allows an EAGLE mated pair to route traffic for two or more countries with overlapping (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, refer to the `chg-feat` command in *Commands User's Guide*.

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 to discriminate between two nodes in different countries with the same true point code. The EAGLE uses the group code to distinguish between the two nodes. The group code is used internally in the EAGLE only and is assigned to an incoming message based on the linkset on which it was received.

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

Figure 2-3 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 2-3, 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 User's Guide*.

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 - SS7 User's Guide*.

2.1.6 Asynchronous Replication

Asynchronous replication is the method used to synchronize the various **Provisioning Database**s (**PDB**s) 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 contact My Oracle Support.
- **Standby PDBA Falling Behind** is a minor alarm that signals that one EAGLE of the pair may have received updates at a longer interval than the other EAGLE. This alarm condition does not indicate data loss or corruption.

2.1.7 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.

2.1.8 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.

> **Note:**
>
> If the EPAP A is connected with a Standby PDB and non-provisioning nodes, the nodes will not be updated. These nodes will have to wait until the main Provisioning Network of the EPAP A is UP. The customer can provision Backup IP Addresses in the Standby and Non-provisioning nodes.

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.

2.1.9 Provisioning Multiple EPAPs Support

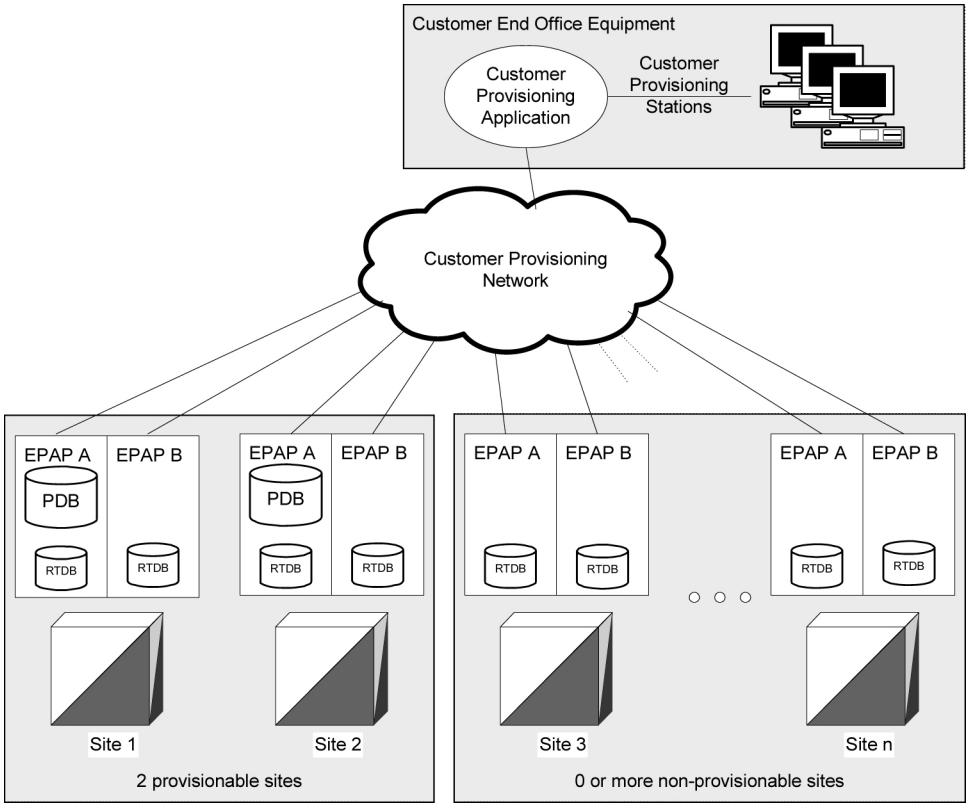
The Provisioning Multiple **EPAP**s Support feature provides the ability for a single **PDBI** connection to provision up to four **MPS**s. Each MPS contains an EPAP A and an EPAP B). The PDBI connects to and provisions an EPAP A and a Provisioning Database (**PDB**). The remaining three MPSs are automatically provisioned from the active EPAP A. This allows users to add additional EAGLEs without changing their provisioning systems and without provisioning the EAGLEs 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 **RTDB**s 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 2-4 shows a view of the provisionable and non-provisionable EPAPs.

Figure 2-4 Support for Provisioning Multiple EPAPs



2.1.10 Selective Homing of EPAP RTDBs

The Selective Homing of **EPAPRTDB**s 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 State.

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 2-4 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 2-4 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 2-5 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 2-5 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
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 2-6 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 2-6 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
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 2-7 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 2-7 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 2-8 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 2-8 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 2-4.) 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 My Oracle Support for information.

2.1.11 File Transfer Options

> **Note:**
>
> For the import to work properly, it's necessary that "PDB_RTDB_SYNC" is set to "YES."

Check the current value of "PDB_RTDB_SYNC" by running the command:

```
uiEdit | grep PDB_RTDB_SYNC
```

If it's set to "NO", set it to "YES" before attempting to import. Run the following command:

```
uiEdit PDB_RTDB_SYNC YES
```

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 3-21.

```
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 3-21.

```
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 3-21

```
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 Guide* 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.

If the export file needs to be automatically transferred to a remote server, the file name should start with "pdbAutoExport".

For example: "`pdbAutoExport_<hostname>_<YYYYMMDDhhmm>`".

For instance, if the following files are present in the `/var/TKLC/epap/free/pdbi_export` directory:

```
pdbExport_Arica-A_202411251131.tar.gz
```

`pdbAutoExport_Arica-A_20241125113147.tar.gz`

`testPdbFile.tar.gz`

Only `pdbAutoExport_Arica-A_20241125113147.tar.gz` will be automatically transferred to the remote server (if Configure File Transfer is enabled). The rest will remain in the directory for manual or other intended use.

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. While performing the "Export PDB to File", the output filename format is *pdbAutoExport_<hostname>_<YYYYMMDDhhmmss>*, which will save the file in `pdbi_export`. The PDBA must be active at the scheduled time of export for the file to be exported.

2.1.12 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.

2.1.13 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 2-9 Example 1 EPAP ADR

Active PDBA (Node 1)	Standby PDBA (Node 2)
DB Level-704	DB Level-700
Updates to replicate to standby PDBA	
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 2-10 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.

2.1.14 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
- The EPAP PDBA Proxy feature is not supported for Standalone PDB EPAP.
- SSH tunneling does not work with the PDB proxy feature as SSH tunneling works with server IP and not with VIP.

> **Note:**
>
> If a replication error (REPLERR) occurs while using the EPAP PDBA Proxy feature, manual intervention is required. Contact My Oracle Support.

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.

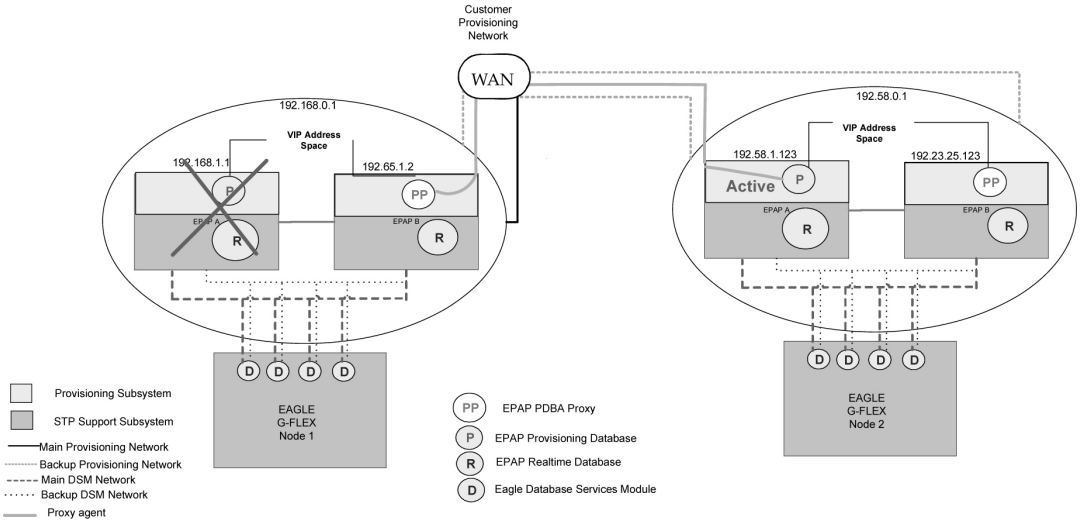
A fault (server failure) on the Node 1 with the active PDBA is shown in Figure 2-5:

- 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 2-5 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 .

2.1.15 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.

2.1.16 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 2-11 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. The default threshold value is 95%.

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 critical 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%, 90% and 95% 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. The 90% and 95% alarms have the same functionality. If the 90% alarm is active when the 95% alarm is triggered, the 90% alarm is replaced by the 95% alarm until the 95% alarm clears, etc.

2.2 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.

2.3 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 2-6 and the DSM provisioning task interface is shown in Figure 2-7.

Figure 2-6 DSM Provisioning Network Architecture

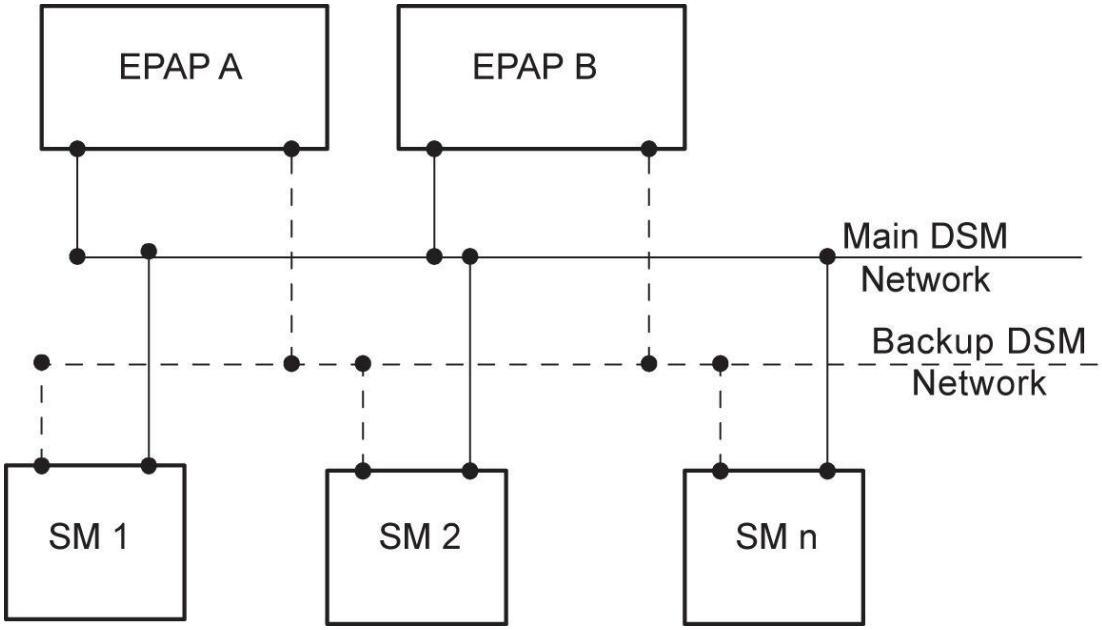
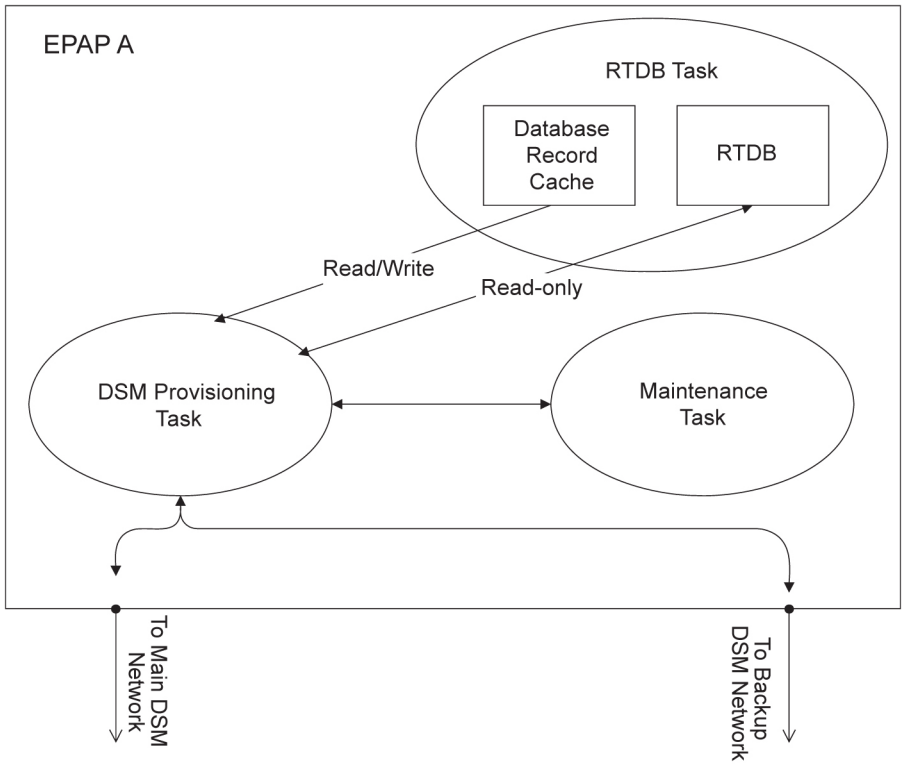


Figure 2-7 DSM Provisioning Task Interfaces



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

- EPAP A, Main DSM network

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

Provisioning and other data is broadcast on one of these channels to all of the 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

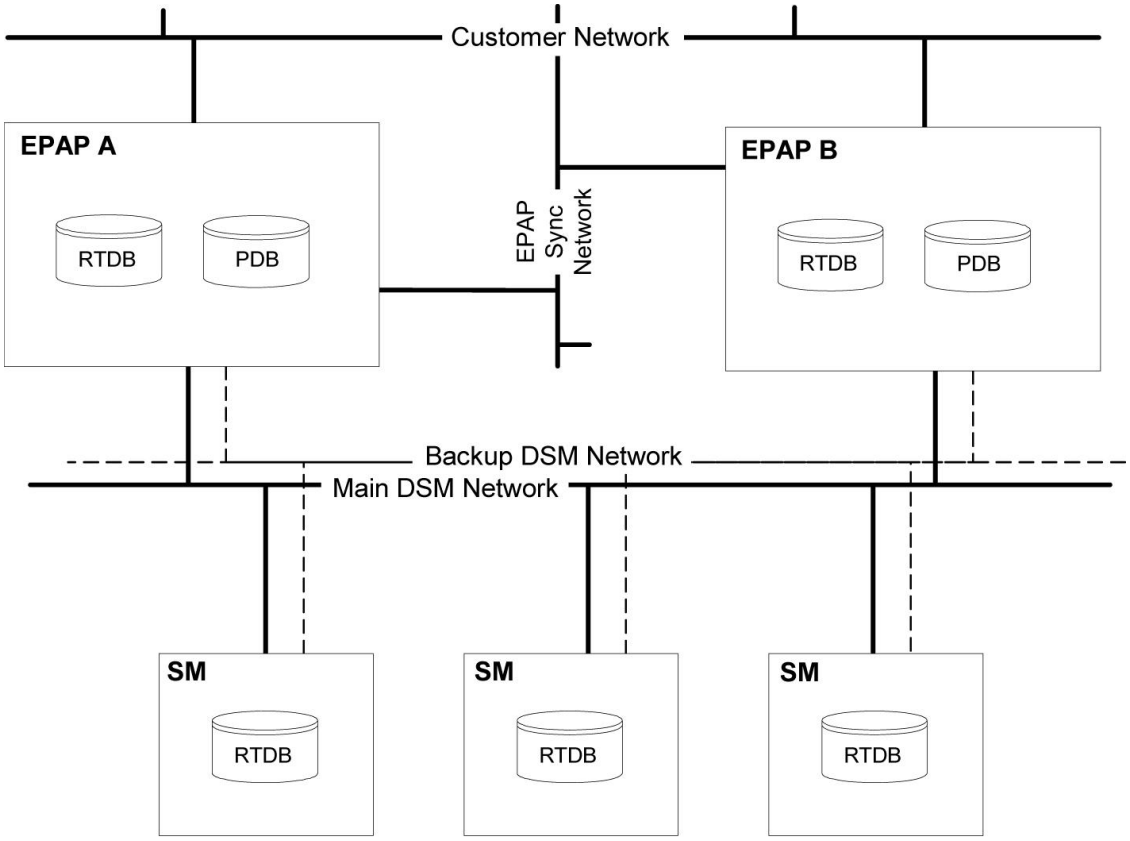
The current database level when the reload started is of special importance during reload. When a Service Module card detects that the last record has been received, it sends a status message back to the EPAP indicating the database level at the start of reload. This action will start incremental loading. 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.

2.4 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 2-8 for the MPS hardware interconnection diagram.

Figure 2-8 MPS Hardware Interconnection



2.4.1 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 for each inconsistent Service Module card. The command `rept-stat-db` displays the database on the Service Module card as *Diff* level. See Table 2-12.

Table 2-12 Inconsistent Service Module Card Alarm

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

EAGLE 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 2-13) 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 2-13 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 2-14

Table 2-14 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.

2.5 Status Reporting and Alarms

The EPAPs have no direct means of displaying output messages on EAGLE 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.

EPAP alarms are sent to the EAGLE based on a configurable Alarm feed parameter `EAGLE Alarm Feed`. If the value of `EAGLE Alarm Feed` is set to *ON*, the EPAP alarms are sent to the EAGLE; otherwise, the EPAP alarms are not sent to the EAGLE. Both alarm feed parameters `EAGLE Alarm Feed` and `SNMP Alarm Feed` can be set to *ON* at the same time. With these settings, the EPAP sends alarms to the EAGLE and SNMPv2c only, SNMPv3 only, or both SNMPv2c and SNMPv3 traps to the OCEEMS. Users must be aware of duplicate alarms if both alarm feed parameters `EAGLE Alarm Feed` and `SNMP Alarm Feed` are set to **ON** and the same OCEEMS is connected to the EPAP and the EAGLE.

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

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 wants to know the status of a Service Module card, the EPAP 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.

2.6 EPAP Provisioning Performance

EPAP provisioning performance values depend on software release, type of command, provisioning method (external PDBI client or import file) and database size. The EPAP provisioning performance values in this section are stated in Commands per Second (CPS), and apply to only the performance of the Provisioning Database Interface (PDBI) and not the Service Order Gateway (SOG) interface. Also, the CPS values apply to only successfully completed PDBI commands when a single PDBI client is connected to the Provisioning Database Application (PDBA); the CPS values may be different for unsuccessful commands or when additional PDBI clients are connected. The stated CPS values apply only to normal transaction mode. If a command is performed in single transaction mode, the CPS value is expected to be significantly lower than the stated value.

The `add`, `update`, `retrieve`, and `delete` variations of each command type have different CPS values. Typically, `retrieve` commands have a higher CPS value compared to other commands. The actual CPS value also depends on the type of data being provisioned: DN, DN Blocks, NE, IMSI, IMEI, IMEI Block. Other factors affecting CPS values are described in Table 2-15.

Table 2-15 Other Factors Affecting CPS Values

Factor	Description	% Impact
Database size or existing data count	The CPS value decreases for most data types with an increase in database size or data count.	5-50%

Table 2-15 (Cont.) Other Factors Affecting CPS Values

Factor	Description	% Impact
Data association	If a DN is associated with an IMSI, then the IMSI CPS value is affected. Up to 8 DNs can be associated with a specific IMSI.	5-20%
	This affect on CPS value is also dependent on whether the DN Block Self Healing feature is on or off. If no DNs are associated with IMSI, then the IMSI CPS value does not depend on the DN Block Self Healing feature being on or off.	
	Also, if more of the fields associated with a DN are provisioned, the CPS value is lower. For example, if the ASD, NE, ST, NSDN, CGBL and CDBL fields are provisioned, then the CPS value is lower than when a DN has only the PT field associated.	
Existing database layout or DN distribution	The layout of existing DNs or DN Blocks impacts the CPS value. Also, if the provisioned DN or DN Block is at the start of the existing DN or DN Block, then the CPS value is higher than provisioned DN or DN Block that is at the end.	5-10%
	If the DN Block size increases, the CPS value decreases.	30-40%
Provisioning method	An increase in the number of PDBI connections may lower the CPS value.	5-10%
	The more fragmented the database is the lower the CPS value.	10-15%
	An increase in number of idle threads lowers the CPS value.	5-10%
	Normal Transaction Mode results in higher CPS values than Single Transaction Mode.	30-40%
	Manual import results in a higher CPS value than automatic import. Similarly, twenty DNs added in a single transaction (begin, end) have a higher CPS value than twenty transactions.	5-10%
EPAP features	Some EPAP features affect the provisioning performance values (CPS values). For example, if the DN Block Self Healing feature or PDBI Statistics Report feature is on, the CPS values may be lower.	5-20%

Table 2-15 (Cont.) Other Factors Affecting CPS Values

Factor	Description	% Impact
Load on the server	The larger the processing load is the lower the CPS value. For example, if the RTDB Backup or PDBA Export process is running, the CPS value decreases.	20-50%
Network latency	A larger network latency reduces the CPS value.	60-70%

EPAP Provisioning Performance for Application B Card

Table 2-16 provides examples of CPS values for an EPAP based on the Application B Card. These CPS values assume that:

- No delay exists.
- No packet loss occurs.
- GigE interface is used.

> **Note:**
>
> The database size used for performance tests was 480M.

Table 2-16 Example Provisioning Performance Values with Application B Card

Type	Description	CPS
DN mixed commands	Auto-import mode `add` = 25%, `update` = 25%, `retrieve` = 25%, `delete` = 25%	480
IMSI mixed commands	Auto-import mode `add` = 25% , `update` = 25% , `retrieve` = 25% , `delete` = 25%	100
IMSI mixed commands	Auto-import mode `add` = 50%, `update` = 10%, `retieve` = 10%, `delete` = 30%	200

3
EPAP Graphical User Interface

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

3.1 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

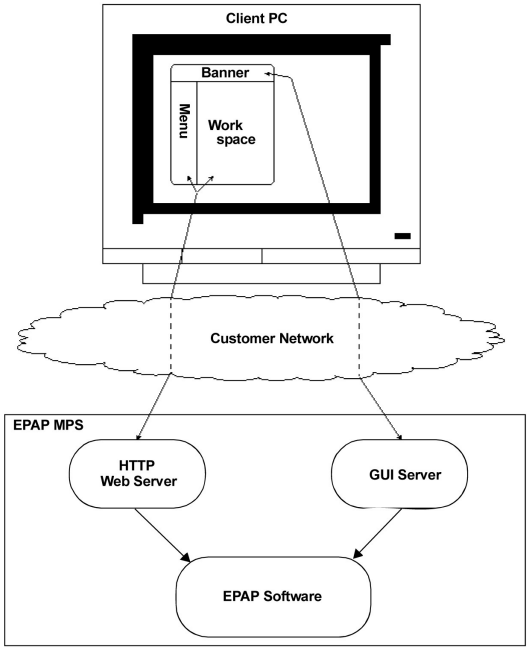
The banner header sections communicate directly with the **GUI** Server process on the MPS. The menu and work area sections primarily consist of CSS3 and **HTML5** generated by Ajax and **CGI** (Common Gateway Interface) scripts on the back end. Perl socket programming, along with CGI scripts, are used for the watchers. The banner displays the current EPAP IP and Status, PDBA IP and Status, Timer, Oracle Logo, Watchers, Alarm Indicators and Message History. The banner 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.

For GUI differences related to Standalone PDB EPAP, see Standalone PDB EPAP .

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

Figure 3-1 Process Architecture View of the EPAP UI



3.1.1 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 (Chromium-based Edge browser). 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.

> **Note:**
>
> GUI cannot be opened using the server hostname for Segmented PDBonly EPAP as the hostname and the alias for GUI interface in the /etc/hosts do not match.

Starting the Secure Web-based GUI

To start the secure web-based GUI, first start a web browser (Chromium-based Edge browser). 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.

Opening HTTPS Mode Without Installing Security Certificate

Opening the EPAP GUI in HTTPS mode without installing the security certificate causes the following menu tabs to fail to open:

Process Control

- Start Software
- Stop Software

Maintenance

- Force Standby
  - View Status (Mixed EPAP)
  - Change Status (Mixed EPAP)
- Decode MPS Alarm
- RTDB Audit
  - View Enabled (Mixed EPAP)
  - Change Enabled (Mixed EPAP)
- Automatic PDB/RTDB Backup
- EPAP Security
  - View Security Configuration
  - Change Security Configuration

RTDB (Mixed EPAP menu)

- Maintenance
  - Reload from Remote
  - Backup RTDB
  - Restore RTDB
  - Configure Record Delay

Debug

- Capture Log Files

- Manage Logs & Backups
- Set Debug Levels (Mixed EPAP)

Platform

- Run Health Check
- Reboot the MPS

PDBA

- Process Control
  - Start PDBA Software
  - Stop PDBA Software
- View PDBA Status
- Manage Data
  - IMSI Range
    - Add
    - Update
    - Delete
  - Prov BL
    - Add
    - Delete
    - Retrieve
- Authorized IP List
  - Add Authorized IP
  - Modify Authorized IP
  - Removed Authorized IP
- Maintenance
  - Backup
    - List Backups
    - Backup the PDB
    - Restore the PDB
  - Transaction Log Params
    - View Params
    - Change Params
  - Number Prefixes
    - View Prefixes
    - Change Prefixes
  - Logs
    - Set Log Params

User Administration

- Authorized IPs
  - Add Authorized IP
  - Removed Authorized IP
  - Change UI IP Authorization
- HTTP(S) Support
  - Change Configuration
- Modify Defaults

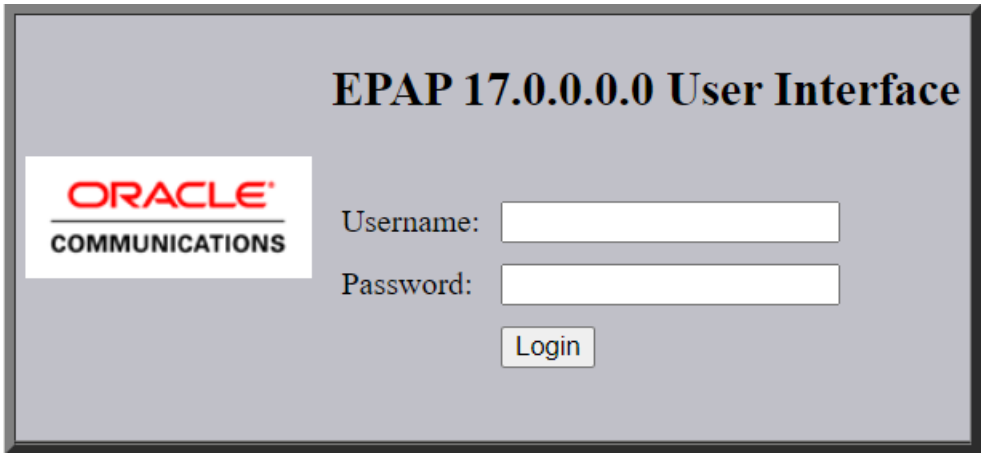
> **Note:**
>
> GUI cannot be opened using the server hostname for Segmented PDBonly EPAP as the hostname and the alias for GUI interface in the /etc/hosts do not match.

3.1.1.1 Enabling HTTPS and Installing Security Certificate

This procedure configures the PDB databases on an Active Site. Perform the following procedure to enable HTTPS and install the Security Certificate.

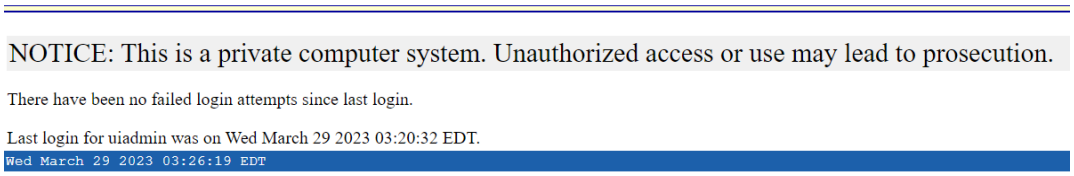
1. Access the EPAP GUI by opening a web browser and entering the IP address of Server A.

Figure 3-2 EPAP Login



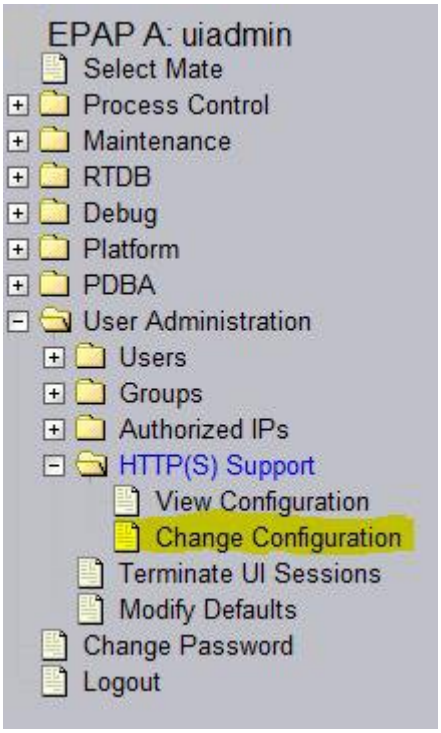
2. Login as `uiadmin`.

Figure 3-3 Login Successful



3. On the EPAP A site, select **User Administration**, and then **HTTP(S) Support**, and then **Change Configuration**.

Figure 3-4 Change Configuration Menu Option



4. Select the check box "HTTPS Enabled," and uncheck "HTTP Enabled."

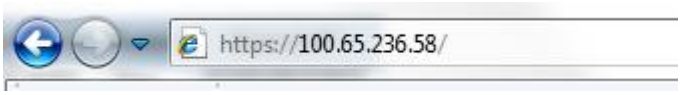
Figure 3-5 HTTPS Enabled

5. Click on the **Submit Changes** button to enable HTTPS. A success screen will appear.
6. Select **User Administration**, and then **HTTP(S) Support**, and then **View Configuration** to confirm HTTP Enabled is **NO** and HTTPS Enabled is **YES**.
7. Log out of the EPAP GUI by clicking on the **Logout** menu option. Then click the **Logout** button in response to the following message:

Figure 3-6 EPAP GUI Logout

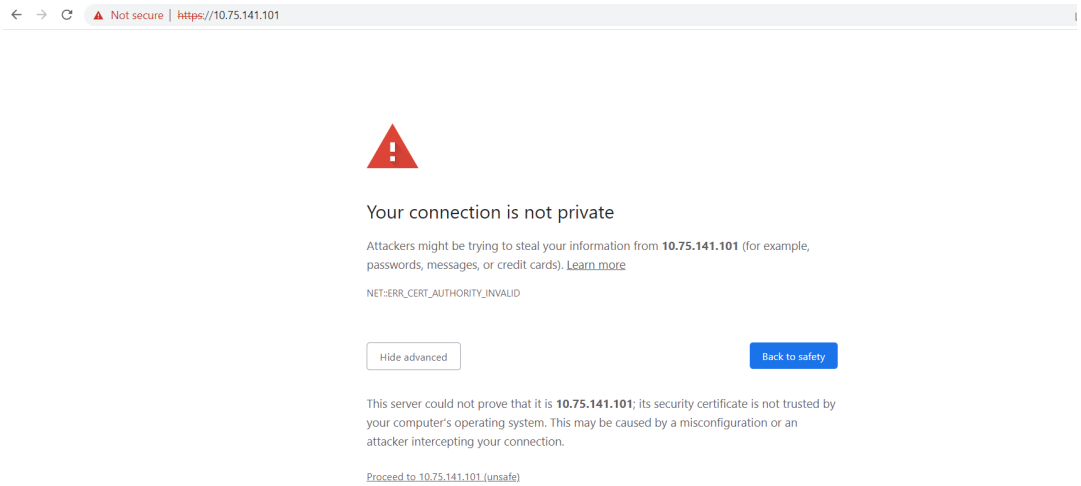
8. Access the EPAP GUI using **HTTPS**.

Figure 3-7 HTTPS Address Bar



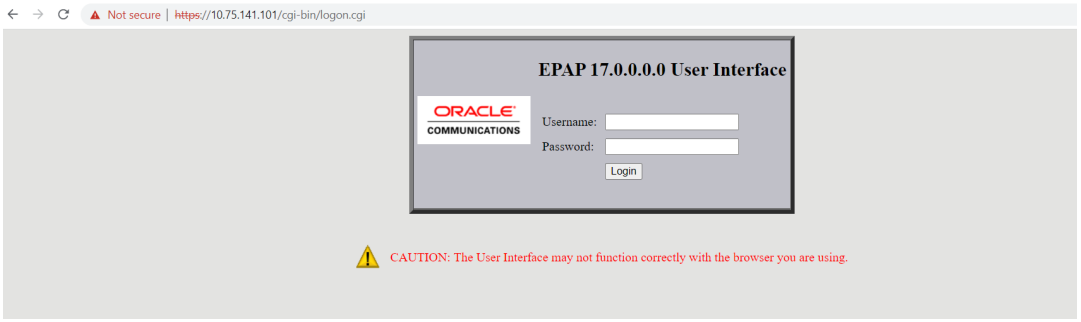
9. Click on "Continue to this website (not recommended)."

Figure 3-8 Security Certificate



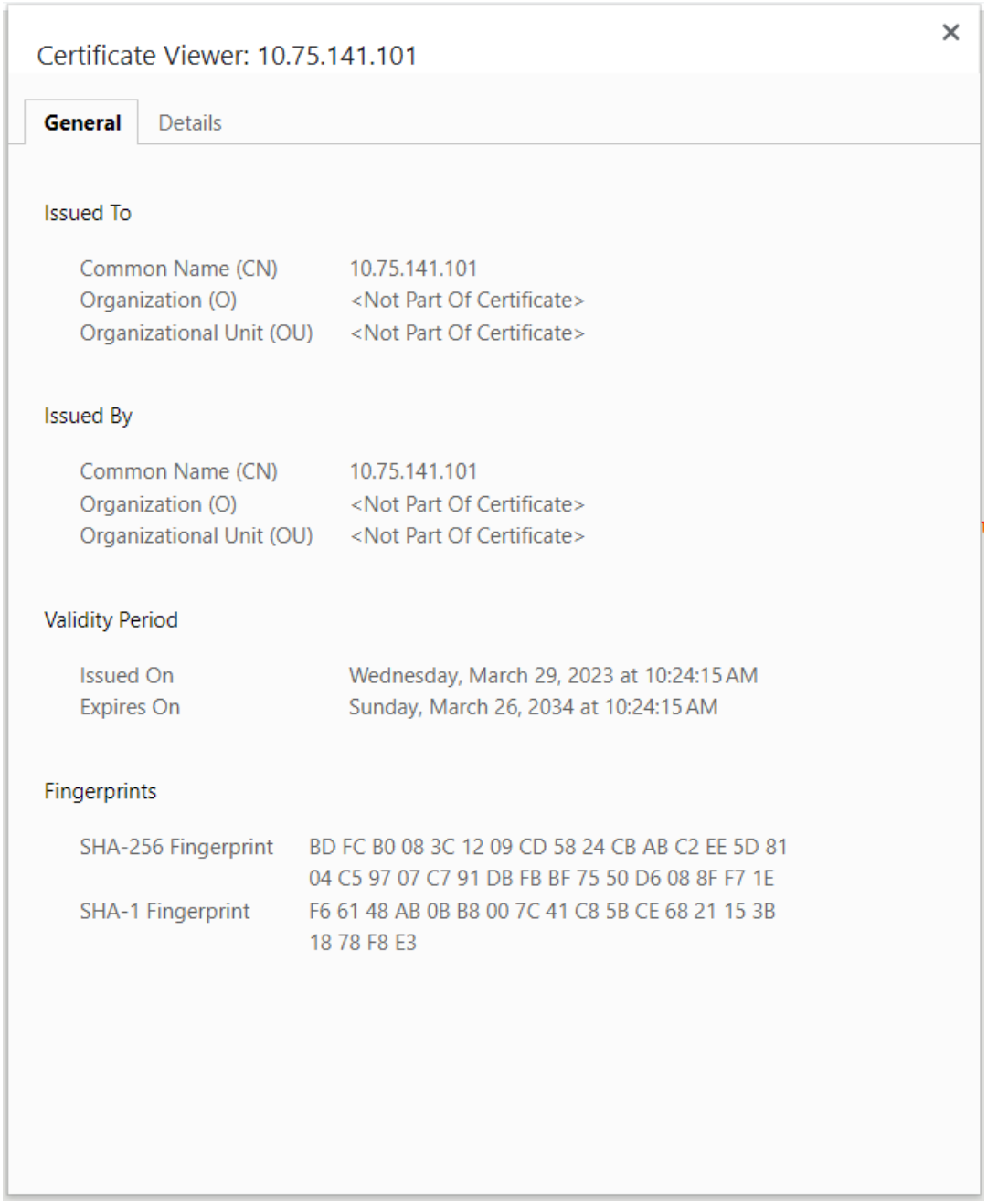
The Login Page is displayed:

Figure 3-9 HTTPS Login Page



10. Click on **Certificate Error**.
11. In the popup window titled "Certificate Invalid," click on the **View certificates** link to display the Certificate dialog box.

Figure 3-10 Certificate



If **Install Certificate...** is not available, execute the following steps:

a. Select **Tools**, and then **Internet Options**.

b. Select **Security**, and then **Trusted Sites**, and then **Sites**.

c. Confirm that the URL matches, then select **Add**, and then **Close**.

d. Close the **Internet Options** by selecting either **OK** or **Cancel**. Refresh the page.

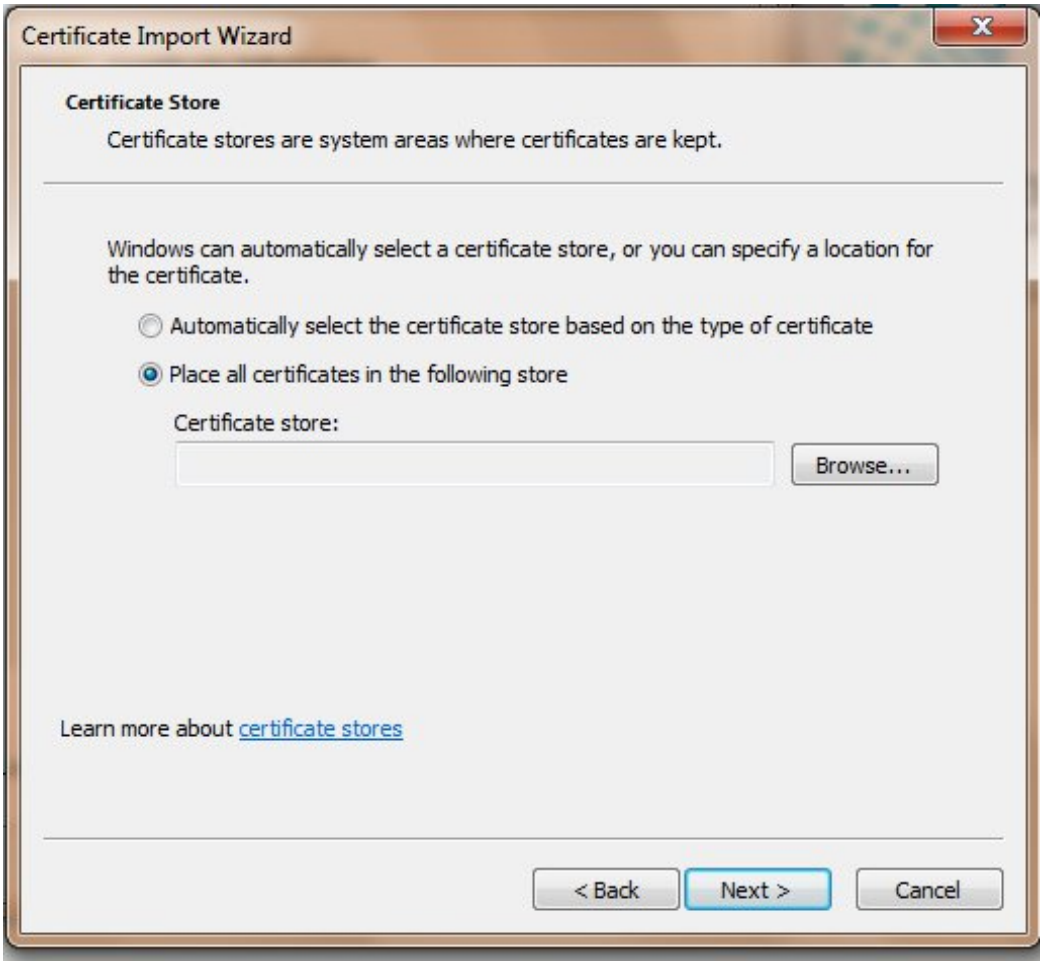
e. Follow 9 to 11, then proceed to 12.

12. Click **Install Certificate...** to begin the Certificate Import Wizard. The Certificate Import Wizard "Welcome" page is displayed:

Figure 3-11 Certificate Import Wizard

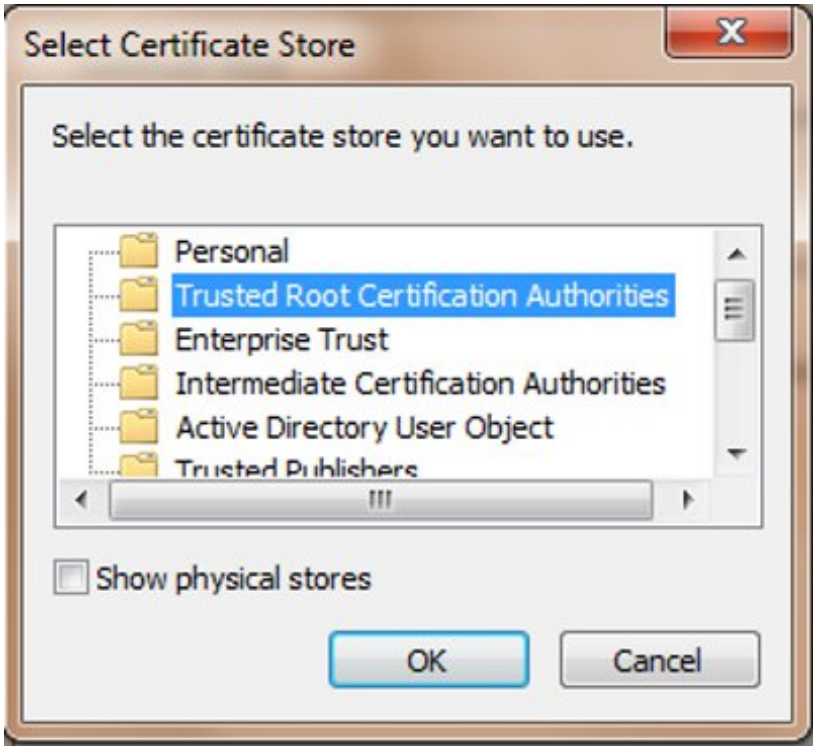
13. Click on **Next** to display the Certificate Store page of the Certificate Import Wizard. The Certificate Import Wizard "Certificate Store" page is displayed:

Figure 3-12 Certificate Store



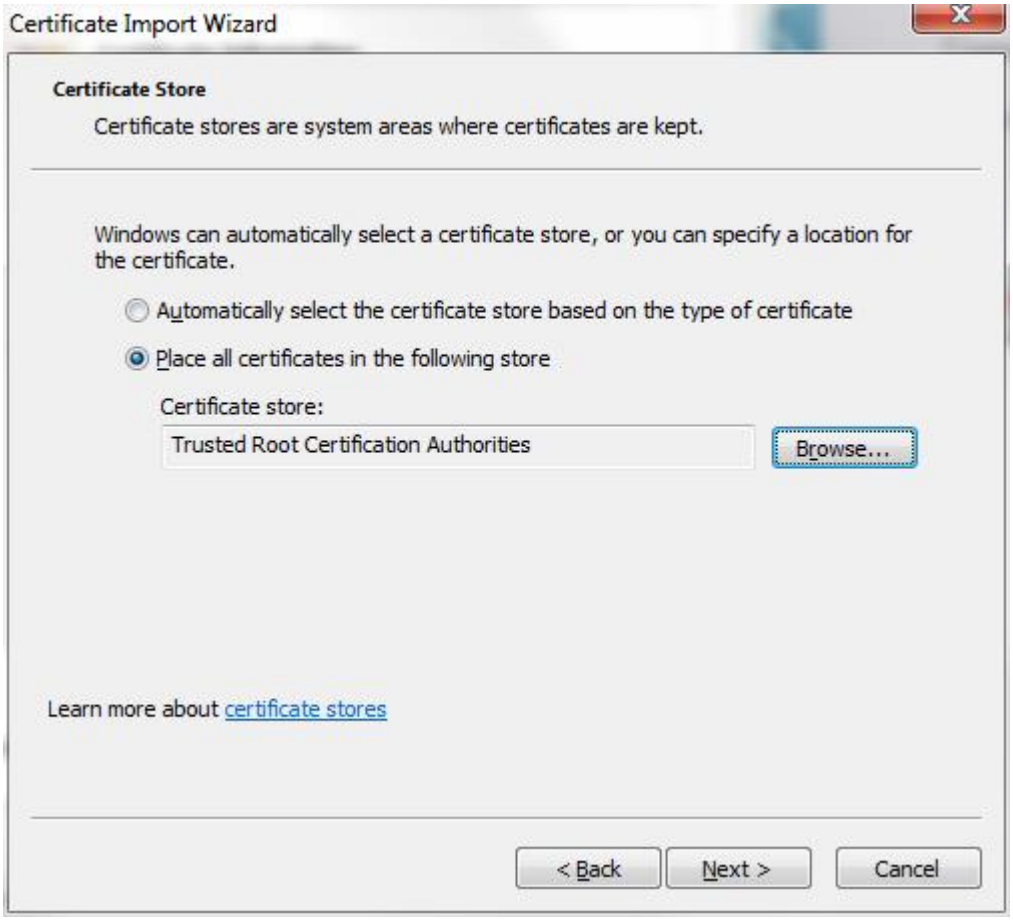
14. Select the "Place all certificates in the following store" radio button, then click **Browse** to display the Select Certificate Store window.

Figure 3-13 Select Certificate Store



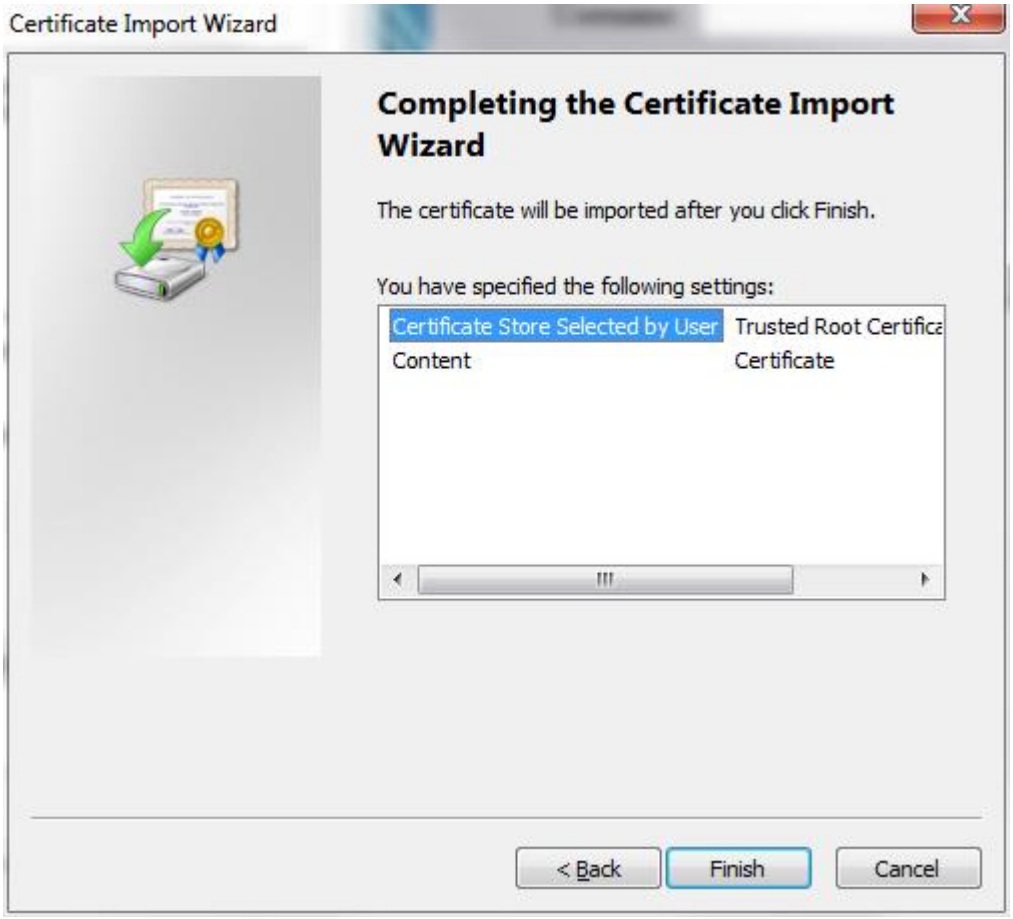
15. Select the "Trusted Root Certification Authorities" option and click **OK** to display the Certificate dialog box.

Figure 3-14 Certificate Store



16. Click **Next**. The Certificate Import Wizard "Completing the Certificate Import Wizard" page is displayed:

Figure 3-15 Completing the Certificate Import Wizard



17. Click **Finish**. If a Security Warning dialog box is displayed, click **Yes**.

Figure 3-16 Security Warning

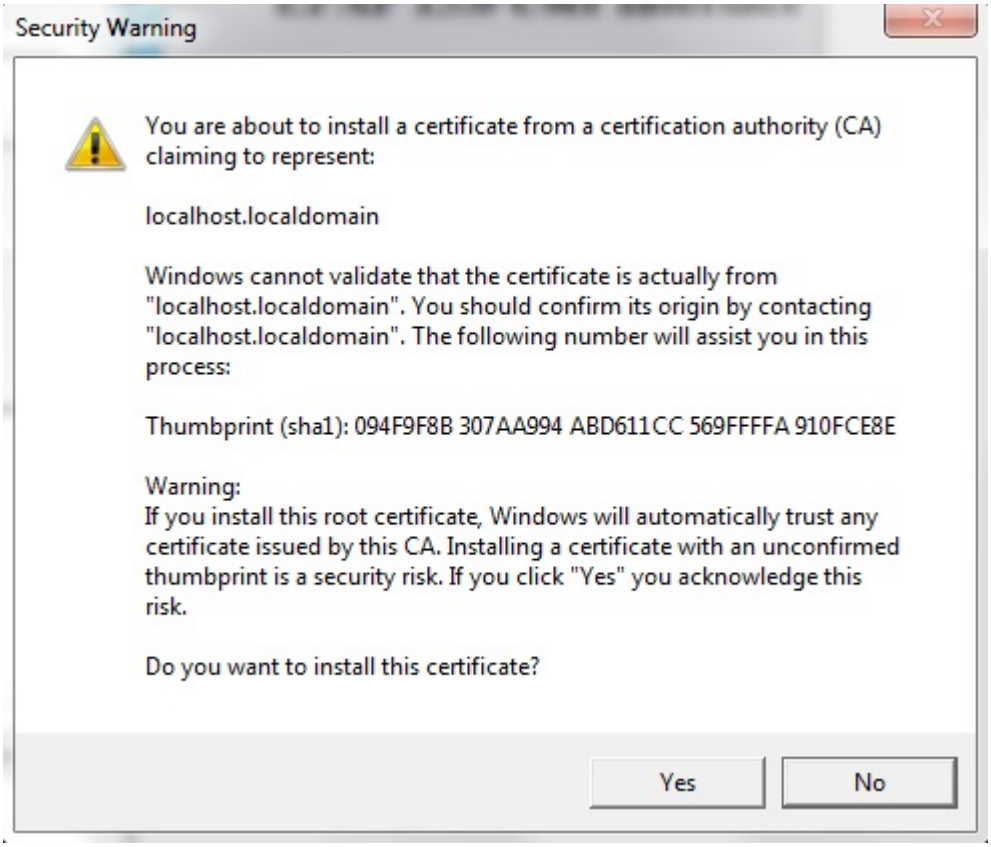


Figure 3-17 Import Successful

18. After the message box "The import was successful" is displayed, click **OK** to close the Certificate Import Wizard.
    a. Select **Tools**, and then **Internet Options**.
    b. Select **Security**, and then **Trusted Sites**, and then **Sites**.
    c. Select the URL you just added, then select **Remove**, and then **Close**.
    d. Shut down all running instances of Chromium-based Edge Browser and restart the browser.

    The site's certificate should now be trusted.
19. Log in to the EPAP GUI as `uiadmin` or any other user, and verify that all GUI pages are opening successfully.

To access the EPAP GUI on Chromium-based Edge Browser in secure mode (https), exceptions are required for two ports: 443 and 8002.

The exception for port 443 is automatically added. The exception for port 8002 must be manually added by completing the following steps:

1. Open Mozilla Firefox.
2. Select **Tools**, and then **Options** .
3. Select **Advanced**, and then **Certificates**, and then **View Certificates**.
4. Select the **Servers** tab, then select **Add Exception**.
5. Enter `https://<server_gui_ip>:8002` and select **Get Certificate** to add the port exception.
6. Select **Confirm Security Exception** to finish.

> **Note:**
>
> The user must complete the port exception steps for both IPv4 and IPv6 server IPs.

To install the certificate on Microsoft Edge®, complete the following steps:

1. Start Microsoft Edge®.
2. Install the certificate on Microsoft Edge®.
3. Close Edge and open the GUI again to check if the certificate is installed.

To open the EPAP GUI with IPv6 IP on Microsoft Edge®, complete the following steps:

1. Start Microsoft Edge®.
2. Select **Tools**, and then **Internet Options**.
3. Select the **Connections** tab, then select **LAN Settings**.
4. Uncheck all boxes under **Automatic configuration** and ensure the box for `Use a proxy server for your LAN` is unchecked. Click **OK**.
5. Close the current sesson of Microsoft Edge®.
6. Open a new session of Edge and open the IPv6 GUI.

3.1.1.2 Enabling HTTP

Perform the following steps to manually enable HTTP.

1. Login to EPAP A as `admusr`.
2. Use **uiEdit** variable to set "HTTP_ENABLED" to yes.

   ```
   $ uiEdit HTTP_ENABLED Yes
   ```

3. Make sure the **uiEdit** variables "HTTP_ENABLED" and "HTTPS_ENABLED" both are set to "Yes".

   ```
   $ uiEdit |grep _ENABLED | grep HTTP
   "HTTP_ENABLED" is set to "Yes"
   "HTTPS_ENABLED" is set to "Yes"
   ```

> **Note:**
>
> HTTPS_ENABLED is not mandatory if you only want HTTP.

4. Login to EPAP A as `epapdev`.
5. Execute the following commands:

```
$ ssh -l epapdev mate ". /etc/profile; /opt/TKLCappl/bin/httpConfig.pl
both" 2> /dev/null
$ . /etc/profile; /opt/TKLCappl/bin/httpConfig.pl both 2> /dev/null
```

6. Login as `admusr` again and verify that the required processes are running.

```
# netstat -anp |grep http
tcp        0      0 0.0.0.0:8002
0.0.0.0:*                   LISTEN      10116/httpd
tcp        0      0 0.0.0.0:443
0.0.0.0:*                   LISTEN      10116/httpd
tcp        0
0 :::8001                     :::*                        LISTEN
10116/httpd
tcp        0
0 :::80                       :::*                        LISTEN
10116/httpd
```

> **Note:**
>
> If the above httpd processes are not listed, try the following command:
>
> ```
> # systemctl start httpd  Starting httpd: Syntax error on line 1090
> of /etc/httpd/conf/httpd.conf: Invalid command 'f', perhaps
> misspelled or defined by a module not included in the server
> configuration
>      [FAILED]
> ```

If you see the error above, delete the extra line from httpd.conf. If you see any other error, contact My Oracle Support.

```
 #sed -i.bak -e
'$d' /etc/httpd/conf/httpd.conf
```

7. Start httpd service and verify using the `netstat` command.

```
$ sudo sytemctl start httpd
# netstat -anp |grep http
tcp        0      0 0.0.0.0:8002
0.0.0.0:*                   LISTEN      10116/httpd
tcp        0      0 0.0.0.0:443
0.0.0.0:*                   LISTEN      10116/httpd
```

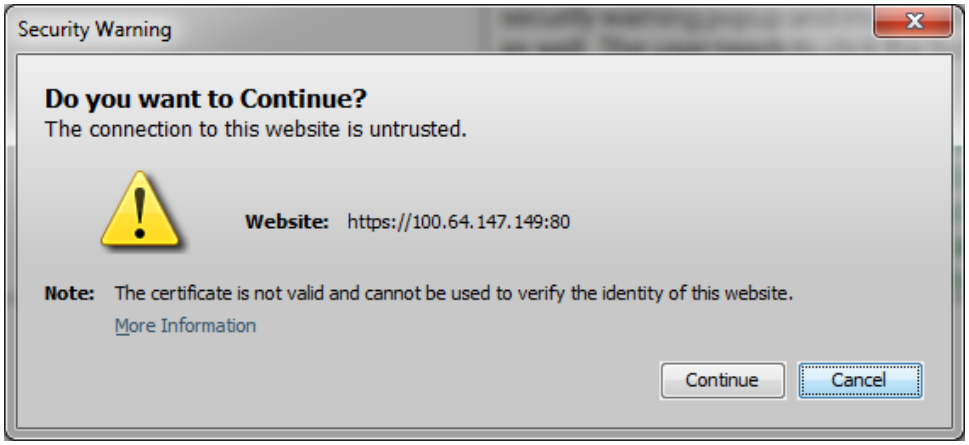
```
tcp        0
0 :::8001                 :::*                    LISTEN
10116/httpd
tcp        0
0 :::80                   :::*                    LISTEN
10116/httpd
```

3.1.2 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.

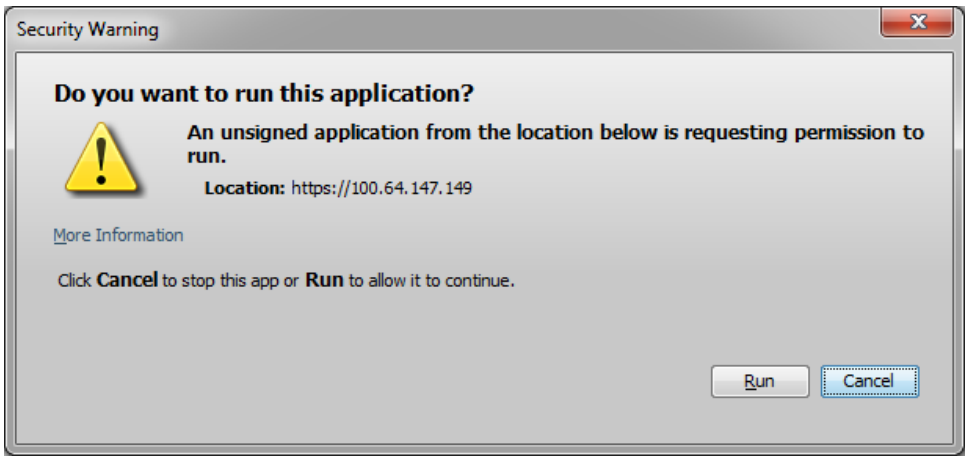
After logging in, a Security Warning dialog box alerts the user that the connection is untrusted. The user clicks **Continue** to proceed to the second Security Warning dialog box.

Figure 3-18 Security Warning for Untrusted Connection



The second Security Warning dialog box asks the user whether to run the unsigned application. The user clicks **Run** to run the application.

Figure 3-19 Security Warning for Unsigned Application



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.

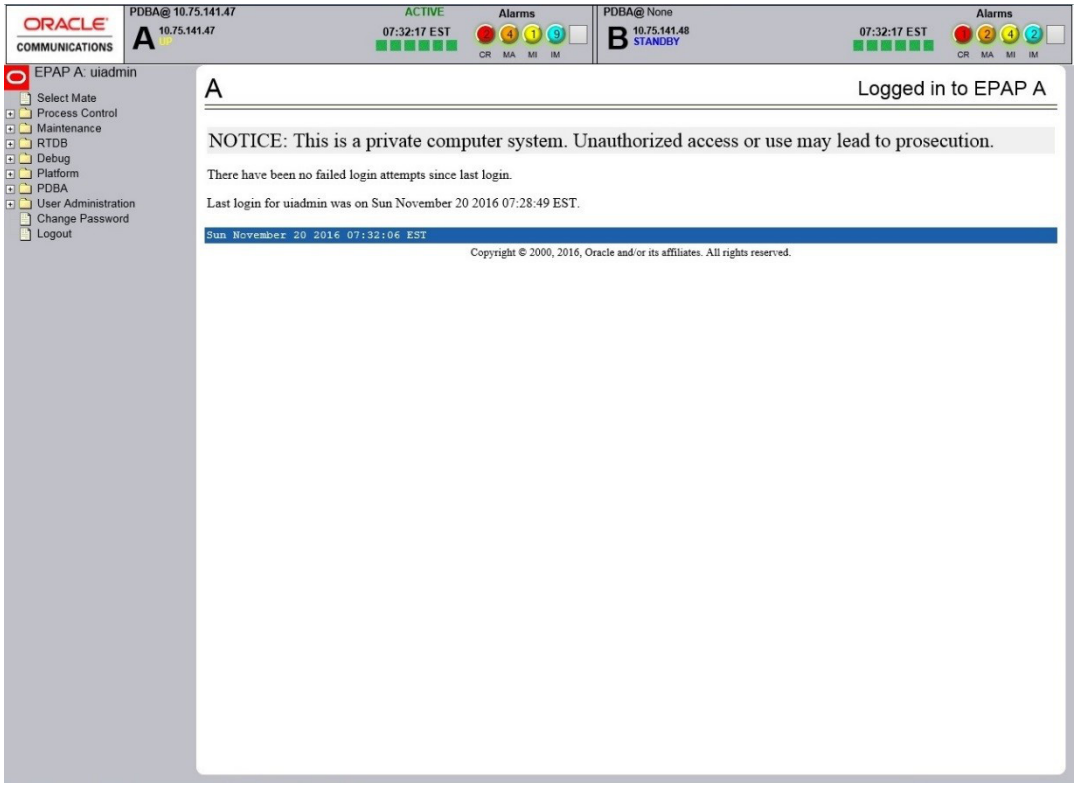
3.1.3 EPAP GUI Main Screen

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.

EPAP Banner Components

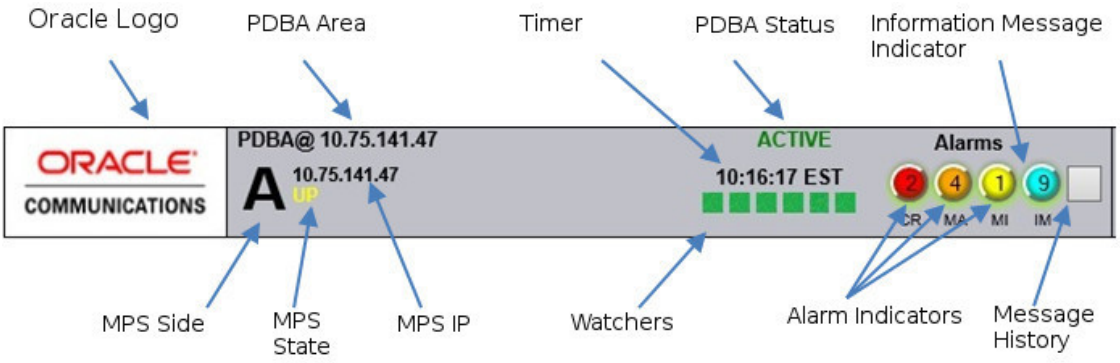
The EPAP A and EPAP B areas contain information and displays to inform the user about the status and operation of the servers.

Figure 3-20 EPAP GUI



Tool tips are displayed for all EPAP banner components. Tool tips are activated when the mouse cursor (mouse-over event) is placed over the component. Each tip is unique to the banner component. The components of the EPAP Banner are displayed in Figure 3-21:

Figure 3-21 EPAP Banner Components



PDBA and EPAP Status

The first row of the EPAP banner displays the PDBA details with PDBA IP and its status. This displays the details of both the Local PDBA and Remote PDBA. The color coding is applied for the different statuses of the PDBA, as seen in Table 3-1.

Table 3-1 PDBA Status

Status	Description	Color Code
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	Black
DOWN	EPAP was contacted, but the PDBA software is not running	Red
STANDBY	PDBA software is running as STANDBY	Blue
ACTIVE	PDBA software is running as ACTIVE	Green
REPLERR	PDBA detected presence of a PDB replication failure	Red
ACTIVE (By Proxy)	PDBA is running on EPAP B using the PDBA Proxy feature, when EPAP A goes down	Green
TERMINATED	Connection has been closed by the server	Red

The second row of the EPAP banner displays the EPAP details. This includes the MPS side, MPS IP, MPS status, Timer, Alarm Indicators, Message History, Watchers (if enabled) and acronyms for alarms and informational messages (CR, MA, MI and Info Msg). This MPS panel is dependent on the EPAP configuration. There are two panels for mixed EPAP configuration (both for MPS A and MPS B) and a single panel for PDBonly configuration (MPS A). The different statuses of the EPAP are seen in Table 3-2.

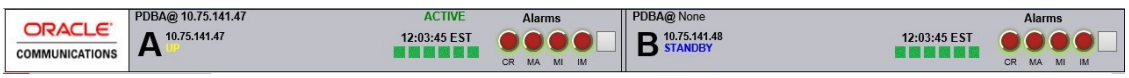
Table 3-2 EPAP Status

Status	Description	Color Code
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	Black
DOWN	The maintenance task is not running. The box may be running or not	Red
UP	The maintenance task is running (UP), but the EPAP is experiencing some problem that prevents is from becoming ACTIVE or STANDBY. This condition can result from a hardware, software, or database problem	Yellow
FORCED STANDBY	This EPAP has been forced into standby state by the user	Yellow
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 cards for the passage of maintenance and alarm information	Green
TERMINATED	Connection has been closed by the server	Red

Alarm Functionality

The first three indicators (from left) are the alarm indicators on the EPAP GUI. These indicators displays the number of respective alarms on the EPAP. The left indicator indicates the Critical alarms; it turns red when a Critical alarm occurs. The middle indicator indicates the major alarms, and turns orange when a Major alarm is raised. The right indicator indicates the Minor alarm, and turns yellow when Minor alarm is raised. A maximum of 99 alarm counts can be displayed, considering the sum of all 3 alarm types. The indicator will remain brown if no alarm of that type is raised on the EPAP, as seen in Figure 3-22.

Figure 3-22 EPAP GUI With No Raised Alarms



Clicking on any of the alarm indicators displays the details of each prevailing alarm on the EPAP, depending on which alarm indicator is clicked, in a new window. The new window with alarm details will remain persistent until either the GUI is terminated or the user logs out of the GUI. The user will have to close all opened alarm windows manually. The details of alarm include:

1. Alarm severity and type (heading)

2. Alarm name

For more information about the alarm categories, refer to Decode MPS Alarm.

Information Messages

The fourth indicator (from left) for each MPS side is the informational messages indicator. It displays all the current informational banner messages on the EPAP system. It also displays the number of informational banner messages on the EPAP. A max total of 99 information banner messages can be displayed on the indicator. The information message indicator will remain brown if there is no information banner message on EPAP. Clicking on the indicator will display the details of each informational banner message in a new tab. The details include:

1. Time when the banner message was raised
2. Information banner message

Timer

The time, along with the time zone, is displayed on the MPS panel. It displays the time of the MPS on MPS A and MPS B (not on PDBonly configuration). The time will change dynamically on the MPS panel. The time zone displayed will be the time zone that is configured on the EPAP.

Watchers

The watchers are the utility on the EPAP that provides the information about the processes running on the EPAP system. The processes that are monitored by watchers including the following (in the order from left to right):

1. PDBA
2. Topnode A
3. Topnode B
4. Prov
5. RTDB
6. Maint
7. PDBA Proxy (only on EPAP B)

When the above processes are working as expected, these watchers are green in color; otherwise, the watchers turn red if there is some error in any of the processes. These watchers are optional for the user. By default the watchers will be disabled and it not visible on the EPAP GUI. It can be enabled/disabled by the user by executing the `$ /usr/TKCL/epap/bin/setDebug <EPAP GUI User> <Enable/Disable Flag>` command, where `Flag` is either 0 (disable) or 1 (enable).

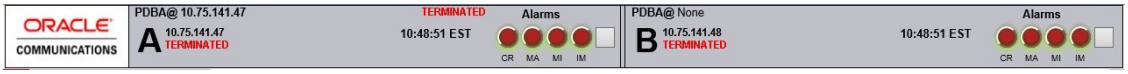
The user will have to re-open the GUI (with the user for which the watchers have been enabled/disabled) to see the change on the EPAP GUI.

Figure 3-23 EPAP GUI With Watchers When Processes Are Not Running

Banner Sessions

The banner session works according to the banner session termination value. The session will remain valid according to the idle timeout value or session timeout value. If the banner is kept idle for more than the idle timeout value, then it will be terminated, resulting in updating the banner components value with a terminated status on the GUI banner.

Figure 3-24 EPAP GUI Terminated Session



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 Oracle copyright notice information.

Workspace Syntax Checking

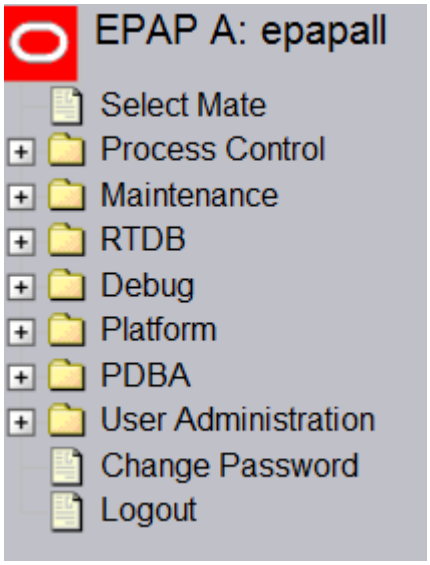
The web browser user interface uses layers of syntax checking to validate user input for text-entry fields.

- Mouse-over syntax check: For many of the entry fields, a list of syntax hints can be displayed when the mouse is moved over 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.

3.2 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 3-25 shows the EPAP main menu.

Figure 3-25 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.

Table 3-3 Summary of IPv6 Support on Different Features

Feature	Supported Configuration
Configure File Transfer	IPv4 or IPv6
Auto PDB/RTDB backup	IPv4 or IPv6
PDBA Authorized IP	All IPv4 or all IPv6 or Mixed
EPAP Authorized IP	All IPv4 or all IPv6 or Mixed
Static NAT Addresses	IPv4 only

3.2.1 Select Mate

The Select Mate menu selection changes the menus and workspace areas to point to the **EPAP** mate. This selection exchanges the status of the active and standby EPAPs. This basic action is available to all users and is accessible from the main menu (Figure 3-25).

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.

3.2.2 Process Control Menu

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

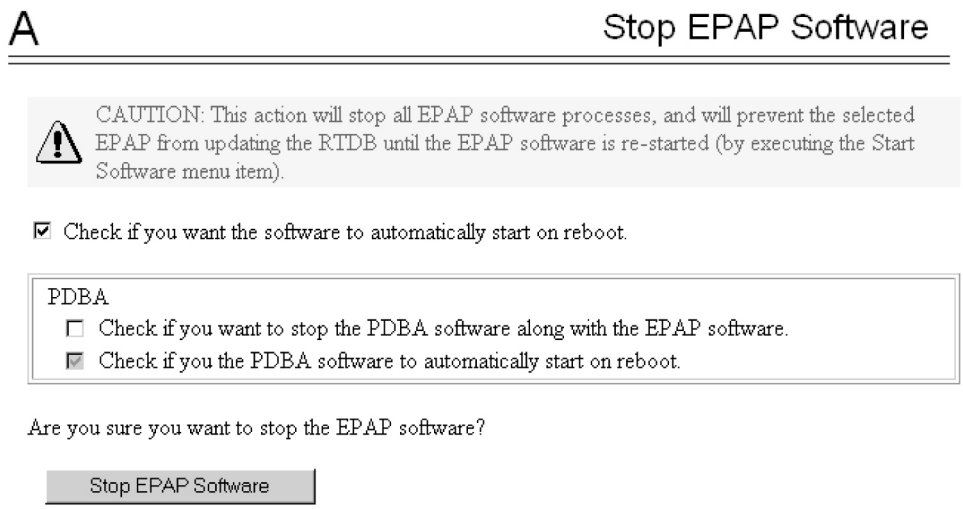
Start EPAP Software

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 3-26 Stop EPAP Software Screen



3.2.3 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

3.2.3.1 Force Standby

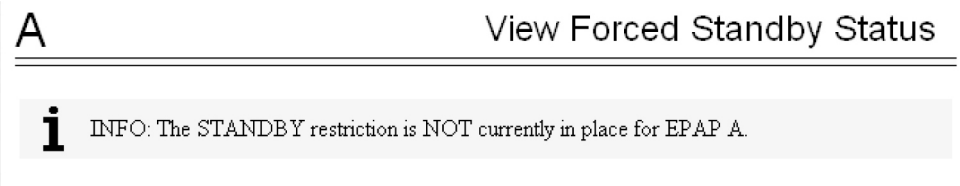
The Maintenance / Force Standby menu gives the user the ability to view the **EPAP** status and change the status.

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 3-27 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 3-28 Change Forced Standby Status Screen

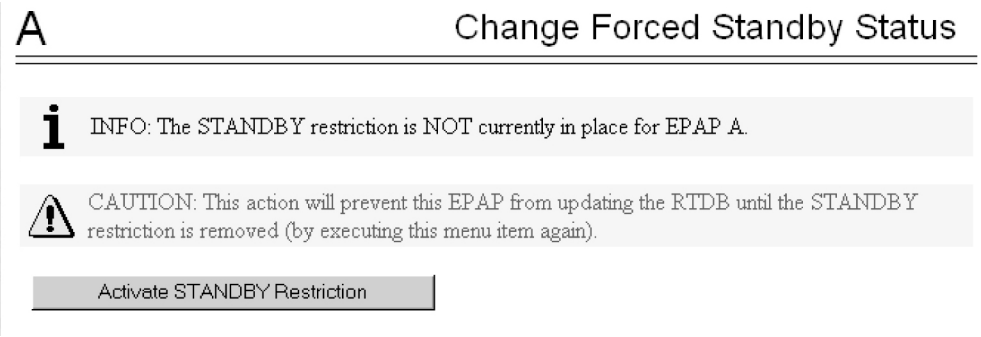


Table 3-4 Rules for Change Forced Standby Status

Semantic Rules		Error Code
A connection to the EPAP maintenance process must be available		E1005
Other Messages		
Condition	Message Text	
Standby restriction removed	Forced standby restriction removed from EPAP <selected EPAP>.	
Forced standby completed	EPAP <selected EPAP> now in forced standby mode	

3.2.3.2 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

Retrieve Entries Screen

The Retrieve Entries screen lets the user retrieve log entries from the transaction log. The user is prompted for the start and end time range, along with the maximum number of records to display to the screen.

Figure 3-29 Retrieve Entries from Transaction Log Screen

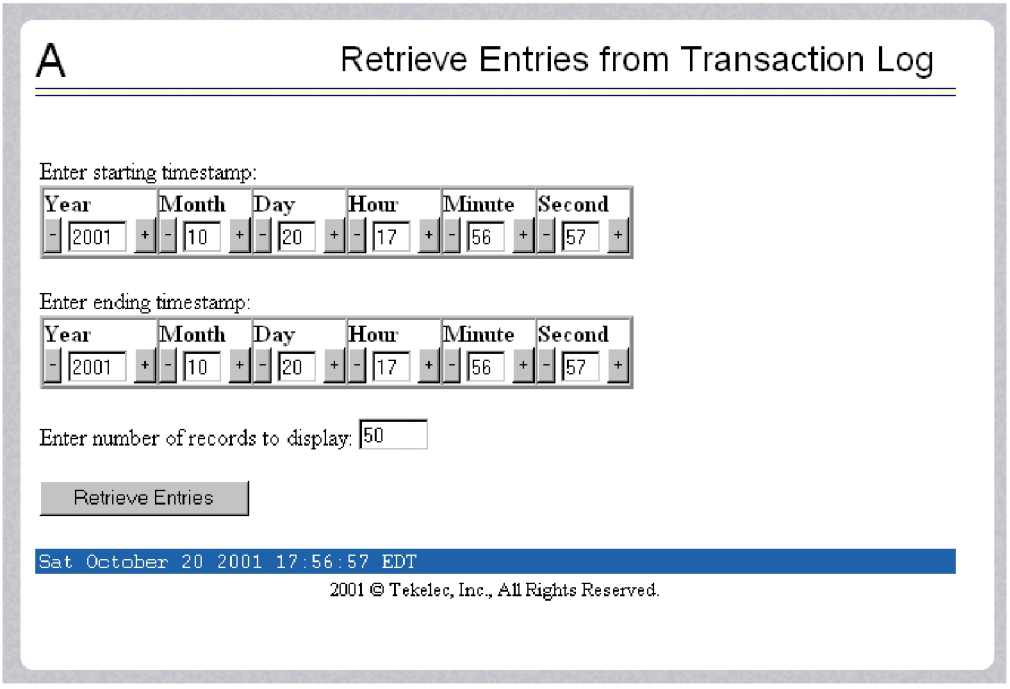


Table 3-6 shows the syntactic and semantic rules for retrieving transaction log entries.

Table 3-5 Rules for Retrieving Transaction Log Entries

Syntax Rules	Error Code
Dates/Times must be valid: **Field Valid Range** Year: 0000 - 9999 Month: 01 - 12 Day:01 - 31 Hour: 00 - 23 Minute: 00 - 59 Second: 00 - 59 (The day must be appropriate for the month and year.)	E1002

Table 3-5 (Cont.) Rules for Retrieving Transaction Log Entries

Maximum number of records must be in the range of 1 to 10,000	E1002
Semantic Rules	Error Code
Transaction log task must successfully process query	E1039
Transaction log task must create a file containing the result	E1040
UI task must successfully parse the result	E1041

See Figure 3-30 for a sample of the output from the Retrieve Transaction Log, followed by a table with the output field descriptions.

Figure 3-30 Sample of Retrieve Transaction Log Entry Output

```
    ID SRC         LOGGED-AT       LSMS-TIMESTAMP CMD (* DATA)
------- ---------- -------------- -------------- --------------------
     2 UI          20001004083255 20001004083255 RTRV_TTSERV_REQ
     * 1

     2 RTDB        20001004083255 20001004083255 RTRV_TTSERV_RSP
     * 16|78|100|150||255

     2 RTDB        20001004083255 20001004083255 RTRV_TTSERV_RSP
     * FAILURE - Invalid response

     3 UI          20001004083255 20001004083255 RTRV_SUB_REQ
```

Output Field Descriptions

Field	Description
ID	This field represents a unique identifier for the corresponding transaction. It is used internally with the Transaction log to correlate commands and responses. Any entries with the same **ID** are part of the same transaction. This field is used by customer service or engineering to investigate an issue.
SRC	This field stores the source of the corresponding transaction. The **SRC** field correlates to an internal task with the **EPAP** software and is used to determine the originator of the transaction. This field is used by customer service or engineering to investigate an issue.
LOGGED-AT	This field is the timestamp when the transaction was logged by the **EPAP** software. The format is: “yyyyMMddhhmmss” which indicates: yyyy: Year **MM**: Month dd: Day hh: Hour mm: Minute ss: Second
LSMS-TIMESTAMP	This field is the timestamp from the **LSMS** for the transaction.
CMD (* **DATA**)	This field contains a command identifier string and the command string from the **LSMS**. Command strings too long to be displayed on one line are not truncated.

For details about the contents of the Transaction Log, refer to Figure 3-30, which shows sample output as obtained by the Retrieve Entries action.

Table 3-6 shows the syntactic and semantic rules for exporting the transaction log.

Table 3-6 Rules for Exporting the Transaction Log

Syntax Rules	Error Code
Response must be a valid **UNIX** file name	E1002
Semantic Rules	Error Code
The file must be createable	E1042
Transaction log task must create the export file containing the result	E1042

3.2.3.3 Decode MPS Alarm

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

- Critical Platform **Alarm** (UAM #0370, alarm data h‘1000 . . .’)
- 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 *Alarms and Maintenance Guide*.

Table 3-7 shows the syntactic and semantic rules for the Decode Eagle MPS Alarm.

Table 3-7 Rules for the Decode Eagle MPS Alarm

Syntax Rules	Error Code
Entry must be a 16 character hexadecimal string	E1002
Semantic Rules	Error Code
The hexadecimal string must be properly encoded from one of the above five alarm categories	E1046

3.2.3.4 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.

Table 3-8 shows the syntactic and semantic rules for the Change Enabled screen of RTDB Audit.

Table 3-8 Rules for the Change Enabled of RTDB Audit

Syntax Rules	Error Code
A connection to the RTDB process must be available.	E1005
Other Messages	
Condition	Message Text
Audit turned off	RTDB auditing disabled for EPAP <selected EPAP>.
Audit turned on	RTDB auditing enabled for EPAP <selected EPAP>.

3.2.3.5 Configure File Transfer

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

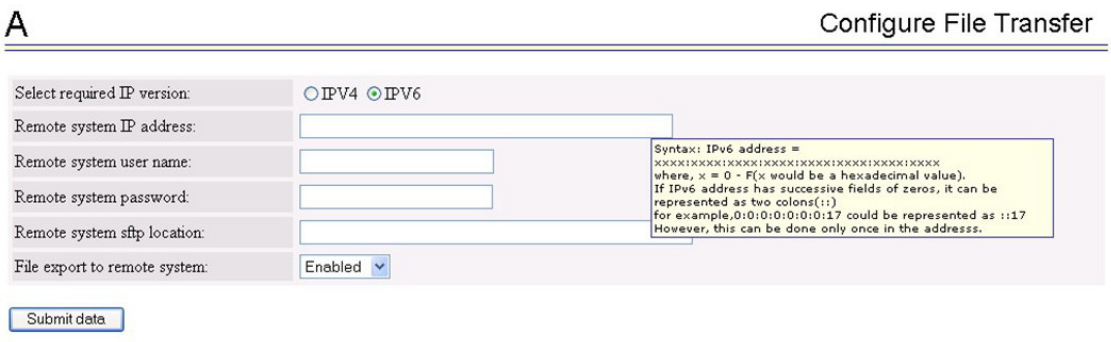
- Define the location of where the results of the automatic import are stored.
- Provide the options for enabling/disabling the Automatic Export capability.
- Provide a mechanism for testing the connection to the remote machine. This is done by using the username/ password and **IP** address provided 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:

- Choice of IPv4 or IPv6 remote system address:
  - The user is allowed to configure IPv4 only remote system address
  - The user is allowed to configure IPv6 only remote system address
  - On dual stack - the user is allowed to configure IPv4 or IPv6 remote system address
- Remote System **IP Address** - the IP address from where the data will be exported (customer system).
- Remote System User Name - required for logging onto the customer system
- Remote System Password - required for logging onto the customer system. This password will be stored in encrypted format.
- Remote System SFTP Location - the location of the directory on the customer system.
- File Export to Remote System - this is used to return the results of the import file (default = enabled).

The Configure File Transfer Screen is shown in Figure 3-31.

Figure 3-31 Configure File Transfer Screen



3.2.3.6 Automatic PDB/RTDB Backup

This screen is used to configure the Automatic **PDB**/**RTDB** Backup using either IPv4 or IPv6 addresses for a remote machine IP. 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 3-9 as a guide when populating the Automatic PDB/RTDB Backup screen. See Figure 3-32.

Table 3-9 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

Table 3-9 (Cont.) Mandatory and Optional Parameters

Parameter	Backup Type		
	Local	Mate	Remote
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

Oracle 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. 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.

PDB only maintains a single copy of backup file, if this backup file is already present automatic backup will fail for PDB. Therefore it is required to schedule remote transfer of PDB backup file using Configure File Transfer as described in section Configure File Transfer.

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.

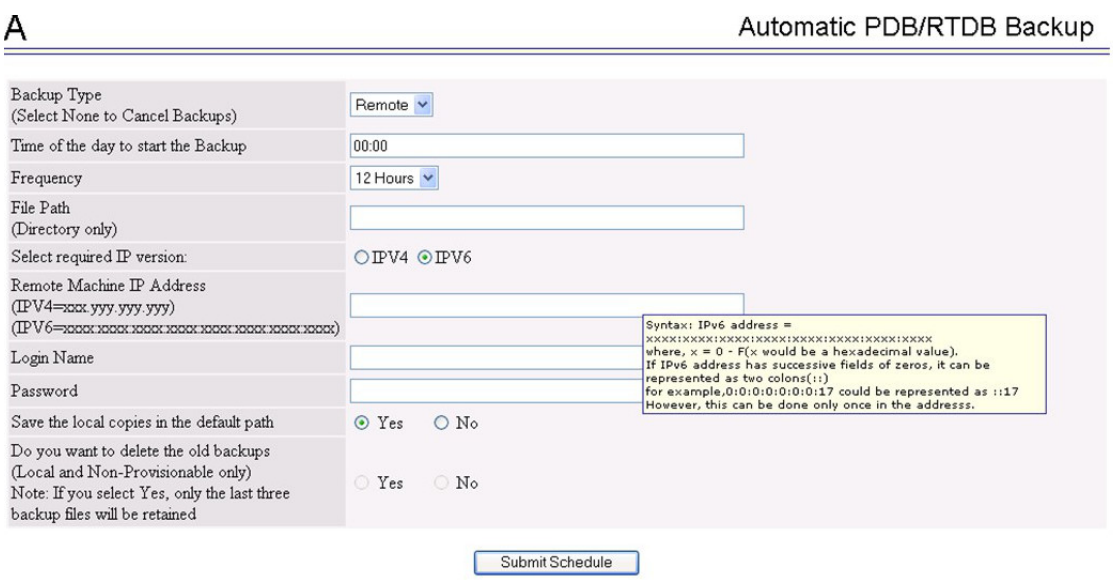
Time of the Day should be in hh:mm 24 hour (14:03) format.

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 will be displayed in asterisks (*)

Figure 3-32 Automatic PDB/RTDB Backup Screen



3.2.3.7 Schedule EPAP Tasks

Maintenance /Schedule EPAP Task

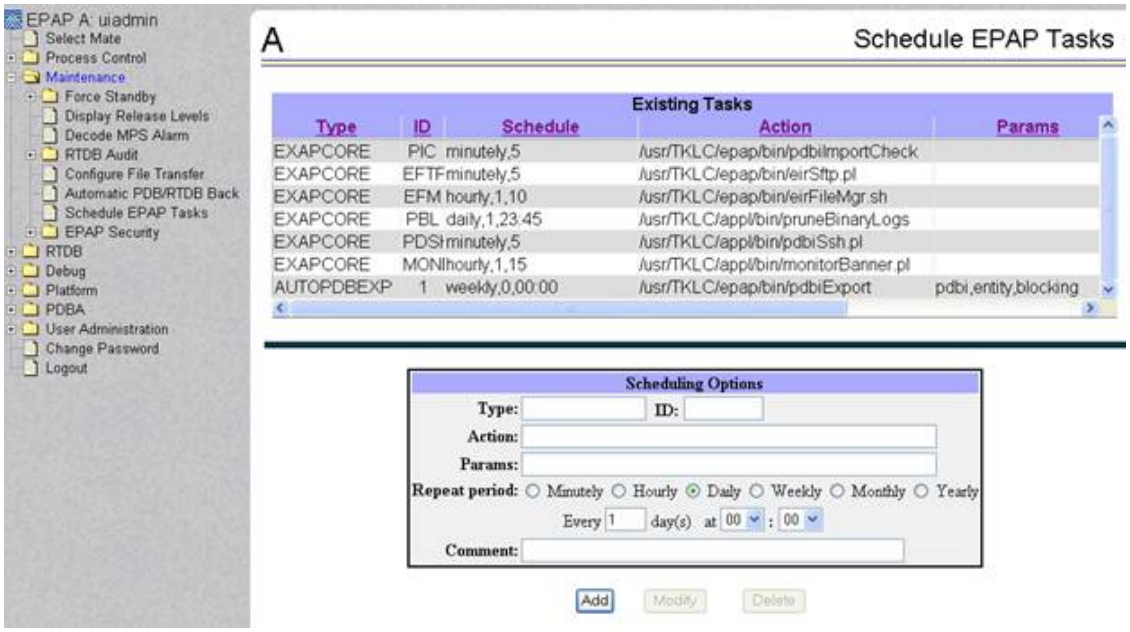
This screen is used to Schedule EPAP Tasks. Through this screen the customer has a choice of what tasks to be scheduled as well as the day and time of day for the execution of the tasks.

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 3-33 is an example of the Schedule EPAP Tasks screen.

Figure 3-33 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.

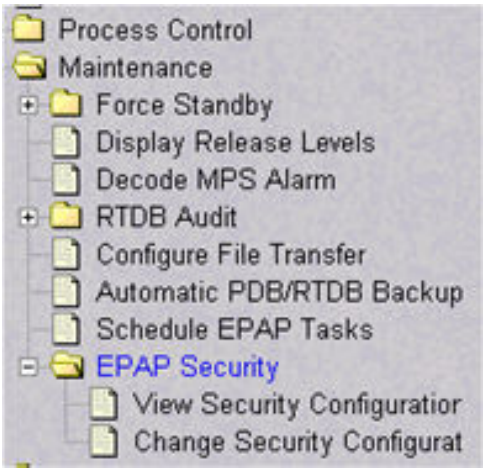
Delete
To delete a scheduled Task, click that task in the Existing EPAP Tasks table, and click the Delete button.
The **Delete** button is selectable only when an entry in the Existing Tasks table at the top of the screen has been selected.

3.2.3.8 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 3-34 EPAP Security menu



View Security Configuration

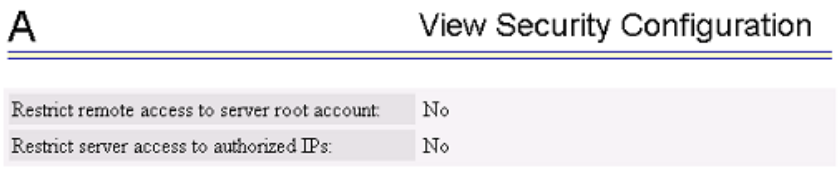
This menu allows the user to view security access for EPAP server on which the GUI is open. The user can view the following two configurations:

- 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**, and then **EPAP Security**, and then **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 3-35 View Security Configuration



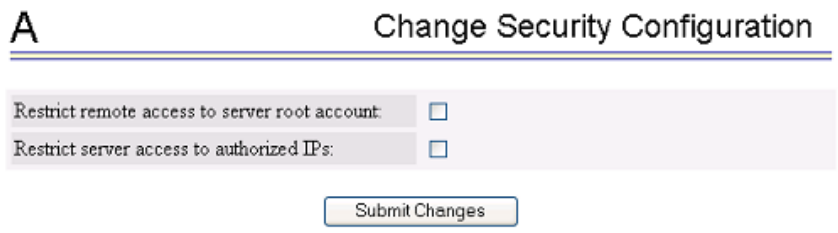
Change Security Configuration

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**, and then **EPAP Security**, and then **Change Security Configuration**.

Figure 3-36 Change Security Configuration



3.2.4 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:

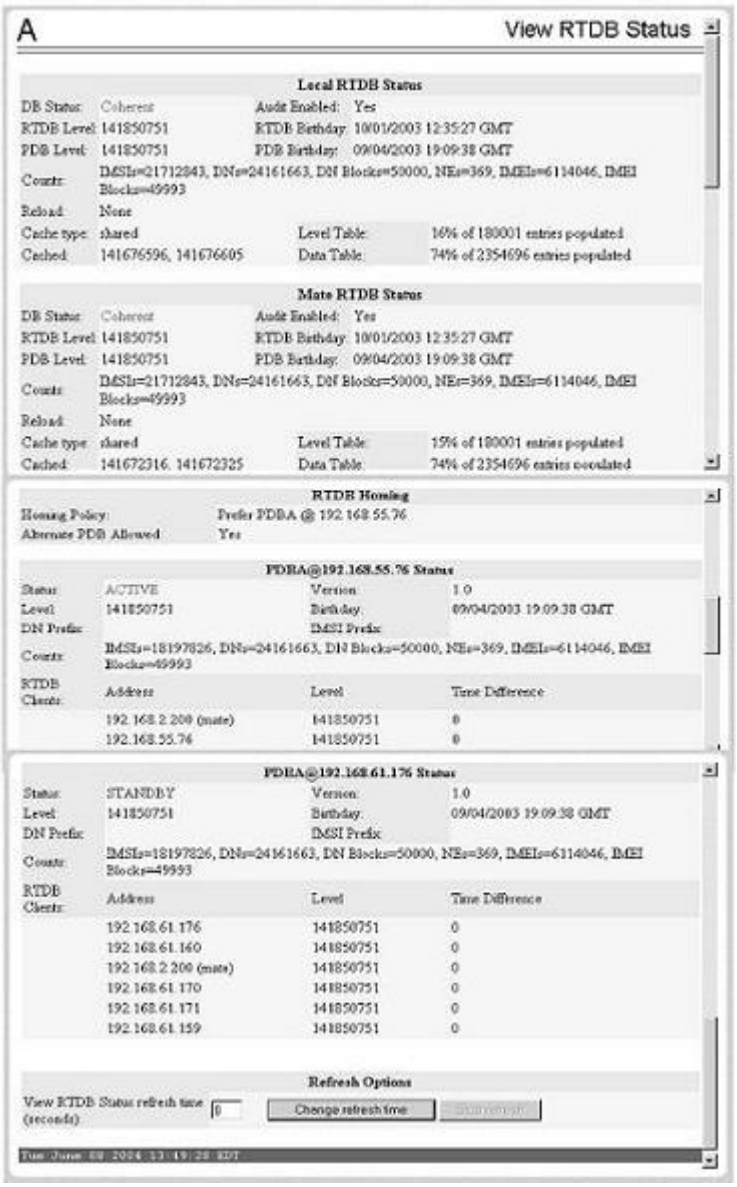
- View RTDB Status
- Maintenance
- Retrieve Records

3.2.4.1 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 3-37 View RTDB Status Screen



3.2.4.2 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
- Configure Record Delay

3.2.4.2.1 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.

See Table 3-10 for the rules about reloading the RTDB from the PDBA.

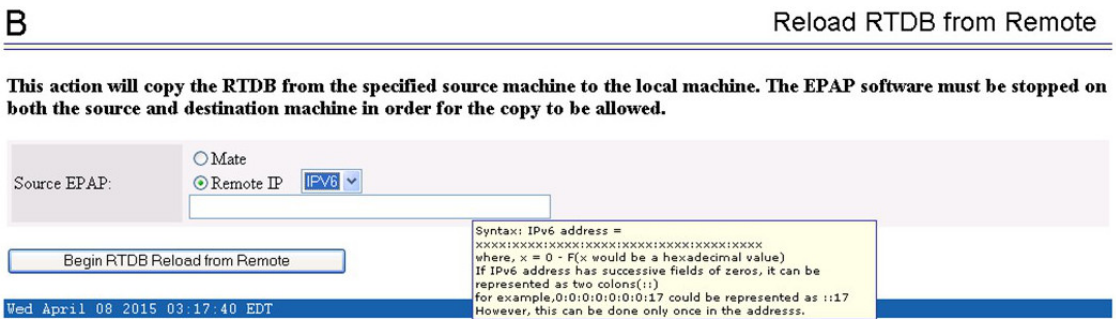
Table 3-10 Rules for the Reload RTDB from PDBA

Semantic Rules	Error Code
Other Messages	
Condition	Message Text

3.2.4.2.2 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 IPv4 or IPv6 address. Note: the EPAP software must be stopped on both of the machines involved:

Figure 3-38 Reload RTDB from Remote Screen



See Table 3-11 for the rules about reloading the **RTDB** from a remote.

Table 3-11 Rules for the Reload RTDB from Remote

Semantic Rules	Error Code
The mate EPAP must be available.	E1006
RTDB must acknowledge receipt of the reload request within 15 seconds.	E1031
Other Messages	

Table 3-11 (Cont.) Rules for the Reload RTDB from Remote

Condition	Message Text
RTDB reload started.	RTDB reload started. You will be notified when the reload is complete.
RTDB reload complete.	RTDB successfully reloaded from mate EPAP. You must remove the **STANDBY** restriction (by logging in as user 'epapmaint' and executing the “Remove Standby Restriction” menu item) before the selected EPAP can update the RTDB.

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

3.2.4.2.3 Backup the RTDB

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

See also Table 3-12 for the rules about backing up a **RTDB**.

Figure 3-39 Backup the RTDB Screen

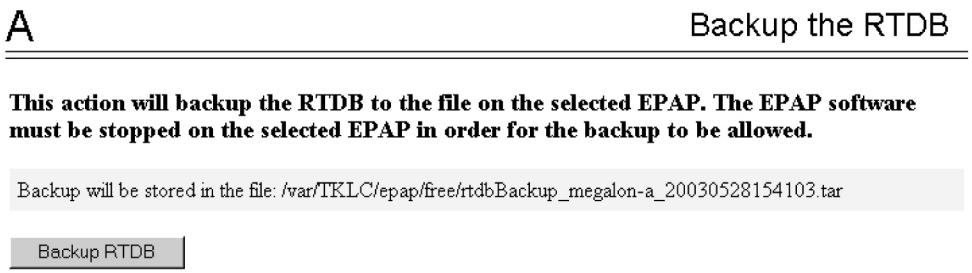


Table 3-12 Rules for Backup the RTDB Screen

Semantic Rules	Error Code
The device must exist.	E1019
Other Messages	
Condition	Message Text
Backup started.	Backup in progress. The backup requires approximately 35 minutes. You will be notified when the backup is complete
Backup did not start.	Backup failed.
Backup complete.	RTDB backup complete.

3.2.4.2.4 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.

See also Table 3-13 for the rules about backing up a RTDB.

Figure 3-40 Restore the RTDB

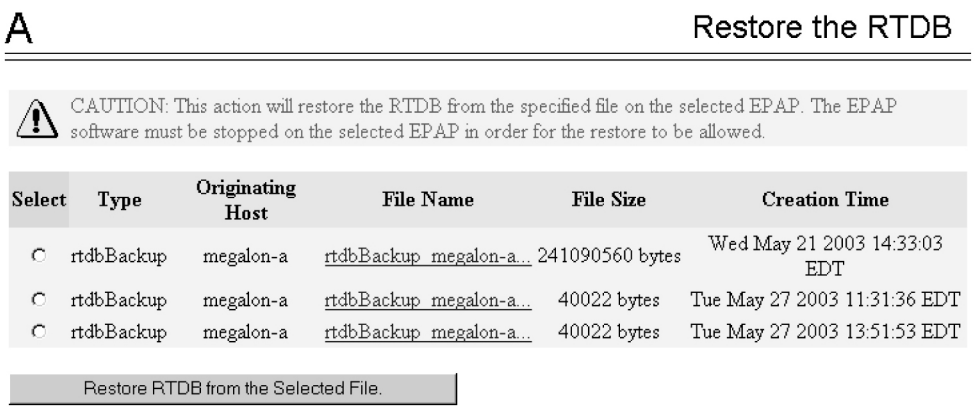


Table 3-13 Rules for Backup the RTDB Screen

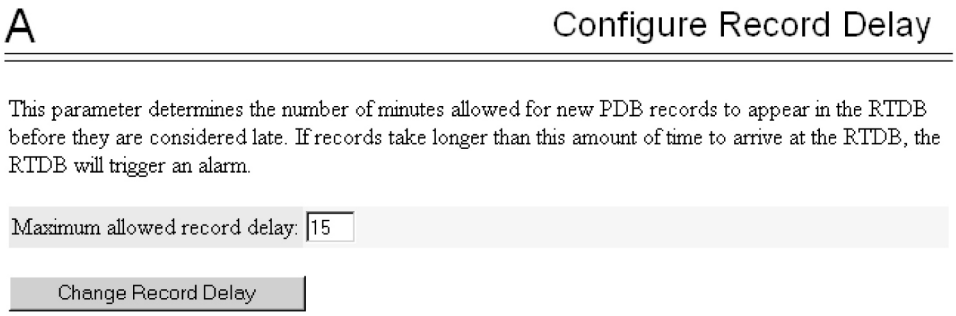
Semantic Rules		Error Code
The device must exist.		E1019
Other Messages		
Condition	Message Text	
Backup started.	Backup in progress. The backup requires approximately 35 minutes. You will be notified when the backup is complete	
Backup did not start.	Backup failed.	
Backup complete.	RTDB backup complete.	

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.

3.2.4.2.5 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 3-41 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.

Table 3-14 Rules for Configure Record Delay

Semantic Rules		Error Code
Other Messages		
Condition	Message Text	

Table 3-15 Rules for Backup the RTDB Screen

Semantic Rules		Error Code
The device must exist.		E1019
Other Messages		
Condition	Message Text	
Backup started.	Backup in progress. The backup requires approximately 35 minutes. You will be notified when the backup is complete	
Backup did not start.	Backup failed.	
Backup complete.	RTDB backup complete.	

3.2.4.3 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

A limit of 1,000 is imposed on the retrieval of DN, DN Blocks, NE, IMSI and IMEI. In order to fetch the next 1,000 entries the user has the following options:

1. Run another retrieval starting with the last entry in the last GUI retrieval.
2. Run the PDBA export (see PDBA / Maintenance / Export PDB to File).
3. Use the PDBA retrievals from the CLI PDBI Interface (see the "Simple Queries" section in *Provisioning Database Interface User's Guide*.

3.2.4.3.1 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)

3.2.4.3.2 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.

The maximum number of 9digs for a DN is 65K entries, which includes two (2) default entries representing 5 digits and 6 digits of DN, regardless if they are provisioned or not. If all provisioned DNs have digits greater than or equal to 7, the max number of 9digs parsed from these provisioned DNs cannot exceed 65K - 2 entries.

3.2.4.3.3 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.

3.2.4.3.4 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

3.2.4.3.5 IMEI

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

The output information displays:

- IMEI ID
- Software Version (SVN)
- Block list indicator
- Gray list indicator
- Allow 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.

3.2.4.3.6 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

- Block list indicator
- Gray list indicator
- Allow list indicator

3.2.5 Debug Menu

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

The Debug menu actions are:

- View Logs menu
- Capture Log Files screen
- Manage Logs and Backups screen
- View Any File screen
- List EPAP Processes screen

3.2.5.1 View Logs

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

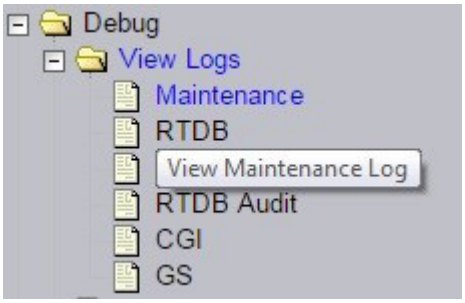
The View Logs submenu under the Debug menu has the following options:

- 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. Complete the following steps to view logs from the EPAP GUI menu:

1. Log in to the EPAP GUI
2. Expand the Debug Menu, then Select View Logs
3. Select a log file. Figure 3-42 shows the selection of the Maintenance log file:

Figure 3-42 Maintenance Log Option



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.

> **Note:**
>
> The system may ask you to change the `appuser` password from the CLI. If you change the password from the `root` user, the system will prompt you to change the password again. If the password is changed using the `appuser`, you will not be asked to change it an additional time.

4. Enter the password for the appuser and select the Submit button.

Figure 3-43 Log Viewer Password Prompt

When the user selects the Submit button without entering the password, the following error will display:

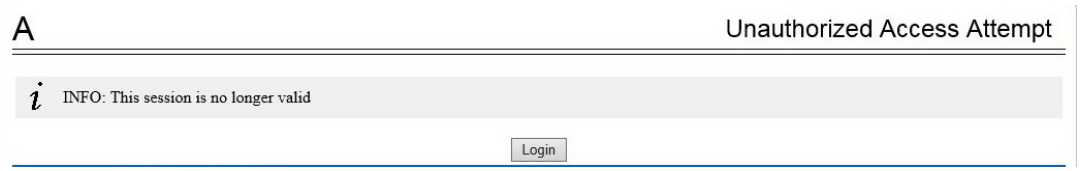
Figure 3-44 Log Viewer Password Missing

If the user enters an invalid password, the following error will display:

Figure 3-45 Log Viewer Invalid Password

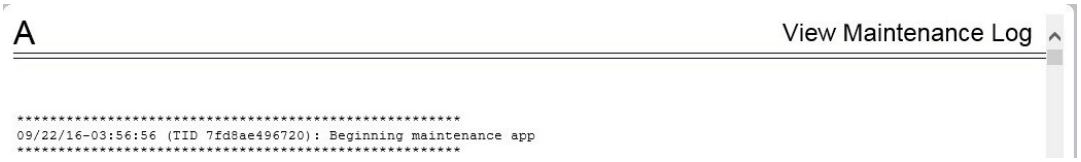
When the GUI session expires before the user submits a valid password, the following screen will display:

Figure 3-46 Log Viewer Session Expired



On the successful submission of the appuser password, the log file contents will be visible in the work area. Figure 3-47 shows an example of the Maintenance Log:

Figure 3-47 Maintenance Log Viewer



EPAP Log Viewer

Use the vertical scroll bar to scroll through the log viewer content. The Prev button will appear if the content of log file is greater than 100K lines. Initially it will be disabled for first 100K lines, as shown in Figure 3-48.

Figure 3-48 Log Viewer First Page

The Next button will appear if the content of the log file is greater than 100K lines. The first page will display the first 100k lines. The user will be able to select "Next" to view the next 100k lines (or the whole content if there are fewer than 100k lines), as seen in Figure 3-49.

Figure 3-49 Log Viewer Intermediate Page

When finished, close the Log Viewer window by clicking the Close View Window button.

3.2.5.2 Capture Log Files

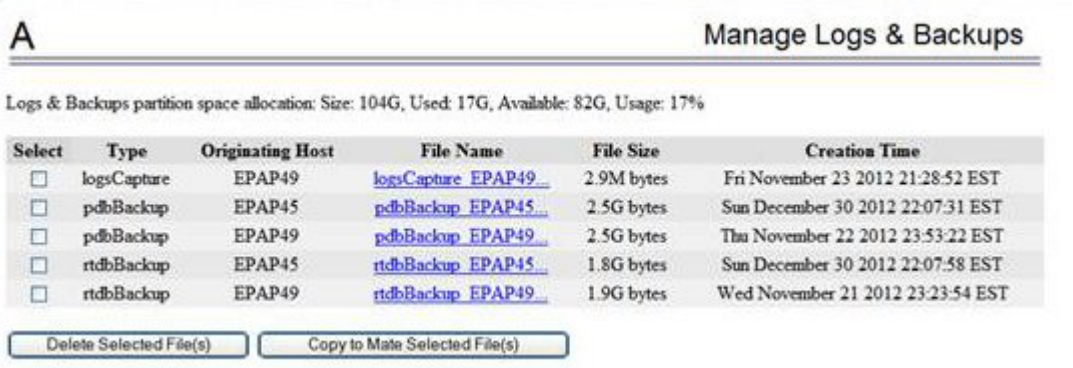
The Debug /Capture Log Files screen allows the user to make a copy of the logs for the current **MPS**. Optionally, you can capture files with the logs.

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

3.2.5.3 Manage Logs and Backups

The Debug / Manage Logs and Backups displays the captured log files and allows the user to delete the copies no longer wanted or copy the selected file to the mate. See Figure 3-50 with an example of one recorded log file on the Manage Log Files screen.

Figure 3-50 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.

3.2.5.4 View Any File

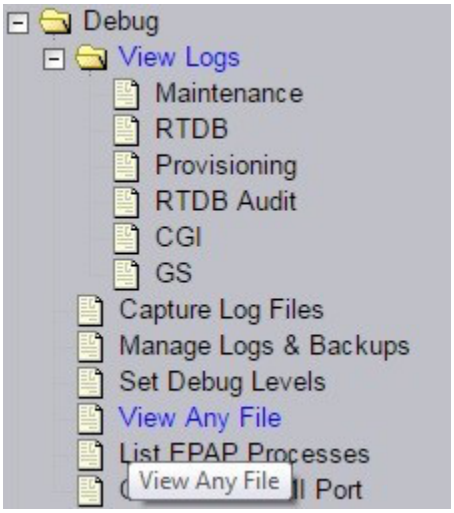
The View Any File screen allows the user to "view any log file" on the system using the Log Viewer by entering the authorized password for the user `appuser`. Log files that cannot be viewed from this utility include:

- `exinit.log`
- `slow-queries.log`
- `platwrap.log`
- `backupPdb.out`

When the user enters a filename, the Log Viewer is invoked. Complete the following steps in order to view logs using the View Any File menu on the EPAP GUI:

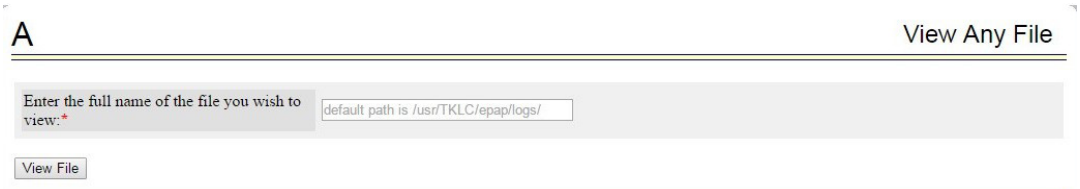
1. Log in to the EPAP GUI.
2. Expand the Debug menu.
3. Select **View Any File**.

Figure 3-51 View Any File on the EPAP GUI Menu



4. On selecting **View Any File**, the user will be asked to enter the filename to be viewed. The default path for this utility is `/usr/TKLC/epap/logs`. The filename field is mandatory (marked with * as displayed in Figure 3-52).

Figure 3-52 View Any File Filename Prompt

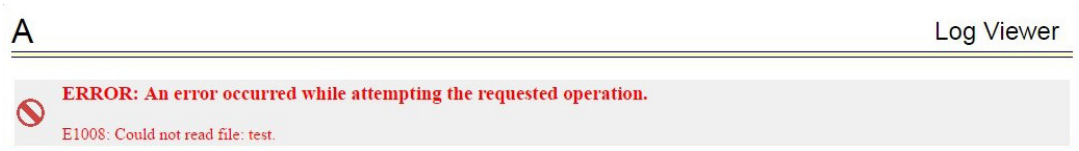


When the **View File** button is selected without inputting the filename, the following error will be displayed:

Figure 3-53 View Any File With Missing Filename

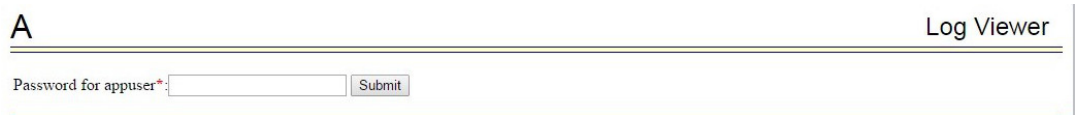
If the user inputs a non-existing filename in the `/usr/TKLC/epap/logs` directory, the following error will be displayed:

Figure 3-54 View Any File Non-Existing Filename Error



5. After entering a valid filename, the user will be prompted for the appuser password, as displayed in Figure 3-55:

Figure 3-55 View Any File Password Prompt

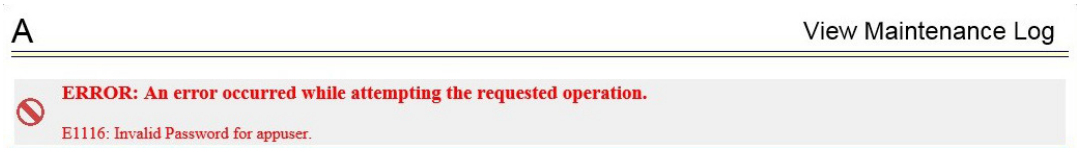


When the **Submit** button is selected without inputting the appuser password, the following error will be displayed:

Figure 3-56 Log Viewer Appuser Missing Password

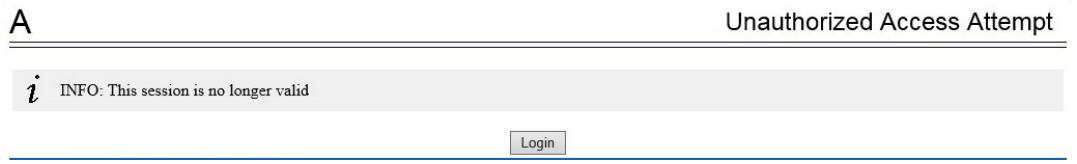
When the user inputs an invalid appuser password, the following error will be displayed:

Figure 3-57 Log Viewer Invalid Password Error



If the user enters a password after the GUI expires and selects **Submit**, the following error will be displayed:

Figure 3-58 Expired Log Viewer



6. After entering the valid appuser password, the log file contents will be visible in the work area, along with the log file name as its heading, as displayed in Figure 3-59:

Figure 3-59 Log Viewer

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.

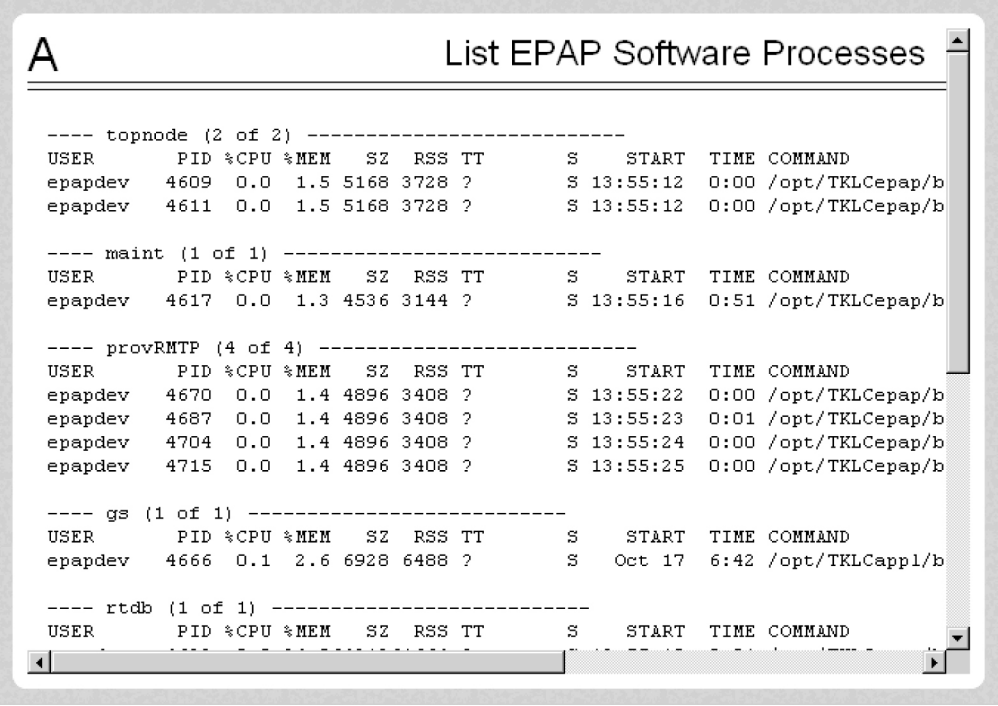
Table 3-16 Rules for Viewing Any File

Semantic Rules	Error Code
The file must exist and be readable.	E1008

3.2.5.5 List EPAP Processes

The Debug / List **EPAP** Processes screen shows the EPAP processes started when the EPAP boots or with the “Start EPAP software” prompt. The `/usr/ucb/ps -auxw` command generates this list. The operating system's manual page for the `ps` command thoroughly defines the output for this command. Figure 3-60 shows an example of the format of the process list.

Figure 3-60 Example of List EPAP Processes Output



3.2.6 Platform Menu

The Platform Menu allows the user to perform various platform-related functions. The Platform menu provides these actions:

- Run Health Check
- List All Running Processing
- View System Log View
- Reboot the MPS

- SSH to MPS

3.2.6.1 Run Health Check

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

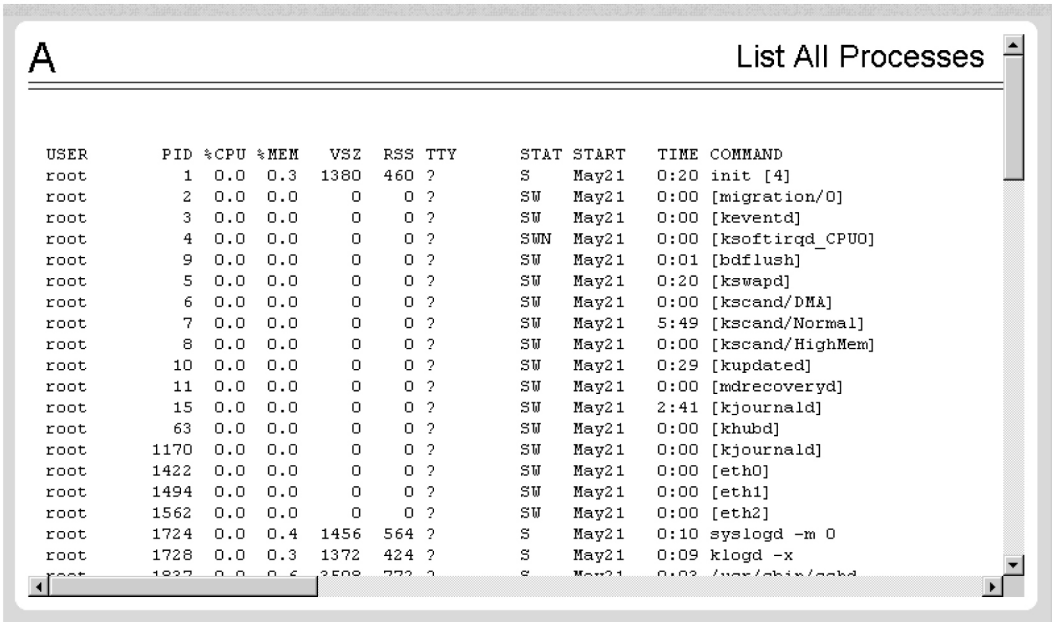
The first screen presented in the workspace frame lets the user select the *normal* or *verbose* mode of output detail.

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 System Health Check in *Alarms and Maintenance Guide* for the functions performed and how to interpret the results of the normal outputs

3.2.6.2 List All Processes

The Platform / List All Processes screen lists all processes running on the selected **EPAP**. The `/usr/ucb/ps -auxw` command generates this list. The operating system's manual page for the `ps` command thoroughly defines the output for this command. Figure 3-61 shows an example of the process list.

Figure 3-61 List All Processes Screen



> **Note:**
>
> The process list 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.

3.2.6.3 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.

The View System Logs - `/var/log/messages` is available under the Platform GUI menu.

3.2.6.4 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.

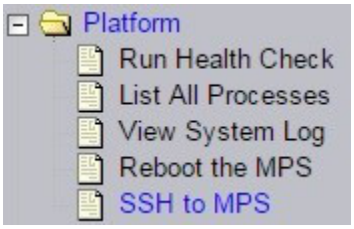
Click the Continue button. Another screen informs you that MPS is being rebooted and that the User Interface will be reconnected when the reboot is completed.

3.2.6.5 SSH to MPS

The Platform / **SSH** to **MPS** screen allows the user to have an `SSH` window to the user interface user. This uses WebStart Java technology, which works independent of the web browser once it is launched. Complete the following steps to perform SSH to MPS:

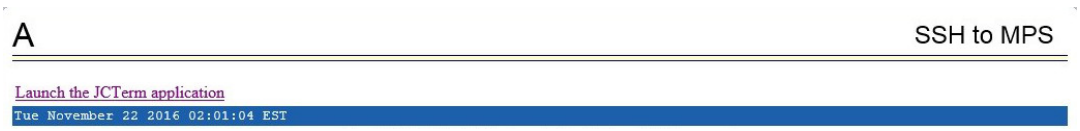
1. Log in to the EPAP.
2. Select **Platform Menu**, and then **SSH to MPS**, as displayed in Figure 3-62:

Figure 3-62 SSH to MPS on the EPAP GUI Menu



3. Select **Launch the JCTerm application**:

Figure 3-63 JCTerm Application Launch Window

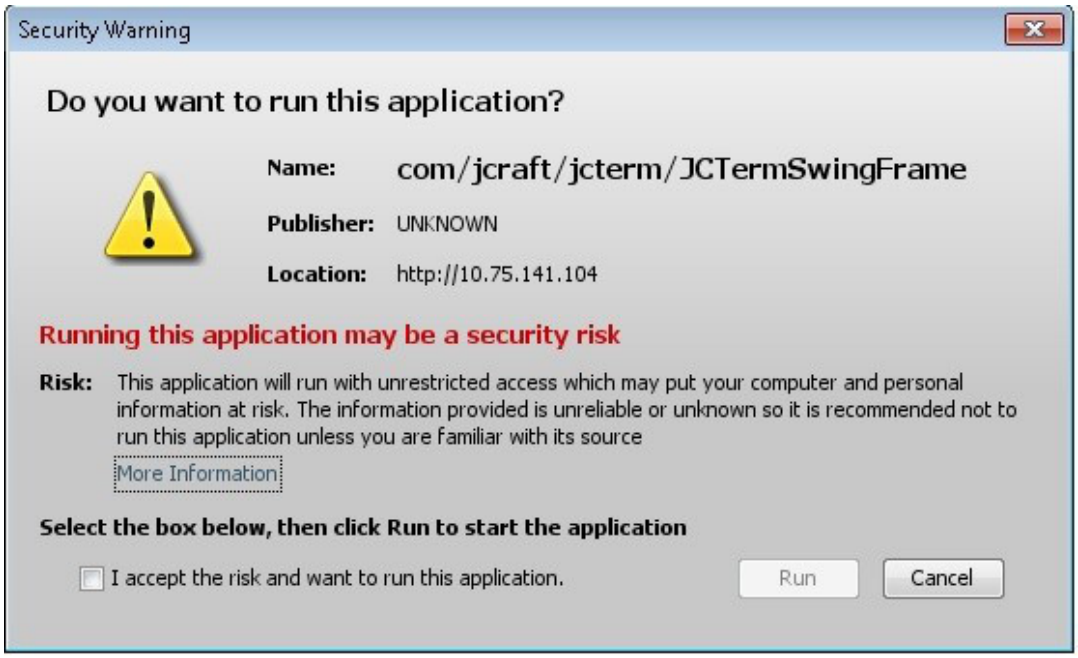


The following screen will appear:

Figure 3-64 Launching WebStart

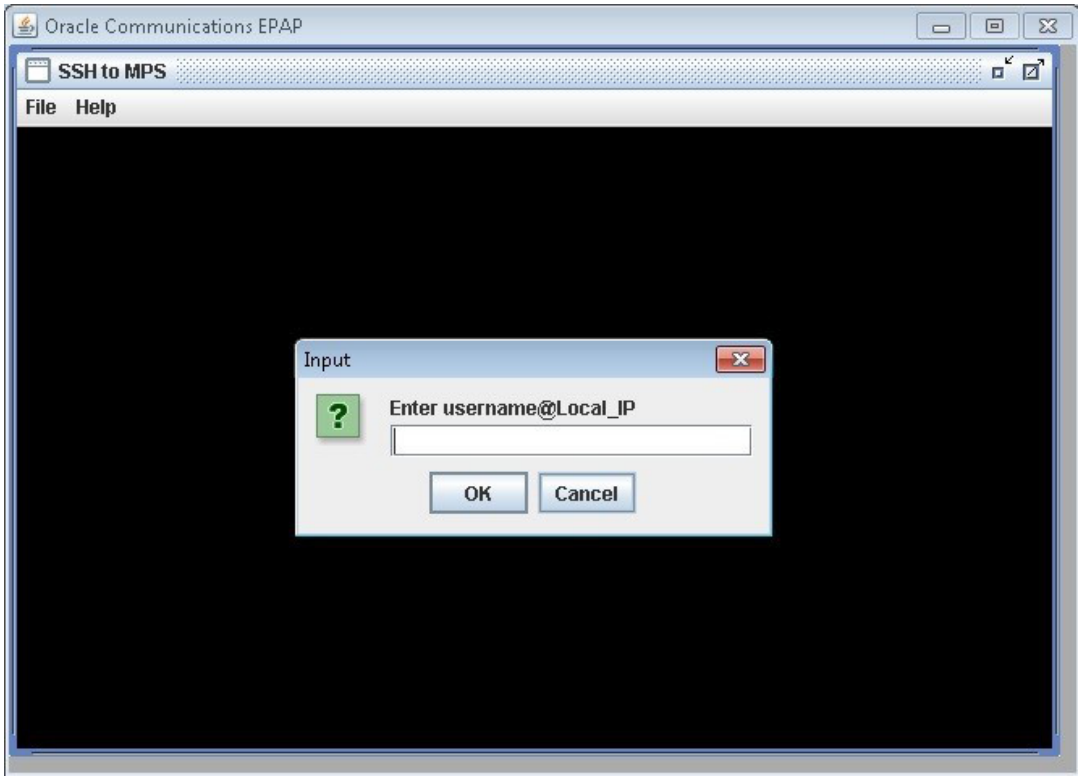
4. The JCTerm jar, along with the `Jzlib jar` and `Jsch jar`, are self-signed. Accept the security check that follows and select **Run** to launch the JCTerm applet for the SSH to MPS interface:

Figure 3-65 JCTerm Security Check Window



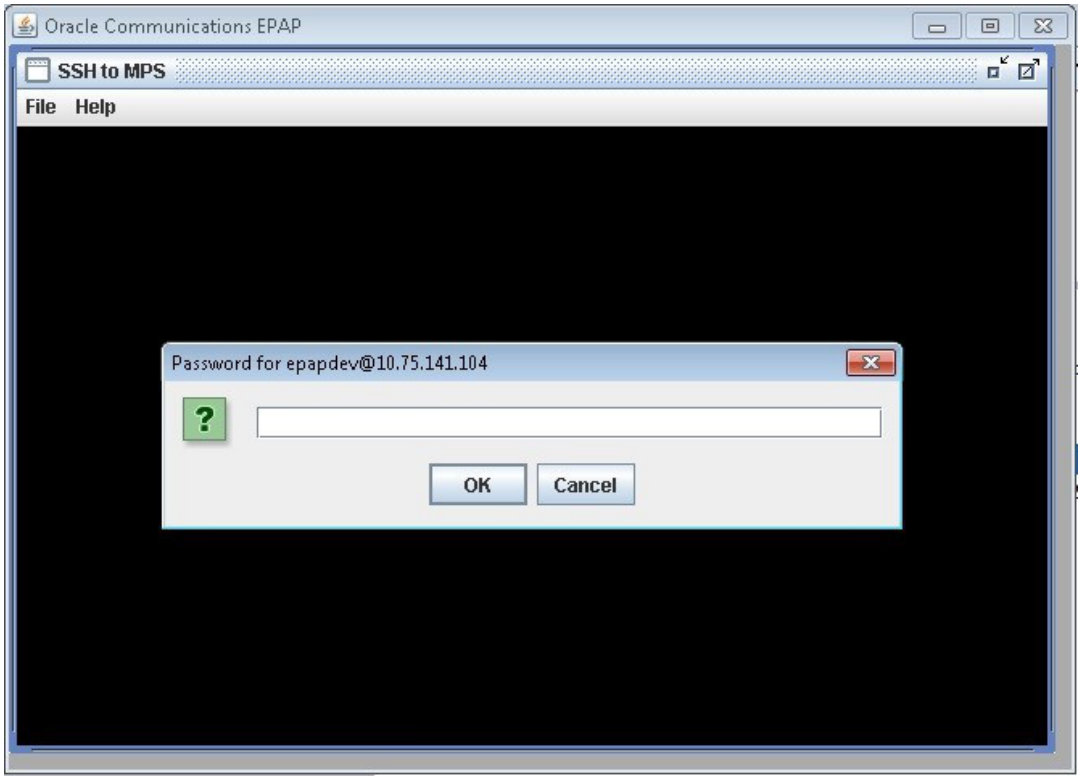
5. The SSH to MPS window will be displayed. A user name and password is required. On the EPAP configured in the dual stack configuration, both the IPv4 and IPv6 addresses for Local EPAP are accepted for the SSH. The following formats are accepted:
   a. sshusername@<IPv4 IP>
   b. sshusername@<IPv4 IP>:<Port>
   c. sshusername@IPv6 IP>
   d. sshusername@[IPv6 IP>]
   e. sshusername@[IPv6 IP>]:<Port>

Figure 3-66 SSH to MPS Log in Window



After inputting a user name and local EPAP IP, the password prompt window appears, as displayed in Figure 3-67:

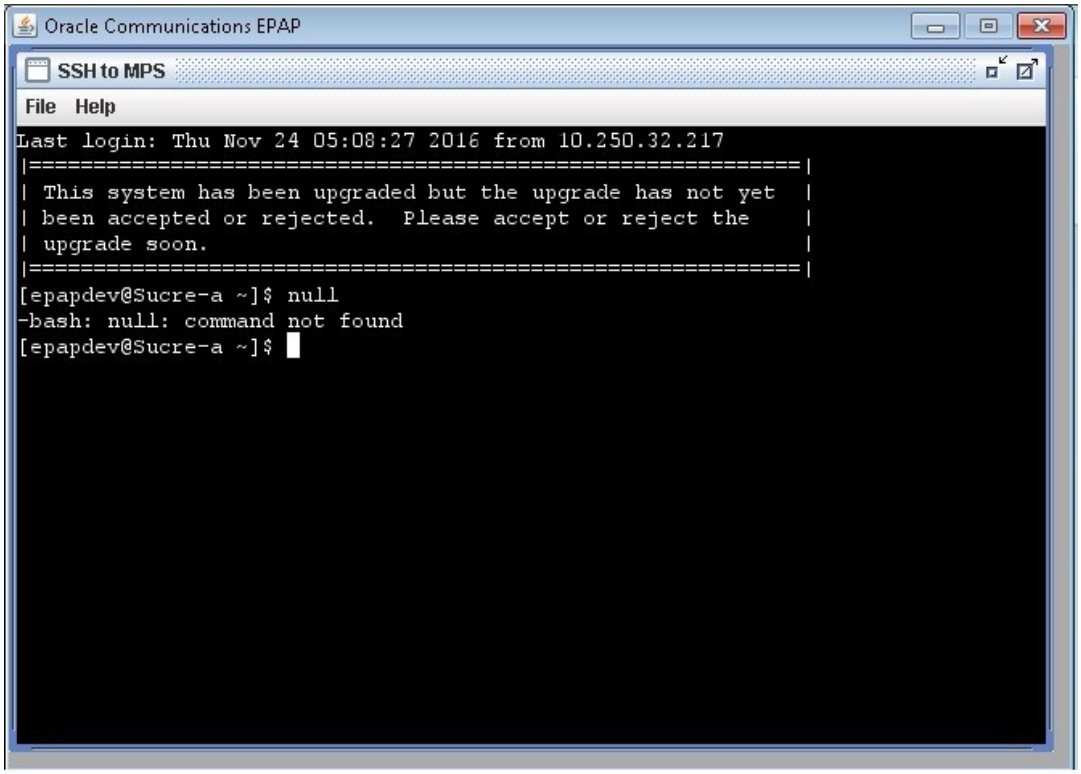
Figure 3-67 SSH to MPS Password Prompt Window



After a successful log in, the SSH window opens and can be used to perform SSH communications, as displayed in Figure 3-68:

> **Note:**
>
> There is no limit to the maximum number of concurrent sessions opened using the SSH to MPS utility.

Figure 3-68 SSH to MPS Interface



3.2.7 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
- List PDBI Connections
- PDBI Statistics Report

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.

3.2.7.1 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. When the EPAP is configured in the dual stack configuration, then the user has the option to configure the remote PDBA in either IPv4 or IPv6 configuration. See PDB Configuration Menu for remote PDBA configuration details.

See Table 3-17 for the rules for the Select Other PDBA screen:

Table 3-17 Rules for Select Other PDBA

Semantic Rules	Error Code
The other PDBA must be reachable.	E1020

3.2.7.2 Switchover PDBA State

The **PDBA** / Switchover PDBA State 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.

3.2.7.3 Process Control

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

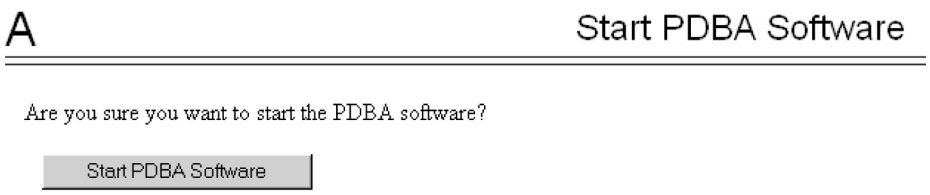
The PDBA / Process Control menu provides these actions:

- 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 3-69 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. If this 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.

3.2.7.4 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.

When the EPAP is configured in the dual stack configuration, the PDBA will also have both IPs. On the "View PDBA Status" screen, the PDBA IP will be in the IP version format with which the EPAP GUI is accessed. If the EPAP GUI is accessed using the IPv6 IP, then the PDBA IP will be displayed in the IPv6 format. If the EPAP GUI is accessed using the IPv4 IP, then the PDBA IP will be displayed in the IPv4 format.

See the rules for screen in Table 3-18.

Figure 3-70 View PDBA Status With IPv6 PDBA IP

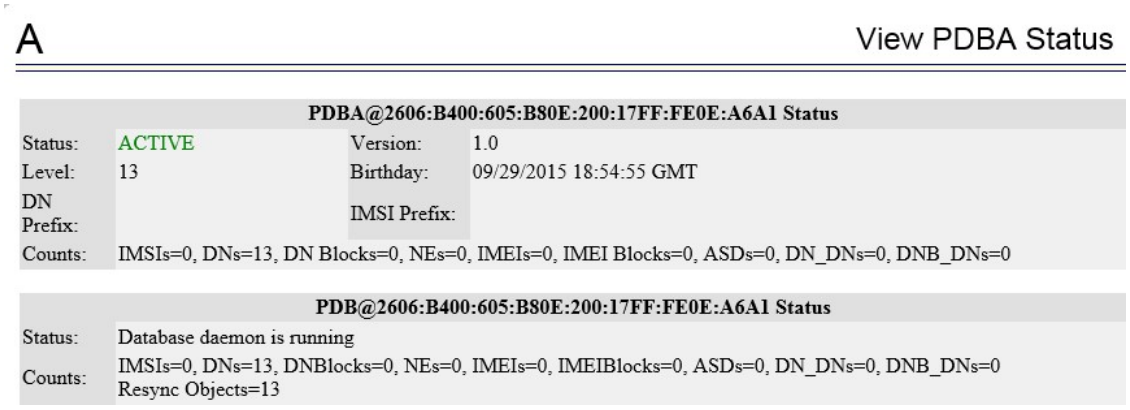


Figure 3-71 View PDBA Status With IPv4 PDBA IP

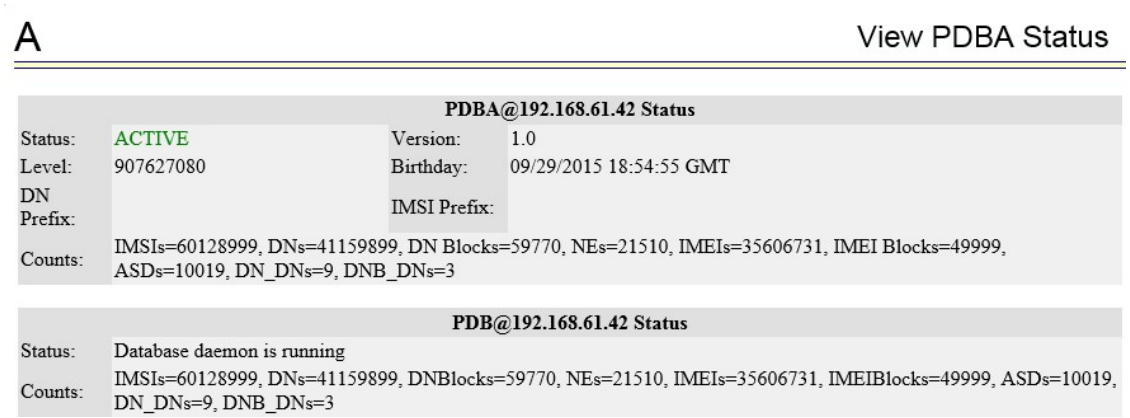


Table 3-18 Rules for Viewing PDBA Status

Semantic Rules	Error Code
PDBA must respond within 15 seconds.	E1030

> **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.

3.2.7.5 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
- DN
- DN Block
- Network Entity
- Individual IMEI
- Block IMEI
- Send Raw PDBI Command
- EPAP Provisioning Blocklist Menu

3.2.7.5.1 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.

There are limited numbers of digit combinations in the first 9 digits of DN/IMSI/IMEI. In DN/IMSI the first 9 digits consist of the Country Code, Area Code, Service Provider Code, and up to 2 digits of Subscriber number. The maximum number of 9digs is 65K entries, which includes two (2) default entries representing 5 digits and 6 digits, regardless if they are provisioned or not. If all provisioned DN/IMSIs have digits greater than or equal to 7, the max number of 9digs parsed from these provisioned DNs cannot exceed 65K - 2 entries.

Figure 3-72 Add an IMSI

Table 3-19 describes the rules that the EPAP user interface uses to perform the Add IMSI action. The table also describes other messages generated by the EPAP user interface while performing this action.

Table 3-19 Rules for Add IMSI Screen

Syntax Rules	Error Code
The user must enter a valid **SP**.	E1002
The user must enter a valid IMSI.	E1002
The user must enter a valid **DN**.	E1002
Semantic Rules	Error Code
This menu option is valid only if the **G-Flex** feature is installed.	None
The SP must exist in the PDB.	E1014
The user may enter up to 8 DNs	None
The user may elect to force the transaction to be entered into the PDB, even if there are conflicting subscriptions.	None
The PDBI must return a success status.	E1017
PDBI command `ent-sub`, on the creation of a single IMSI with or without DNs, supports a response "PDBI_MAX_IMSI9DIG_LIMIT" if the to-be provisioned IMSI causes the first 9 digits go above its max limit of 65,000.	E1066
PDBI command `ent-sub`, on the creation of one IMSI to 1-8 DNs, supports a response "PDBI_MAX_DN9DIG_LIMIT" if the to-be provisioned DN causes the first 9 digits go above its max limit of 65,000.	E1068
Other Messages	
Condition	Message Text

Table 3-19 (Cont.) Rules for Add IMSI Screen

The new subscription already exists in the PDB.	This subscription conflicts with an existing subscription.
The new subscription was attempting to overwrite an existing IMSI.	IMSI <imsi> already exists in the PDB. If you choose to overwrite the existing subscription, all data associated with the existing IMSI will be lost. All DNs associated with the existing IMSI will be deleted.
The subscription was added.	Subscription successfully added.
The subscription was not added.	Subscription not added.

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).

Figure 3-73 Update an IMSI

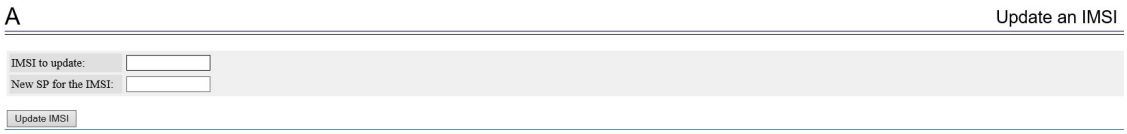


Table 3-20 describes the rules that the EPAP user interface uses to perform the Update IMSI action. The table also describes other messages generated by the EPAP user interface while performing this action.

Table 3-20 Rules for Update IMSI Screen

Syntax Rules	Error Code
The user must enter a valid SP.	E1002
The user must enter a valid IMSI.	E1002
Semantic Rules	**Error Code**
This menu option is valid only if the G-Flex feature is installed.	None
The IMSI must exist in the PDB.	E1015
The SP must exist in the PDB.	E1014
The PDBI must return a success status.	E1017
Other Messages	
Condition	**Message Text**
The subscription was modified.	Subscription successfully modified.
The subscription was not modified.	Subscription not modified.

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).

Table 3-21 describes the rules that the EPAP user interface uses to perform the Delete IMSI action. The table also describes other messages generated by the EPAP user interface while performing this action.

Table 3-21 Rules for Delete IMSI Screen

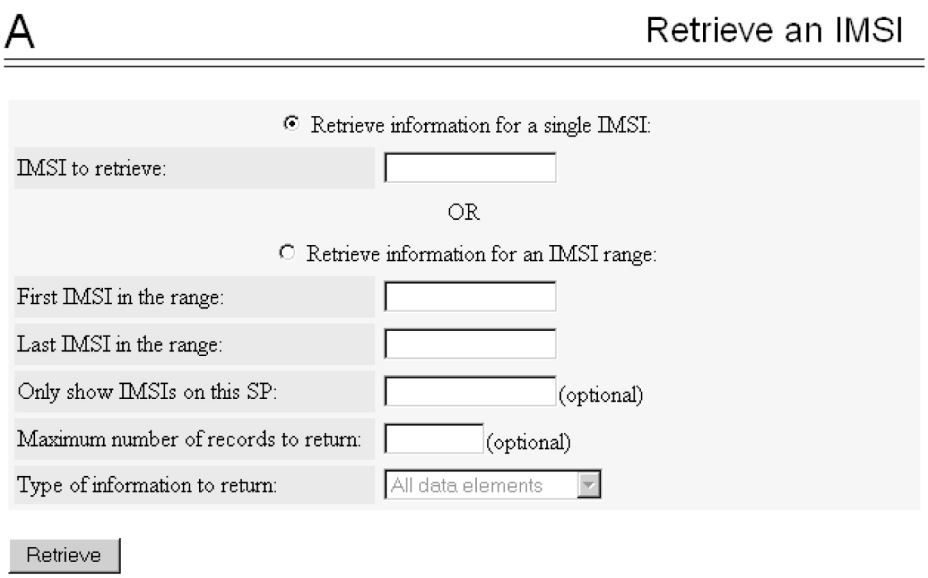
Syntax Rules		Error Code
The user must enter a valid IMSI.		E1002
Semantic Rules		Error Code
This menu option is valid only if the G-Flex feature is installed.		None
The subscription must exist in the PDB.		E1012
The PDBI must return a success status.		E1017
Other Messages		
Condition	Message Text	
The subscription was deleted.	Subscription successfully deleted.	
The subscription was not deleted.	Subscription not deleted.	

Retrieve an IMSI

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

Figure 3-74 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 3-74 Retrieve IMSI Screen



3.2.7.5.2 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.

Table 3-22 describes the rules that the EPAP user interface uses to perform the Add IMSI action. The table also describes other messages generated by the EPAP user interface while performing this action.

Table 3-22 Rules for Add IMSI Range Screen

Syntax Rules	Error Code
The user must enter a valid SP.	E1002
The user must enter a valid IMSI.	E1002
The user must enter a valid DN.	E1002
Semantic Rules	Error Code
This menu option is valid only if the **G-Flex** feature is installed.	None
The SP must exist in the **PDB**.	E1014
The user may enter up to 8 DNs	None
The user may elect to force the transaction to be entered into the PDB, even if there are conflicting subscriptions.	None
The PDBI must return a success status.	E1017
Other Messages	
Condition	Message Text

Table 3-22 (Cont.) Rules for Add IMSI Range Screen

The new subscription already exists in the PDB.	This subscription conflicts with an existing subscription.
The new subscription was attempting to overwrite an existing IMSI.	IMSI <imsi> already exists in the PDB. If you choose to overwrite the existing subscription, all data associated with the existing IMSI will be lost. All DNs associated with the existing IMSI will be deleted.
The subscription was added.	Subscription successfully added.
The subscription was not added.	Subscription not added.

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.

Table 3-23 describes the rules that the EPAP user interface uses to perform the Update IMSI action. The table also describes other messages generated by the EPAP user interface while performing this action.

Table 3-23 Rules for Update IMSI Range Screen

Syntax Rules	Error Code
The user must enter a valid SP.	E1002
The user must enter a valid IMSI.	E1002
Semantic Rules	Error Code
This menu option is valid only if the G-Flex feature is installed.	None
The IMSI must exist in the PDB.	E1015
The SP must exist in the PDB.	E1014
The PDBI must return a success status.	E1017
Other Messages	
Condition	Message Text
The subscription was modified.	Subscription successfully modified.
The subscription was not modified.	Subscription not modified.

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.

Table 3-24 describes the rules that the EPAP user interface uses to perform the Delete IMSI action. The table also describes other messages generated by the EPAP user interface while performing this action.

Table 3-24 Rules for Delete IMSI Range Screen

Syntax Rules		Error Code
The user must enter a valid IMSI.		E1002
Semantic Rules		Error Code
This menu option is valid only if the G-Flex feature is installed.		None
The subscription must exist in the PDB.		E1012
The PDBI must return a success status.		E1017
Other Messages		
Condition	Message Text	
The subscription was deleted.	Subscription successfully deleted.	
The subscription was not deleted.	Subscription not deleted.	

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.

Table 3-25 describes the rules that the EPAP user interface uses to perform the Retrieve IMSI action. The table also describes other messages generated by the EPAP user interface while performing this action.

Table 3-25 Rules for Retrieve IMSI Range Screen

Syntax Rules	Error Code
The user must enter a valid IMSI.	E1002
The user must enter a valid SP.	E1002
Semantic Rules	Error Code
This option is valid only if the G-Flex feature is installed.	None
The type of output data to return may only be entered if a range of IMSIs is requested.	None
The maximum number of records to return may only be entered if a range of IMSIs is requested.	None

Table 3-25 (Cont.) Rules for Retrieve IMSI Range Screen

The PDBI must return a success status.		E1017
Other Messages		
Condition	Message Text	
No records were found.	Query returned no subscriptions.	

3.2.7.5.3 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.

> **Note:**
>
> It is not recommended to provision more than 60 millions of Number Substitute of DN (NSDN). Higher NSDN data causes a failure in the RTDB reload from the PDB.

See Figure 3-75 for an example of the Add a DN screen.

Figure 3-75 Add a DN Screen

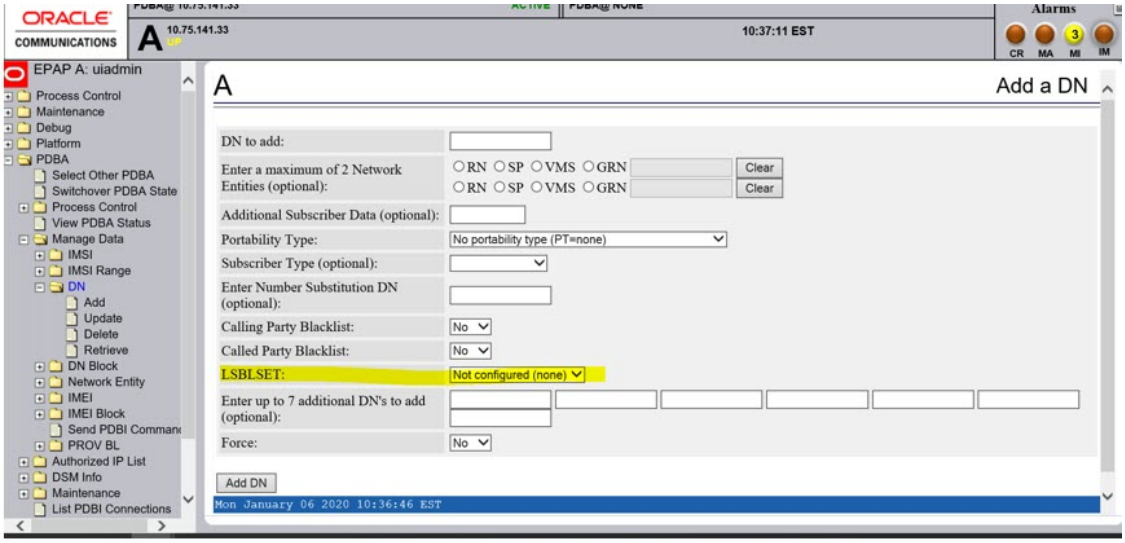


Table 3-26 describes the rules that the EPAP user interface uses to perform the Add DN action. The table also describes other messages generated by the EPAP user interface while performing this action.

Table 3-26 Rules for Add DN Screen

Syntax Rules	Error Code
The user must enter a valid **SP**.	E1002
The user must enter a valid **IMSI**.	E1002
The user must enter a valid **DN**.	E1002
Semantic Rules	**Error Code**
The user may enter a portability type only if an SP was not specified.	None
The SP must exist in the PDB.	E1014
The **RN** must exist in the PDB.	E1014
The user may enter up to 8 DNs	None
The user may elect to force the transaction to be entered into the PDB, even if there are conflicting subscriptions.	None
The PDBI must return a success status.	E1017
PDBI command `ent-sub`, on the creation of one or more DNs on the same NE with no IMSI, supports a response "PDBI_MAX_IMSI9DIG_LIMIT" if the to-be provisioned DN causes the first 9 digits go above its max limit of 65,000.	E1068
Other Messages	
Condition	**Message Text**
The new subscription already exists in the PDB.	This subscription conflicts with an existing subscription.
The new subscription was attempting to overwrite an existing DN.	One of the DNs already exist in the PDB. If you choose to overwrite the existing subscription, all data associated with the existing DN will be lost.
The subscription was added.	Subscription successfully added.

Table 3-26 (Cont.) Rules for Add DN Screen

The subscription was not added.	Subscription not added.

Update a DN

The PDBA / Manage Data / DN / Update a DN screen prompts you for the fields necessary to change the SP or RN for an DN in the Provisioning Database (PDB). See Figure 3-76 for an example of the Update a DN menu.

Figure 3-76 Update a DN Screen

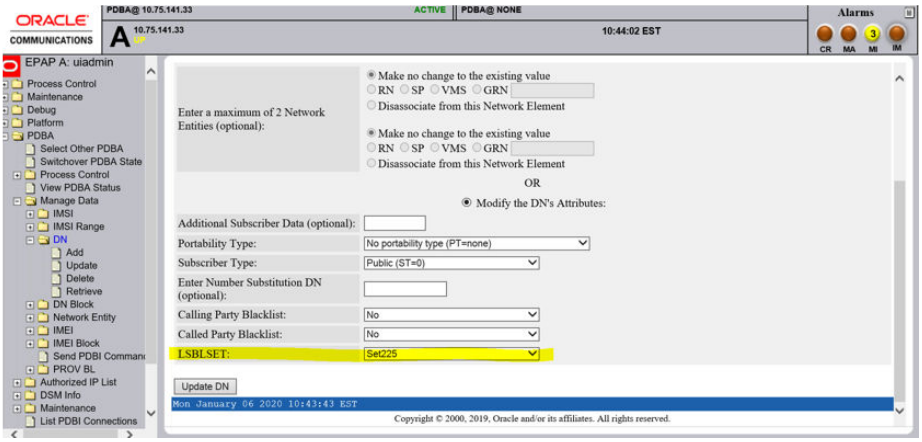


Table 3-27 describes the rules that the EPAP user interface uses to perform the Update DN action. The table also describes other messages generated by the EPAP user interface while performing this action.

Table 3-27 Rules for Update a DN Screen

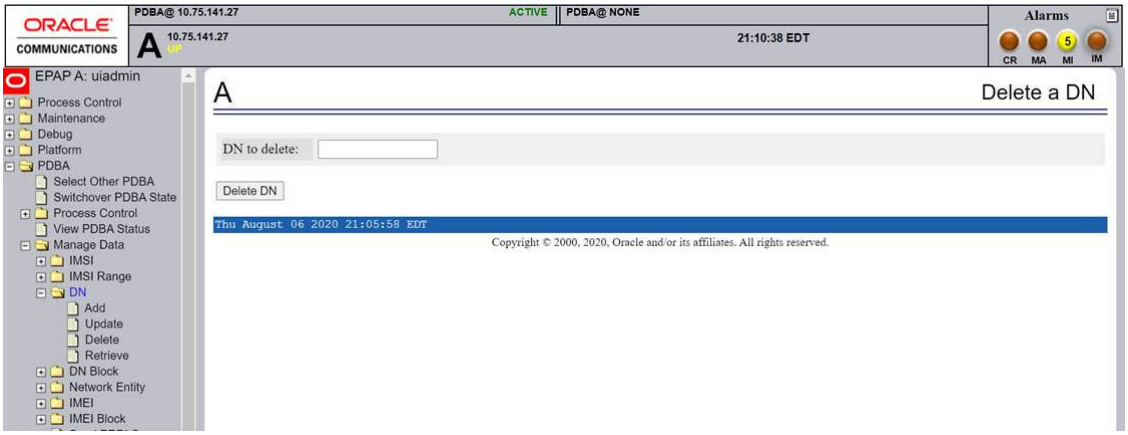
Syntax Rules	Error Code
The user must enter a valid SP.	E1002
The user must enter a valid RN.	E1002
The user must enter a valid IMSI.	E1002
The user must enter a valid DN.	E1002
Semantic Rules	**Error Code**
This menu option is valid only if the **G-Flex** feature is installed.	None
The SP must exist in the PDB.	E1014
The RN must exist in the PDB.	E1022
The DN must exist in the PDB.	E1016
The IMSI must exist in the PDB.	E1015
The DN may not be already associated with an IMSI.	E1018
The user my only enter a portability type if an RN is specified.	None
The PDBI must return a success status.	E1017

Table 3-27 (Cont.) Rules for Update a DN Screen

PDBI command `ent-sub`, on the creation of a single IMSI with or without DNs, supports a response "PDBI_MAX_IMSI9DIG_LIMIT" if the to-be provisioned IMSI causes the first 9 digits go above its max limit of 65,000.	E1066
Other Messages	
Condition	Message Text
The subscription was modified.	Subscription successfully modified.
The subscription was not modified.	Subscription not modified.

Delete a DN

Figure 3-77 Delete a DN Screen



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).

Table 3-28 describes the rules that the EPAP user interface uses to perform the Delete DN action. The table also describes other messages generated by the EPAP user interface while performing this action.

Table 3-28 Rules for Delete DN Screen

Syntax Rules	Error Code
The user must enter a valid DN.	E1002
Semantic Rules	Error Code
The subscription must exist in the PDB.	E1012
The PDBI must return a success status.	E1017
Other Messages	
Condition	Message Text
The subscription was deleted.	Subscription successfully deleted.
The subscription was not deleted.	Subscription not deleted.

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.

Figure 3-78 Retrieve a DN

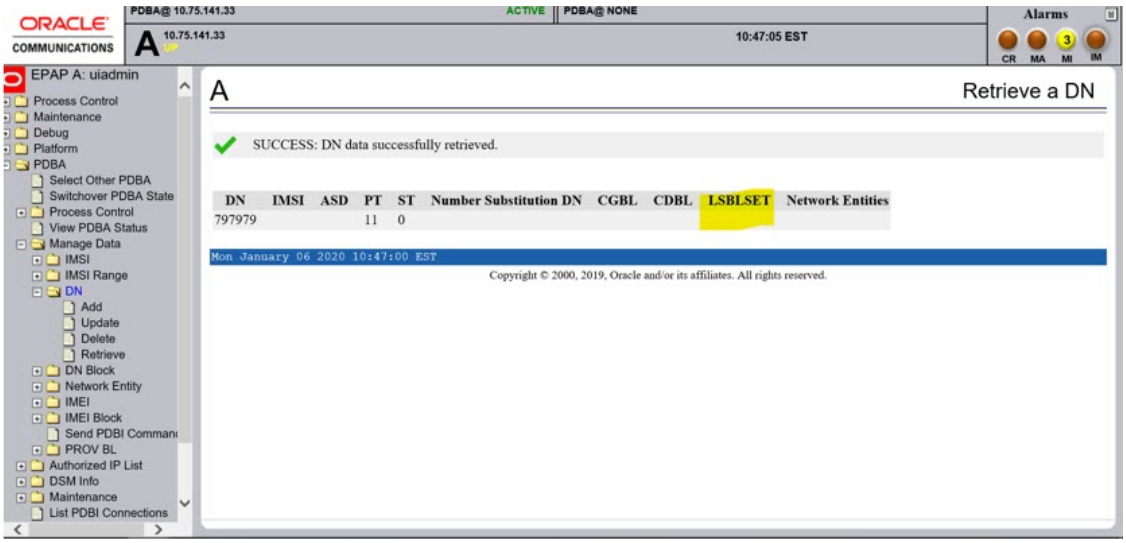


Table 3-29 describes the rules that the EPAP user interface uses to perform the Retrieve DN action. The table also describes other messages generated by the EPAP user interface while performing this action.

Table 3-29 Rules for Retrieve DN Screen

Syntax Rules	Error Code
The user must enter a valid DN.	E1002
The user must enter a valid SP.	E1002
The user must enter a valid RN.	E1002
Semantic Rules	**Error Code**
The user may enter a range of DNs.	None
The user may only enter an SP if **G-Flex** or **G-Port** is installed.	None
The user may only enter an RN if G-Port or **INP** is installed.	None
The type of output data to return may only be entered if a DN range is requested.	None
The maximum number of records to return may only be entered if a DN range is entered.	None
The PDBI must return a success status.	E1017
Other Messages	
Condition	**Message Text**
No records were found.	Query returned no subscriptions.

3.2.7.5.4 DN Block

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

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

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

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.

Figure 3-79 Add a DN Block

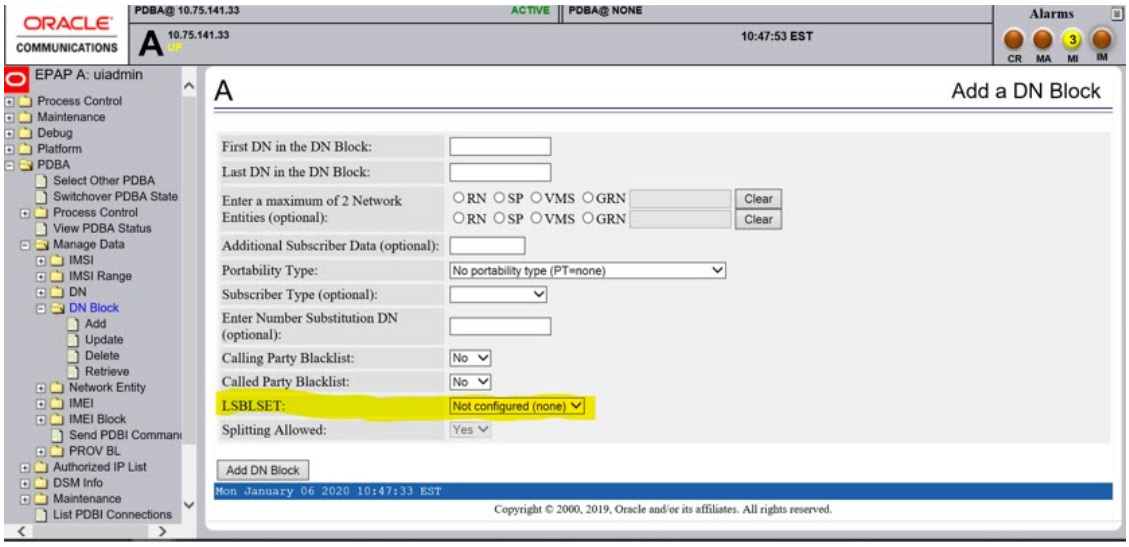


Table 3-30 describes the rules that the EPAP user interface uses to perform the Add DN Block action. The table also describes other messages generated by the EPAP user interface while performing this action.

Table 3-30 Rules for Add DN Block Screen

Syntax Rules	Error Code
The user must enter a valid SP.	E1002
The user must enter a valid RN.	E1002
The user must enter a valid DN.	E1002

Table 3-30 (Cont.) Rules for Add DN Block Screen

Semantic Rules	Error Code
This menu option is valid only if the **G-Port** or **INP** feature is installed.	None
The SP must exist in the PDB.	E1014
The RN must exist in the PDB.	E1014
The user may enter a portability type only if a SP was not specified.	None
The user may elect to force the transaction to be entered into the PDB, even if there are conflicting subscriptions.	None
The PDBI must return a success status.	E1017
Other Messages	
Condition	Message Text
The new subscription already exists in the PDB.	This subscription conflicts with an existing subscription.
The new subscription was attempting to overwrite an existing **IMSI**.	DN block <start DN-end DN> already exists in the PDB. If you choose to overwrite the existing subscription, all data associated with the existing DN block will be lost
The new subscription was attempting to overwrite an existing DN block.	DN block <start DN-end DN> already exists in the PDB. If you choose to overwrite the existing subscription, all data associated with the existing DN block will be lost
The subscription was added.	Subscription successfully added.
The subscription was not added.	Subscription not added.

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).

Figure 3-80 Update a DN Block Screen

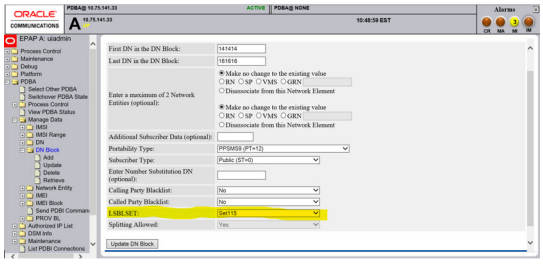


Table 3-31 describes the rules that the EPAP user interface uses to perform the Update DN Block action. The table also describes other messages generated by the EPAP user interface while performing this action.

Table 3-31 Rules for Update a DN Block Screen

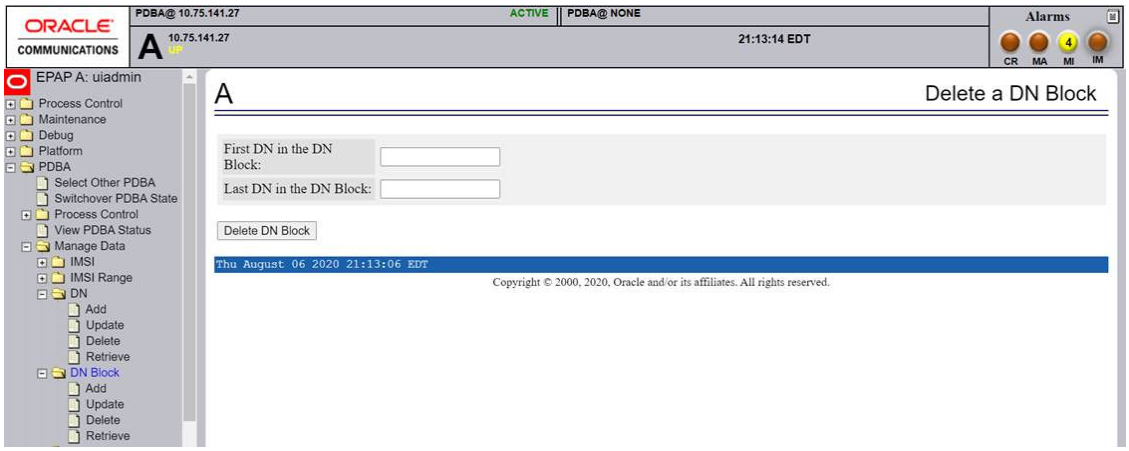
Syntax Rules	Error Code

Table 3-31 (Cont.) Rules for Update a DN Block Screen

The user must enter a valid SP.		E1002
The user must enter a valid RN.		E1002
The user must enter a valid DN.		E1002
Semantic Rules		Error Code
This menu option is valid only if the G-Port or INP feature is installed.		None
The SP must exist in the PDB.		E1014
The RN must exist in the PDB.		E1022
The DN block must exist in the PDB.		E1016
The DN may not be already associated with an IMSI.		E1018
The user my enter a portability type only if an RN is specified.		None
The PDBI must return a success status.		E1017
Other Messages		
Condition	Message Text	
The subscription was modified.	Subscription successfully modified.	
The subscription was not modified.	Subscription not modified.	

Delete a DN Block

Figure 3-81 Delete a DN Block Screen



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).

Table 3-32 describes the rules that the EPAP user interface uses to perform the Delete DN Block action. The table also describes other messages generated by the EPAP user interface while performing this action.

Table 3-32 Rules for Delete DN Block Screen

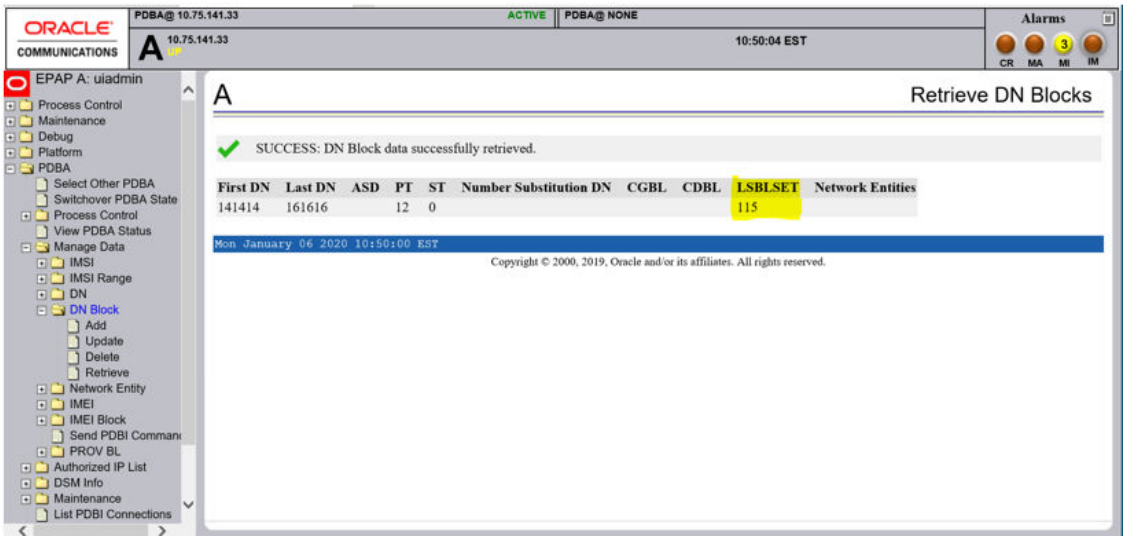
Syntax Rules	Error Code

Table 3-32 (Cont.) Rules for Delete DN Block Screen

The user must enter a valid DN.		E1002
Semantic Rules		Error Code
The menu option is valid only if the G-Port or INP feature is installed.		None
The subscription must exist in the PDB.		E1012
The PDBI must return a success status.		E1017
Other Messages		
Condition	Message Text	
The subscription was deleted.	Subscription successfully deleted.	
The subscription was not deleted.	Subscription not deleted.	

Retrieve DN Blocks

Figure 3-82 Retrieve a DN Block Screen



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.

Table 3-33 describes the rules that the EPAP user interface uses to perform the Retrieve DN Block action. The table also describes other messages generated by the EPAP user interface while performing this action.

Table 3-33 Rules for Retrieve DN Block Screen

Syntax Rules	Error Code
The user must enter a valid DN.	E1002
The user must enter a valid SP.	E1002
The user must enter a valid RN.	E1002

Table 3-33 (Cont.) Rules for Retrieve DN Block Screen

Semantic Rules		Error Code
The user may enter a range of DNs.		None
The user may only enter an SP if G-Flex or G-Port is installed.		None
The user may only enter an RN if G-Port or INP is installed.		None
The type of output data to return may be entered only if a DN range is requested.		None
The maximum number of records to return may be entered only if a DN range is entered.		None
The PDBI must return a success status.		E1017
Other Messages		
Condition	Message Text	
No records were found.	Query returned no subscriptions.	

3.2.7.5.5 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 screen

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).

Figure 3-83 Add an NE Example

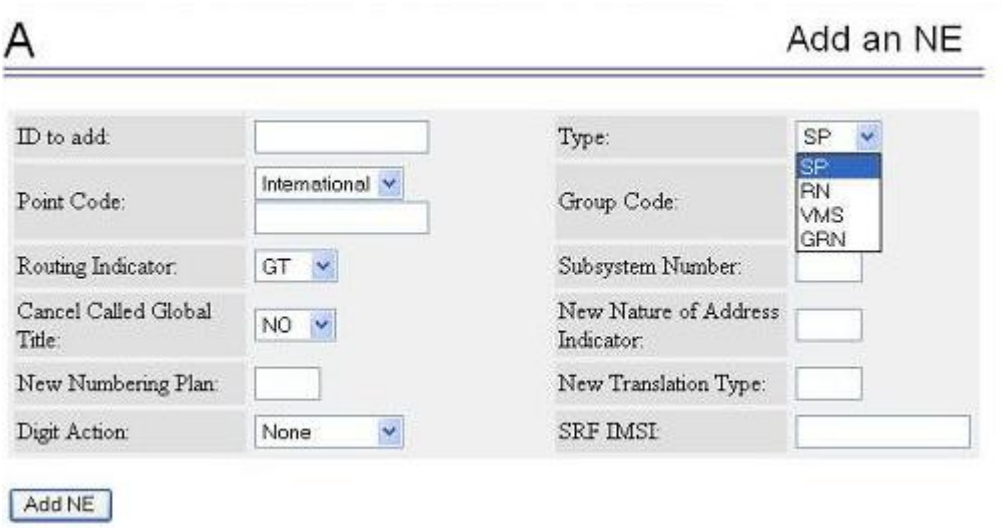


Table 3-34 describes the rules that the EPAP user interface uses to perform the Add Network Entity action. The table also describes other messages generated by the EPAP user interface while performing this action.

Table 3-34 Rules for Add Network Entity Screen

Syntax Rules		Error Code
The user must enter a valid entity **ID**.		E1002
The user must enter a valid **PC** (point code).		E1002
The user must enter a valid **SSN**.		E1002
Semantic Rules		Error Code
For **RNs**, entering a point code is optional.		None
If no point code is entered, no optional parameters can be specified.		None
Only one of the 3 point code types may be entered.		None
If the routing indicator is **GT**, Cancel Called Global Title must be set to **NO**.		None
If the routing indicator is GT, a digit action may be specified.		None
The **PDBI** must return a success status.		E1017
Other Messages		
Condition	Message Text	
The Network Entity was added.	Network Entity successfully added.	
The Network Entity was not added.	Network Entity not added.	

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).

Table 3-35 describes the rules that the EPAP user interface uses to perform the Modify Network Entity action. The table also describes other messages generated by the EPAP user interface while performing this action.

Table 3-35 Rules for Modify Network Entity Screen

Syntax Rules		Error Code
The user must enter a valid entity ID.		E1002
The user must enter a valid point code.		E1002
The user must enter a valid SSN.		E1002
Semantic Rules		Error Code
For RNs, entering a point code is optional.		None
If no point code is entered, no optional parameters can be specified.		None
Only one of the 3 point code types may be entered.		None
If the routing indicator is GT, Cancel Called Global Title must be set to **NO**.		None
If the routing indicator is GT, a digit action may be specified.		None
The PDBI must return a success status.		E1017
Other Messages		
Condition	Message Text	
The Network Entity was modified.	Network Entity successfully modified.	

Table 3-35 (Cont.) Rules for Modify Network Entity Screen

The Network Entity was not modified.	Network Entity not modified.

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).

Table 3-36 describes the rules that the EPAP user interface uses to perform the Delete Network Entity action. The table also describes other messages generated by the EPAP user interface while performing this action.

Table 3-36 Rules for Delete Network Entity Screen

Syntax Rules		Error Code
The user must enter a valid entity ID.		E1002
Semantic Rules		Error Code
The PDBI must return a success status.		E1017
Other Messages		
Condition	Message Text	
The Network Entity was deleted.	Network entity successfully deleted.	
The Network Entity was not deleted.	Network entity not deleted.	

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).

Figure 3-84 Retrieve an NE Example

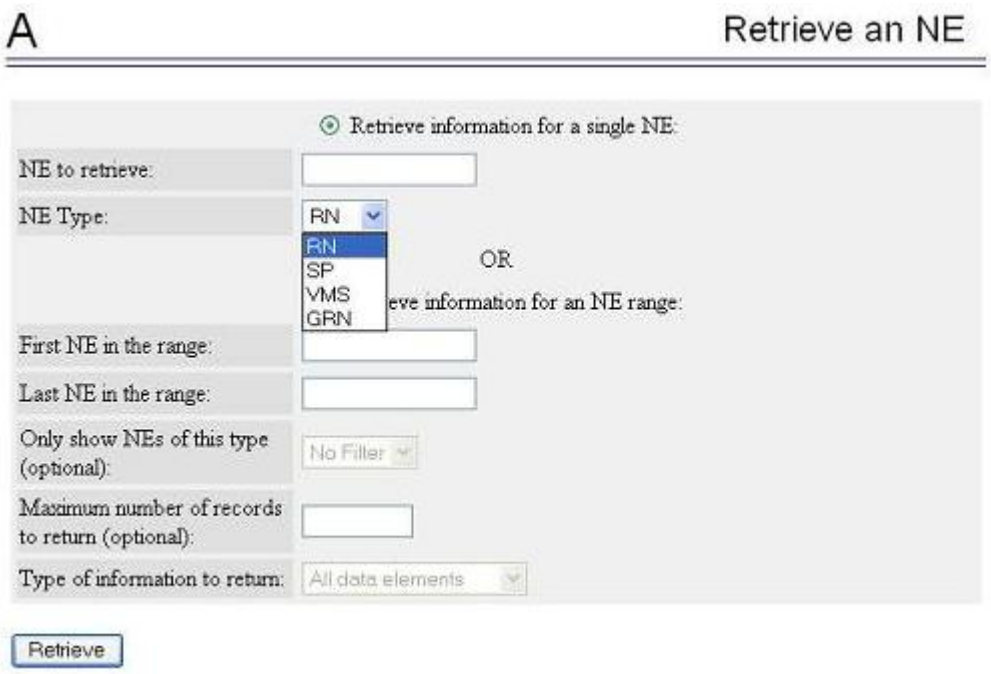


Table 3-37 describes the rules that the EPAP user interface uses to perform the Retrieve Network Entity action. The table also describes other messages generated by the EPAP user interface while performing this action.

Table 3-37 Rules for Retrieve Network Entity Screen

Syntax Rules		Error Code
The user must enter a valid entity ID.		E1002
Semantic Rules		Error Code
The type of output data to return may be entered only if a range of Network Entities is requested.		None
The maximum number of records to return may be entered only if a range of Network Entities is requested.		None
The PDBI must return a success status.		E1017
Other Messages		
Condition	Message Text	
No records were found.	Query returned no network entities.	

Table 3-38 describes the rules that the EPAP user interface uses to perform the Send Raw PDBI Commands action. The table also describes other messages generated by the EPAP user interface while performing this action.

Table 3-38 Rules for Enter Raw PDBI Commands Screen

Semantic Rules		Error Code
The user may enter 'quit' to return to the PDBA Manage Subscriptions Menu.		None
Other Messages		
Condition	Message Text	
A transaction ID was returned.	Transaction ID: <txid>	
A return code was returned. (It is displayed as a text mnemonic corresponding to an error number.)	Return code: <return code>	
Response data was returned. (This response includes all text within the data() portion of the command response.)	Response data: <response data>	

3.2.7.5.6 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

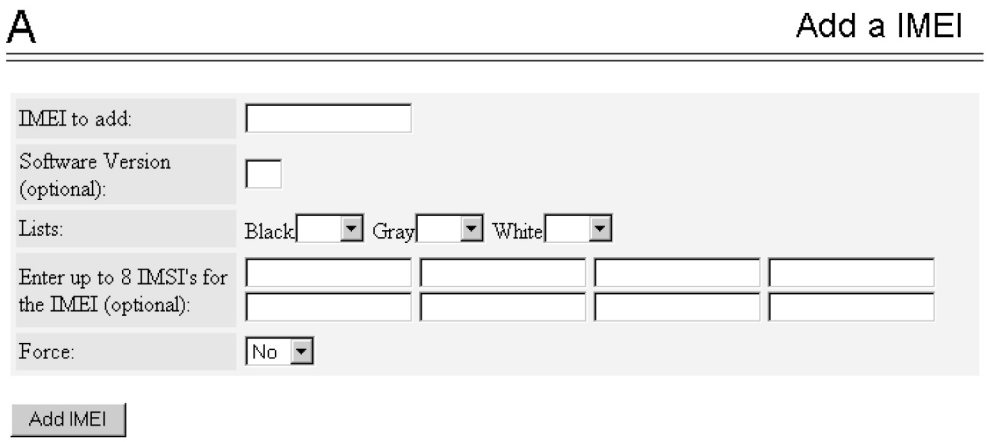
Add an IMEI

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 400 **IMSIs**. An IMEI and at least one List Type must be specified.
- Overwrite an existing IMEI. The IMEI and any other parameters and Force must be specified.
- Add a new IMSI to an existing IMEI. Existing IMEI and IMSI must be specified.

The **SVN** is an optional field. If no value is entered the default is 0. See Figure 3-85 for an example of the Add a IMEI screen.

Figure 3-85 Add an IMEI Screen



There are limited numbers of digit combinations in the first 9 digits of DN/IMSI/IMEI. In IMEI, the first 9 digits are Type Allocation Code (TAC), which must not exceed 250,000 combinations.

Table 3-39 describes the rules that the **EPAP** user interface uses to perform the Add IMSI action. The table also describes other messages generated by the EPAP user interface while performing this action.

Table 3-39 Rules for Add IMSI Screen

Syntax Rules	Error Code
The user must enter a valid SP.	E1002
The user must enter a valid IMSI.	E1002
The user must enter a valid DN.	E1002
Semantic Rules	Error Code
This menu option is valid only if the **G-Flex** feature is installed.	None
The SP must exist in the PDB.	E1014
The user may enter up to 8 DNs	None

Table 3-39 (Cont.) Rules for Add IMSI Screen

The user may elect to force the transaction to be entered into the PDB, even if there are conflicting subscriptions.	None
The PDBI must return a success status.	E1017
PDBI command `ent-sub`, on the creation of a single IMSI with or without DNs, supports a response "PDBI_MAX_IMSI9DIG_LIMIT" if the to-be provisioned IMSI causes the first 9 digits go above its max limit of 65,000.	E1066
"PDBI_MAX_IMEI9DIG_LIMIT" if to-be provisioned IMEI causes the first 9 digits to go above its max limit of 250,000.	E1067
Other Messages	
Condition	Message Text
The new subscription already exists in the PDB.	This subscription conflicts with an existing subscription.
The new subscription was attempting to overwrite an existing IMSI.	IMSI <imsi> already exists in the PDB. If you choose to overwrite the existing subscription, all data associated with the existing IMSI will be lost. All DNs associated with the existing IMSI will be deleted.
The subscription was added.	Subscription successfully added.
The subscription was not added.	Subscription not added.

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.

Table 3-40 describes the rules that the EPAP user interface uses to perform the Update IMSI action. The table also describes other messages generated by the EPAP user interface while performing this action.

Table 3-40 Rules for Update IMEI Screen

Syntax Rules	Error Code
The user must enter a valid SP.	E1002
The user must enter a valid IMSI.	E1002
Semantic Rules	Error Code
This menu option is valid only if the G-Flex feature is installed.	None
The IMEI must exist in the PDB.	E1015
The SP must exist in the PDB.	E1014
The PDBI must return a success status.	E1017
Other Messages	

Table 3-40 (Cont.) Rules for Update IMEI Screen

Condition	Message Text
The subscription was modified.	Subscription successfully modified.
The subscription was not modified.	Subscription not modified.

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.

Table 3-41 describes the rules that the EPAP user interface uses to perform the Delete IMSI action. The table also describes other messages generated by the EPAP user interface while performing this action.

Table 3-41 Rules for Delete IMSI Screen

Syntax Rules		Error Code
The user must enter a valid IMSI.		E1002
Semantic Rules		Error Code
This menu option is valid only if the G-Flex feature is installed.		None
The subscription must exist in the PDB.		E1012
The PDBI must return a success status.		E1017
Other Messages		
Condition	Message Text	
The subscription was deleted.	Subscription successfully deleted.	
The subscription was not deleted.	Subscription not deleted.	

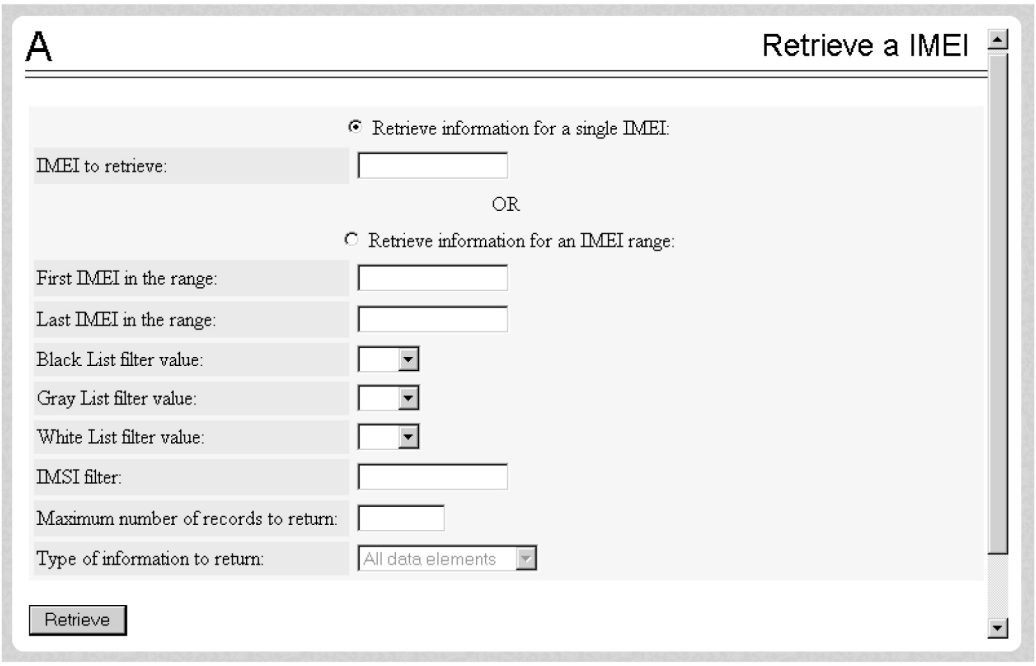
Retrieve an IMEI

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 400 IMSIs. The IMEI must be specified. Once IMSIs are added as part of the add IMEI option, the user will be allowed to add up to 400 IMSIs per IMEI using PDBI commands or import scripts, with no more than 8 IMSIs to be added per command.
- 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 3-86 for an example of the Retrieve a IMEI screen.

Figure 3-86 Retrieve an IMEI Screen



3.2.7.5.7 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.

Table 3-42 describes the rules that the EPAP user interface uses to perform the Add IMSI action. The table also describes other messages generated by the EPAP user interface while performing this action.

Table 3-42 Rules for Add IMSI Screen

Syntax Rules	Error Code
The user must enter a valid SP.	E1002
The user must enter a valid IMSI.	E1002
The user must enter a valid DN.	E1002

Table 3-42 (Cont.) Rules for Add IMSI Screen

Semantic Rules		Error Code
This menu option is valid only if the **G-Flex** feature is installed.		None
The SP must exist in the PDB.		E1014
The user may enter up to 8 DNs		None
The user may elect to force the transaction to be entered into the PDB, even if there are conflicting subscriptions.		None
The PDBI must return a success status.		E1017
Other Messages		
Condition	Message Text	
The new subscription already exists in the PDB.	This subscription conflicts with an existing subscription.	
The new subscription was attempting to overwrite an existing IMSI.	IMSI <imsi> already exists in the PDB. If you choose to overwrite the existing subscription, all data associated with the existing IMSI will be lost. All DNs associated with the existing IMSI will be deleted.	
The subscription was added.	Subscription successfully added.	
The subscription was not added.	Subscription not added.	

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.

Table 3-43 describes the rules that the EPAP user interface uses to perform the Update IMSI action. The table also describes other messages generated by the EPAP user interface while performing this action.

Table 3-43 Rules for Update IMSI Screen

Syntax Rules		Error Code
The user must enter a valid SP.		E1002
The user must enter a valid IMSI.		E1002
Semantic Rules		Error Code
This menu option is valid only if the G-Flex feature is installed.		None
The IMSI must exist in the PDB.		E1015
The SP must exist in the PDB.		E1014
The PDBI must return a success status.		E1017
Other Messages		
Condition	Message Text	
The subscription was modified.	Subscription successfully modified.	
The subscription was not modified.	Subscription not modified.	

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.

Table 3-44 describes the rules that the EPAP user interface uses to perform the Delete IMSI action. The table also describes other messages generated by the EPAP user interface while performing this action.

Table 3-44 Rules for Delete IMSI Screen

Syntax Rules		Error Code
The user must enter a valid IMSI.		E1002
Semantic Rules		Error Code
This menu option is valid only if the G-Flex feature is installed.		None
The subscription must exist in the PDB.		E1012
The PDBI must return a success status.		E1017
Other Messages		
Condition	Message Text	
The subscription was deleted.	Subscription successfully deleted.	
The subscription was not deleted.	Subscription not deleted.	

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:

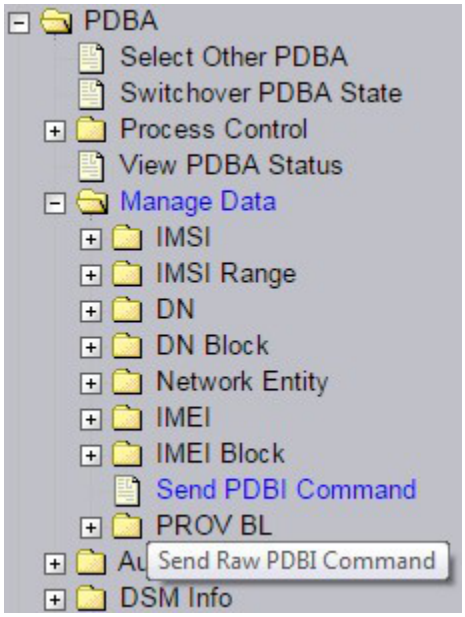
3.2.7.5.8 Send PDBI Command

The **PDBA** / Manage Data / Send **PDBI** Command screen allows only the `epapdev` user to type PDBI (**Provisioning Database Interface**) commands that are not explicitly covered by the menu set. This uses WebStart Java technology, which works independent of the web browser once it is launched. The dynamic JNLP files are used to launch the WebStart application. The Send 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 *Provisioning Database Interface User's Guide*.

1. Log in to the EPAP GUI.
2. Select **PDBA**, and then **Manage Data**, and then **Send PDBI Command**, as displayed in Figure 3-87:

Figure 3-87 Send PDBI Command on the EPAP GUI Menu



3. Select **Launch the JCTerm application**:

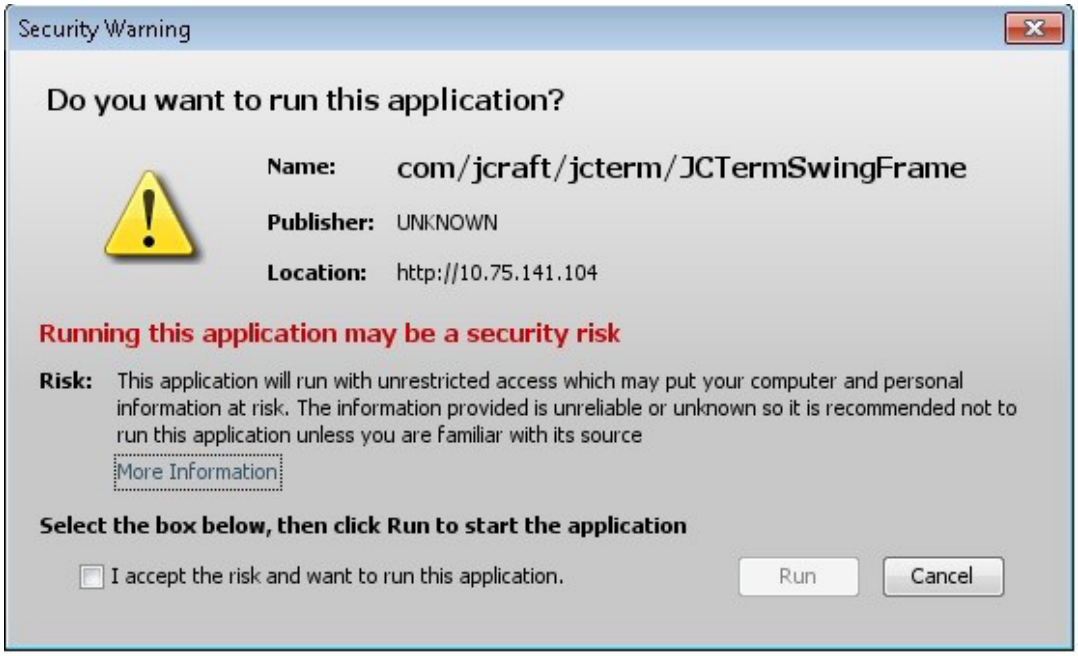
Figure 3-88 JCTerm Application Launch Window

The following screen will appear:

Figure 3-89 Launching WebStart

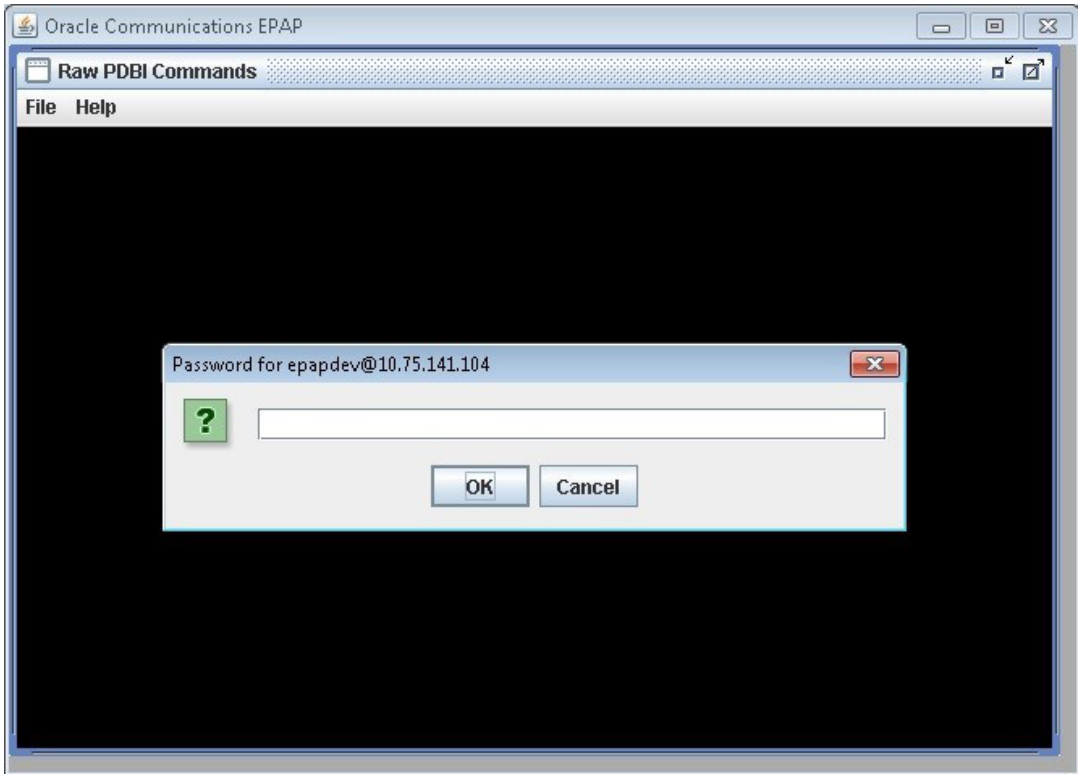
4. The JCTerm jar, along with the `Jzlib jar` and `Jsch jar`, are self-signed. Accept the security check that follows and select **Run** to launch the JCTerm applet for the SSH to MPS interface:

Figure 3-90 JCTerm Security Check Window



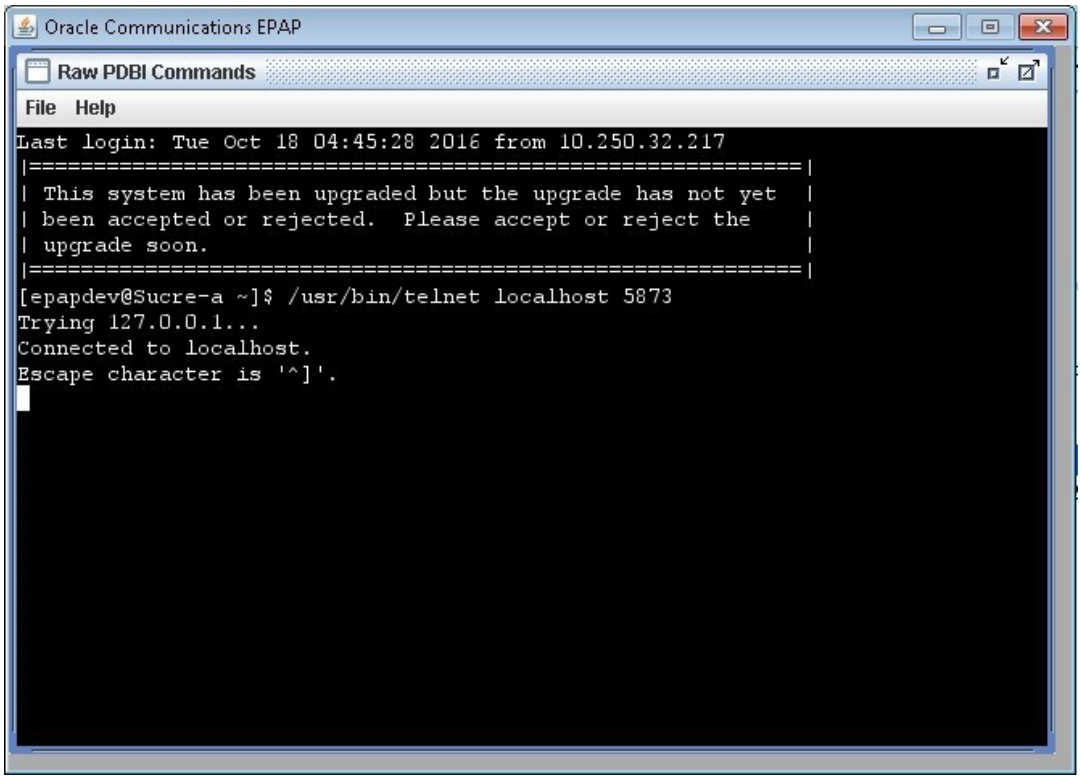
5. The Send PDBI Command window will be displayed, as show in the following figure:

Figure 3-91 Send PDBI Command Log in Window



The epapdev password is required. Select OK to gain access to the Send PDBI Command interface. After a valid epapdev password is entered, the user will be directed to an interface, as shown in the following figure:

Figure 3-92 Send PDBI Command Interface



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 *Provisioning Database Interface User's Guide* for the rules about commands, syntax, and usages.

3.2.7.5.9 EPAP Provisioning Blocklist Menu

The **PDBA** / Manage Data / Prov BL menu is used to add, delete, and view blocklist entries in the Provisioning Database (**PDB**).

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

- Add Provisioning Blocklist
- Delete Provisioning Blocklist
- Retrieve Provisioning Blocklist

Add Provisioning Blocklist

The PDBA / Manage Data / Prov BL /Add **Provisioning Blocklist** screen is used to add **Blocklist** 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 blocklist 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 blocklist value and ending blocklist value must be of the same length.
- The address strings cannot conflict with DN, DN block, or IMSI values in the PDB.

Tekelec recommends adding Network Global Titles in the EPAP Provisioning Blocklist to prevent Network Global Titles from being provisioned in the MNP Database.

Delete Provisioning Blocklist

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

Retrieve Provisioning Blocklist

The PDBA / Manage Data / Prov BL /Retrieve Provisioning Blocklist screen is used to retrieve blocklist 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.

3.2.7.6 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**). Beginning with EPAP 16.1, the user is able to configure both IPv4 and IPv6 for a list of authorized IPs:

- The user is allowed to configure IPv4 only remote system address
- The user is allowed to configure IPv6 only remote system address
- On dual stack - the user is allowed to configure IPv4 or IPv6 remote system address

This menu also allows you specify whether a secure shell (SSH) tunnel should be created between the that IP address and the EPAP, and if so, specify the username, password and port number to use on the machine represented by the IP address.For more information about SSH tunneling, refer to *Provisioning Database Interface User's Guide*. 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

Figure 3-93 Add Authorized PDBA Client IP

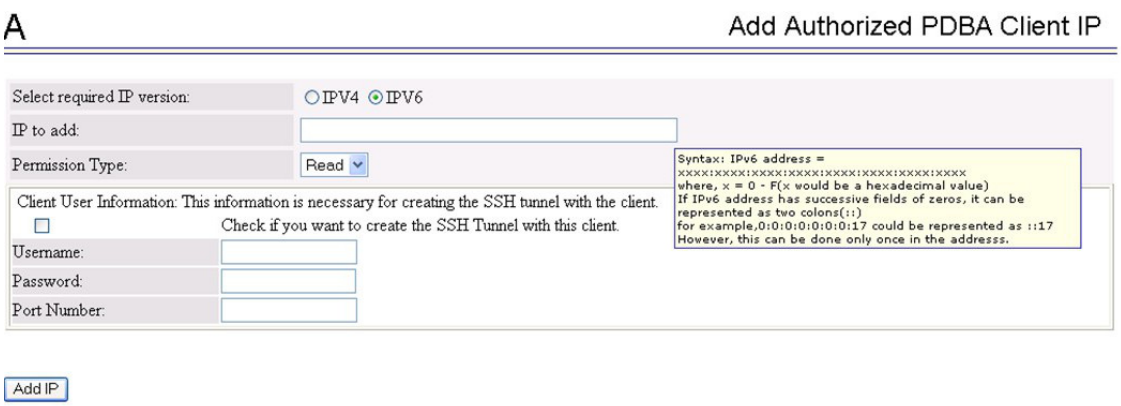


Table 3-45 describes the rules that the EPAP user interface uses to perform the Add Authorized PDBA Client IP action. The table also describes other messages generated by the EPAP user interface while performing this action.

Table 3-45 Rules for Add Authorized PDBA Client IP

Syntax Rules		**Error Code**
The user must enter a valid IP address.		E1002
Other Messages		
Condition	Message Text	
An address with read-only access was added.	IP address xxx.xxx.xxx.xxx is authorized for READ access.	
An address with read-write access was added.	IP address xxx.xxx.xxx.xxx is authorized for READ/WRITE access.	

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

Figure 3-94 Modify Authorized PDBA Client IP

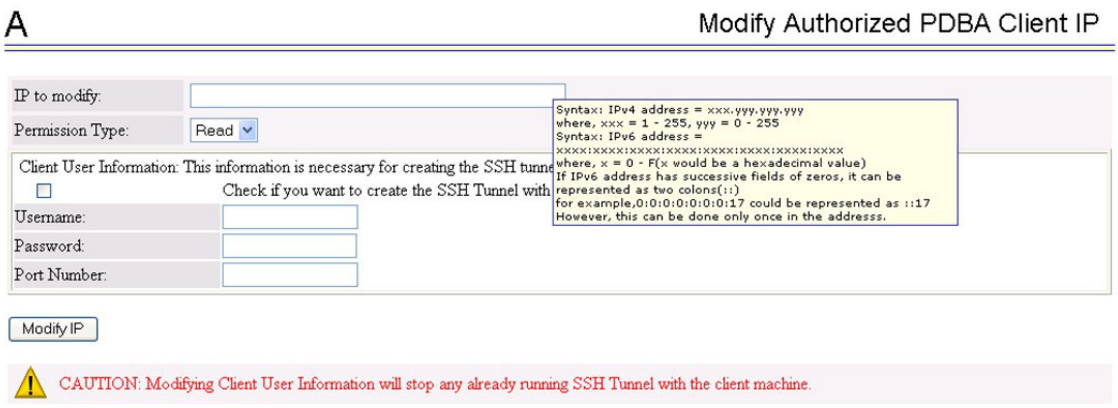


Table 3-46 describes the rules that the EPAP user interface uses to perform the Add Authorized PDBA Client IP action. The table also describes other messages generated by the EPAP user interface while performing this action.

Table 3-46 Rules for Add Authorized PDBA Client IP

Syntax Rules	Error Code
The user must enter a valid IP address.	E1002
Other Messages	
Condition	Message Text
An address with read-only access was added.	IP address xxx.xxx.xxx.xxx is authorized for READ access.
An address with read-write access was added.	IP address xxx.xxx.xxx.xxx is authorized for READ/WRITE access.

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.

Table 3-47 describes the rules that the EPAP user interface uses to perform the Modify Authorized PDBA Client IP action. The table also describes other messages generated by the EPAP user interface while performing this action.

Table 3-47 Rules for Modify Authorized PDBA Client IP Screen

Syntax Rules	Error Code
The user must enter a valid IP address.	E1002
Semantic Rules	Error Code

Table 3-47 (Cont.) Rules for Modify Authorized PDBA Client IP Screen

The IP address must be in the authorized IP address list.	E1021
Other Messages	
Condition	Message Text
Permission downgraded to read-only.	IP address xxx.xxx.xxx.xxx is authorized for **READ** access.
Permission upgraded to read-write.	IP address xxx.xxx.xxx.xxx is authorized for READ/ **WRITE** access.

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.

Figure 3-95 Remove Authorized PDBA Client IP

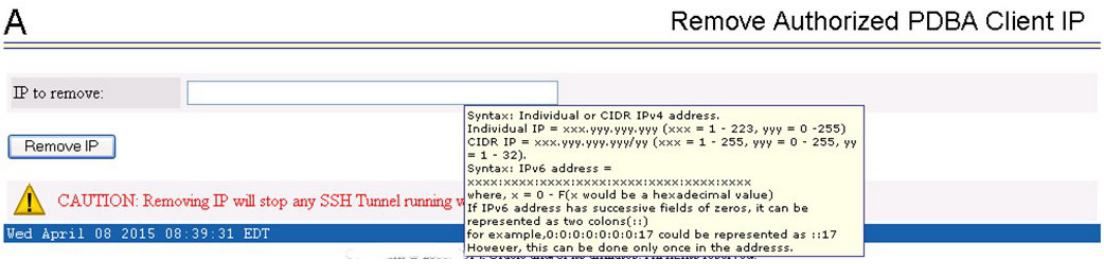


Table 3-48 describes the rules that the EPAP user interface uses to perform the Add Authorized PDBA Client IP action. The table also describes other messages generated by the EPAP user interface while performing this action.

Table 3-48 Rules for Add Authorized PDBA Client IP

Syntax Rules	**Error Code**
The user must enter a valid IP address.	E1002
Other Messages	
Condition	Message Text
An address with read-only access was added.	IP address xxx.xxx.xxx.xxx is authorized for READ access.
An address with read-write access was added.	IP address xxx.xxx.xxx.xxx is authorized for READ/ WRITE access.

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.

Table 3-49 describes the rules that the EPAP user interface uses to perform the Remove Authorized PDBA Client IP action. The table also describes other messages generated by the EPAP user interface while performing this action.

Table 3-49 Rules for Remove Authorized PDBA Client IP Screen

Syntax Rules		Error Code
The user must enter a valid IP address.		E1002
Semantic Rules		Error Code
The IP address must be in the authorized IP address list.		E1021
Other Messages		
Condition	Message Text	
An address was removed.	IP address xxx.xxx.xxx.xxx is removed from the authorized IP address list.	

List All Authorized IPs

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

Figure 3-96 List All Authorized PDBA Client IPs Screen

Table 3-50 describes the rules that the EPAP user interface uses to perform the List All Authorized PDBA Client IPs action. The table also describes other messages generated by the EPAP user interface while performing this action.

Table 3-50 Rules for List All Authorized PDBA Client IPs Screen

Other Messages	
Condition	Message Text
The authorized IP address list is empty.	There are no authorized IP addresses.

3.2.7.7 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:

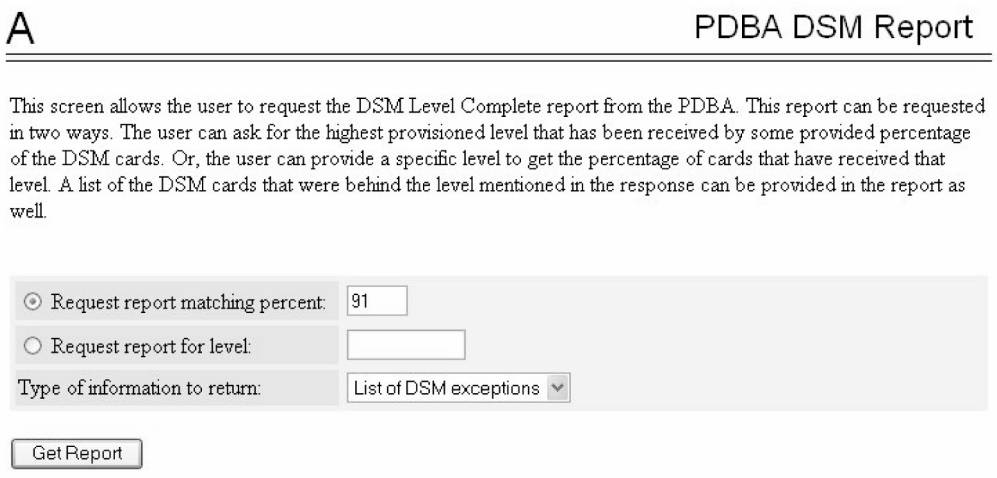
- PDBA DSM Report
- PDBA DSM List

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 3-97 for the PDBA DSM Report screen.

Figure 3-97 PDBA DSM Report Screen



PDBA DSM List

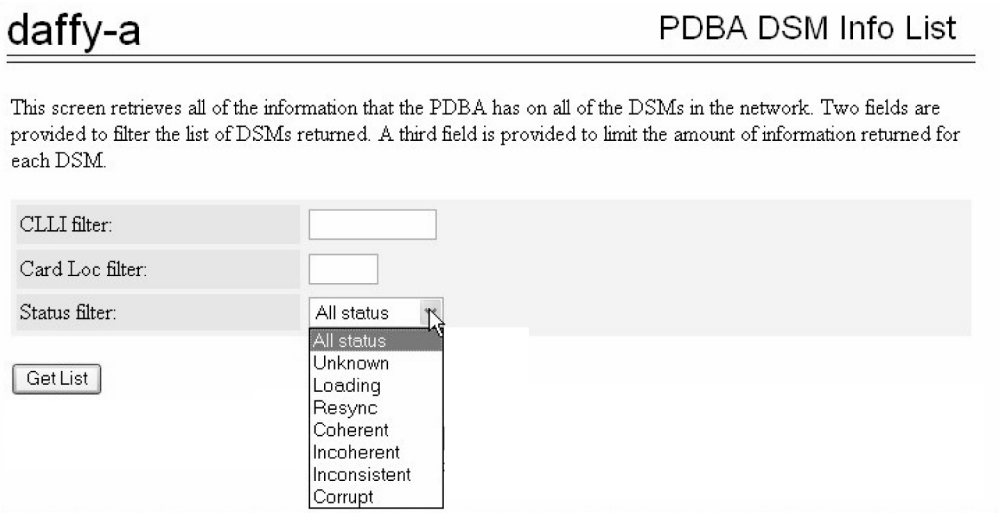
Table 3-51 describes the rules that the EPAP user interface uses to perform the Add Authorized PDBA Client **IP** action. The table also describes other messages generated by the EPAP user interface while performing this action.

Table 3-51 Rules for Add Authorized PDBA Client IP

Syntax Rules		**Error Code**
The user must enter a valid IP address.		E1002
Other Messages		
Condition	Message Text	
An address with read-only access was added.	IP address xxx.xxx.xxx.xxx is authorized for **READ** access.	
An address with read-write access was added.	IP address xxx.xxx.xxx.xxx is authorized for READ/ **WRITE** access.	

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 3-98 for an example of the PDBA DSM Info List.

Figure 3-98 PDBA DSM Info List Screen (with Status filter pulldown)



3.2.7.8 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:

- Backup Menu
- Import File to PDB screen
- Export PDB to File screen
- Transaction Log Params
- Number Prefixes
- Logs menu
- Schedule Export
- Configure PDBA Record Delay
- PDBA / Maintenance / View License Capacity

3.2.7.8.1 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.

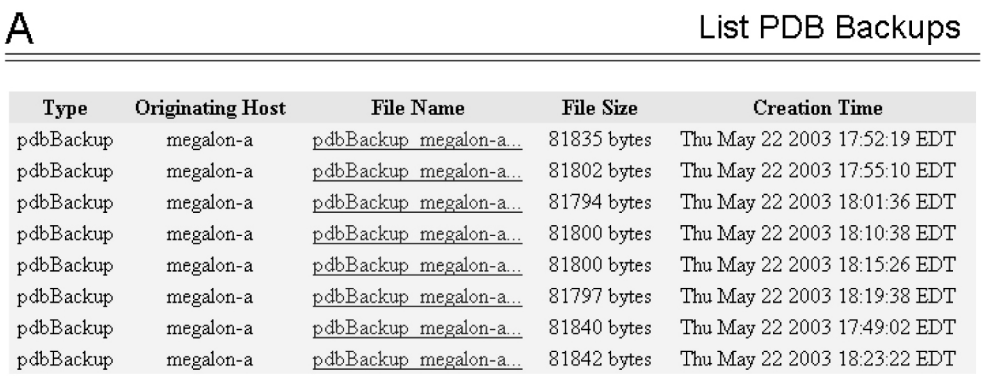
The PDBA / Maintenance / Backup menu provides these actions:

- List Backups screen
- Backup the PDB screen
- Restore the PDB screen

List Backups

The PDBA / Maintenance / Backup / List PDB Backups screen lists the details of the backup. See Figure 3-99 for an example of the List PDB Backups screen.

Figure 3-99 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.

PDB Backup Successful Banner Message Table 3-52 gives the EPAP user interface rules for performing the Backup the PDB. The table also lists other messages generated by the EPAP user interface while performing this action.

> **Note:**
>
> PDB only maintains a single copy of backup file. If the backup file is already present, the **PDB Backup already exists in free directory error message** is displayed. Therefore it is required to transfer PDB backup file to remote server using Configure File Transfer as described in section Configure File Transfer or manually by using sftp.

Table 3-52 Rules for Backup the PDB Screen

Semantic Rules		Error Code
The device must exist.		E1019
Other Messages		
Condition	Message Text	
Backup started.	Backup in progress. The backup will take approximately 35 minutes. You will be notified when the backup is complete.	
Backup did not start.	Backup failed.	
Backup complete.	PDB backup complete.	

Restore the PDB

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 *Alarms and Maintenance Guide*.

> **Caution:**
>
> Do not attempt to use this operation until you have contacted My Oracle 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.

3.2.7.8.2 PDBA / Maintenance / Import File to PDB

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

> **Note:**
>
> Do not use this action to restore a damaged Provisioning Database. 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 My Oracle Support for information and assistance.

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.

Table 3-53 describes the rules that the EPAP user interface uses to perform the Import File to PDB action. The table also describes other messages generated by the EPAP user interface while performing this action.

Table 3-53 Rules for Import File to PDB Screen

Semantic Rules		Error Code
The import file must exist.		E1008
Other Messages		
Condition	Message Text	
User cancelled the import.	Import aborted.	
Import started.	Import in progress. The import will take approximately 5 minutes. You will be notified when the import is complete.	
Import did not start.	Import failed	
Import complete.	PDB import complete.	

For additional information on Importing Files to the Provisioning Database (PDB), refer to the *Provisioning Database Interface User's Guide* section about importing and exporting files.

3.2.7.8.3 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 Provisioning Database (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 User's Guide* section titled "PDBI Format."

> **Note:**
>
> Do not use this action as a substitute for the Backup the PDB action. Do not use a file generated by the Export PDB to File action to restore a damaged database. Use this action only as 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>`.

To export a PDB to File, click the **Continue** button.

In the input field titled *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 ASCII, select a delimiter from the drop-down menu. After making the selections, click the **Export** button.

The path to your copy of the exported file is 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 User's Guide* sections "PDBI Format" and "Raw Delimited ASCII Format."

Table 3-54 describes the rules with which the EPAP user interface performs the Export File from PDB action. The table also describes other messages generated by the EPAP user interface while performing this action.

Table 3-54 Rules for Export File from PDB Screen

Semantic Rules		Error Code
The import file must exist and be writable.		E1008
Other Messages		
Condition	Message Text	
Export started.	Export in progress. The export will take approximately 25 minutes. You will be notified when the export is complete.	
Export did not start.	Export failed	
Export complete.	PDB export complete.	

For additional information about Importing Files to the PDB, refer to the *Provisioning Database Interface User's Guide* section titled "Import/Export Files."

3.2.7.8.4 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 Transaction Log Parameters
- Change Transaction Log Parameters

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.

3.2.7.8.5 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 *Provisioning Database Interface User's Guide* .

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

- View Number Prefixes
- Change Number 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 number prefixes, refer to *Provisioning Database Interface User's Guide*.

Enter either the DN or DN block prefix and/or the IMSI prefix. After entering the values, click the **Change Prefixes** button.

3.2.7.8.6 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 My Oracle Support in diagnosing system operation and problems. If assistance is required, contact My Oracle Support for more information.

The PDBA / Maintenance / Logs menu provides these actions:

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

Logs under the Maintenance option include the following options:

- Command Log - pdba.cmd
- Debug Log - pdba.dbg
- Error Log - pdba.err

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 .

Table 3-55 describes the rules that the EPAP user interface uses to perform the View PDBA Command Log action.

Table 3-55 Rules for View PDBA Command Log

Semantic Rules	Error Code
The log file must exist.	E1008

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 .

Table 3-56 describes the rules that the EPAP user interface uses to perform the View PDBA Debug Log action.

Table 3-56 Rules for View PDBA Debug Log

Semantic Rules	Error Code
The log file must exist.	E1008

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 .

Table 3-57 describes the rules that the EPAP user interface uses to perform the View PDBA Error Log action.

Table 3-57 Rules for View PDBA Error Log

Semantic Rules	Error Code
The log file must exist.	E1008

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 My Oracle Support for more information.

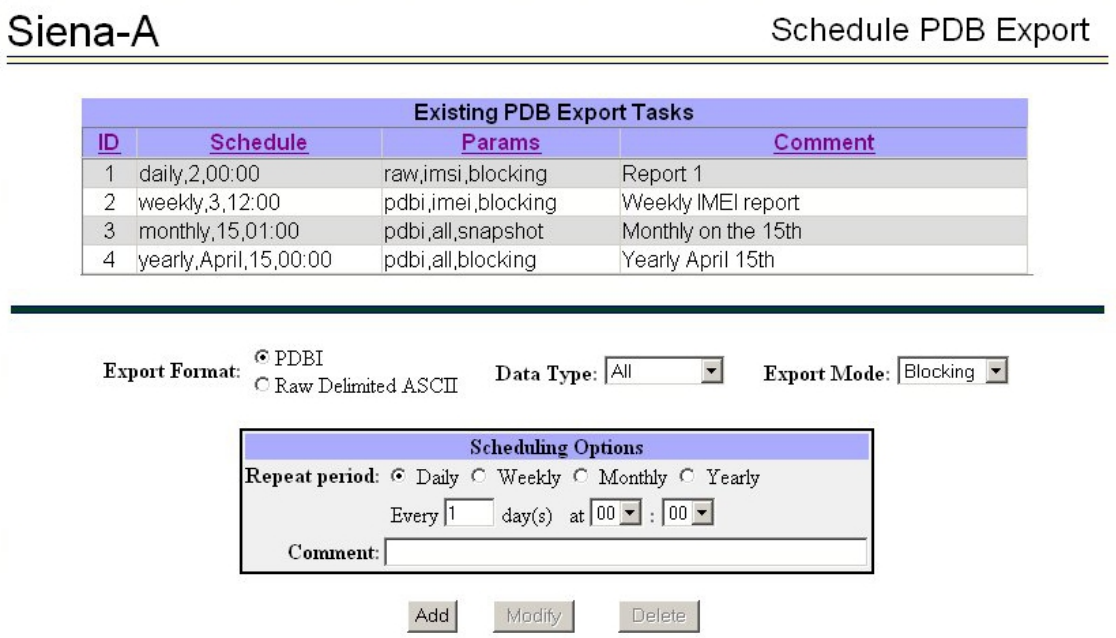
3.2.7.8.7 PDBA / Maintenance / Schedule PDB Export

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

The export can be scheduled at a specific time for each of the following repeat periods: every N number of days (N can be up to 365) on 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 3-100 Schedule PDB Export Example



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 *Provisioning Database Interface User's Guide*.

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.

3.2.7.8.8 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.

3.2.7.8.9 PDBA / Maintenance / View License Capacity

This screen displays information about the purchased Provisioning Database (PDB) capacity license supported on a specific EPAP. The total Purchased DB License Capacity and the percentage of PDB occupation are displayed. Licenses are applied in increments of 0.5 Million; a customer who purchases 20 licenses has a Provisioning Database capacity of 10 million subscribers.

The 80%, 90%, and 100% capacity alarms are based on the licensed capacity if configured. Before the 240M DN and 240M IMSIs via Split Database feature is turned on from the EAGLE side, these alarms are based on a total capacity of 240 million. After the 240M DN and 240M IMSIs via Split Database feature is turned on from the EAGLE side, these alarms are based on a total capacity of 480 million by default or based on the purchased capacity if configured.

Incremental Capacity Control

As of EPAP 16.1, a Feature Access Key (FAK) is no longer required to enable or use the EPAP Capacity Control feature. Operators are responsible for ensuring their system stays within the scope of the licenses they have purchased. Because the License Capacity is updated incrementally, whenever a new capacity is added, it will be added in addition to the previous capacity.

By default, the license capacity is set to 0 (not configured). A PDB percentage full alarm is raised when the capacity is not set.

The utility `manageLicenseInfo` is used to check and set DB license capacity. To check and set the value of purchased license capacity, complete the following steps:

1. Log on to the EPAP CLI as `epapdev`.
2. `$ manageLicenseInfo -l`

> **Note:**
>
> The value of the purchased capacity is mentioned in "Current license capacity."

3. `$ manageLicenseInfo -a <License Capacity value>`

> **Note:**
>
> "License Capacity value" is the number of licenses required to set desired PDB capacity.

The utility is available on the EPAP Provisional server. The "License Capacity value" is stored in `LicenseInfo` table in PDB database.

3.2.7.9 List PDBI Connections

The PDBA / List PDBI Connections screen enables EPAP GUI users to view all provisioning connections to the PDBA. This menu option provides non-persistent data about PDBI and SOG connections along with some performance data based on the totals for the entire lifetime of each connection.

3.2.7.10 PDBI Statistics Report

The PDBA / PDBI Statistics Report screen enables EPAP GUI users to view available statistics reports. After clicking the PDBI Statistics Report menu item, a screen is displayed to select the Report Type and identify the time period for the report.

Available Report Types are:

- 5 minutes
- 1 hour
- 1 day

Click on the **Generate Report** button to display the report.

The reports are stated in commands per second (CPS). Reported statistics include information on provisioning patterns, degradation of performance, and performance impact due to various activities.Reports generted for a specified time period (Report Type) contain at least the following information:

- Average number of PDBI connections for the reported period
- Peak number of PDBI connections for the reported period
- Average system PDBI commands per second (CPS) for the reported period
- Peak system PDBI commands per second (CPS) for the reported period (calculated per second)
- Percentage of commands with a return code of zero that successfully updated the database for the reported period (`ent/upd/dlt` commands only).
- Total number of commands with a return code of zero that successfully updated the database for the reported period (`ent/upd/dlt` commands only; `rtrv` commands are not included).

Statistics related to numbers of PDBI connections are based on the number of PDBI connections at one time.

3.2.8 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.
- MultipleSessions perUser: 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.
- ManageUnusedUserIDs: 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.
- RevokeFailed 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

3.2.8.1 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 3-58 for the current login names.

Table 3-58 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.

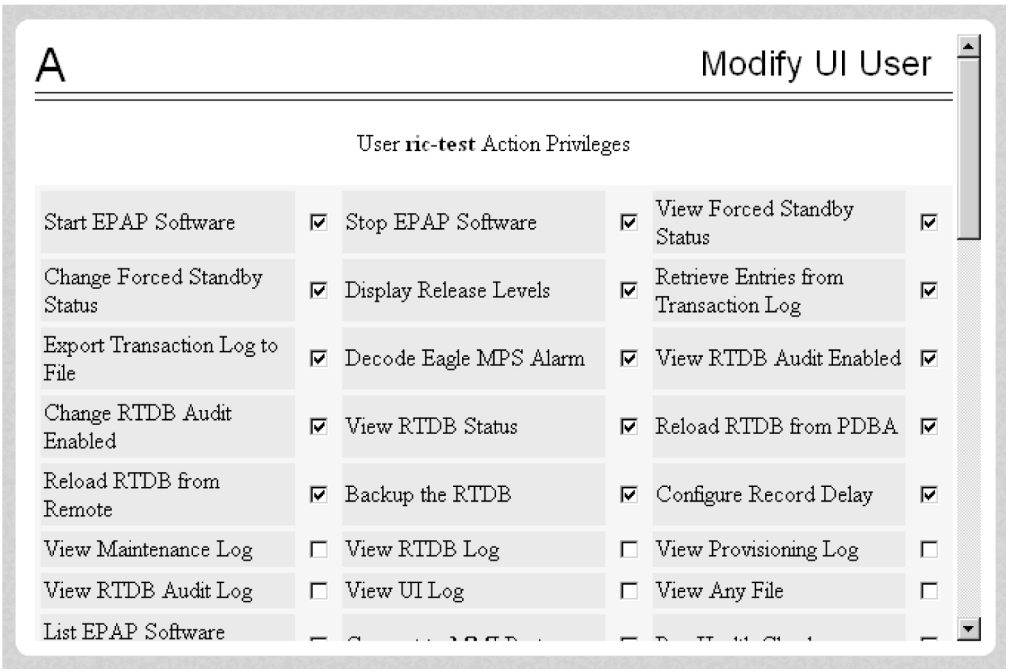
After selecting a User Name, the user permissions screen appears. In this screen, the permissions allowed to the user can viewed and specified.

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 3-101.

Figure 3-101 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.

3.2.8.2 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.

3.2.8.3 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. Beginning with EPAP 16.1, the user is able to add/ remove both IPv4 and IPv6 addresses.

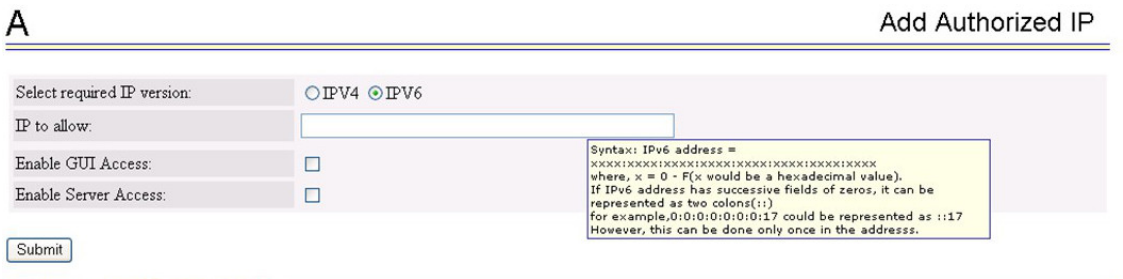
The User Administration / Authorized IP List menu provides these actions:

- Add Authorized UI IP
- Remove Authorized UI IP
- List All Authorized UI 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.

Figure 3-102 Add Authorized IP



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.

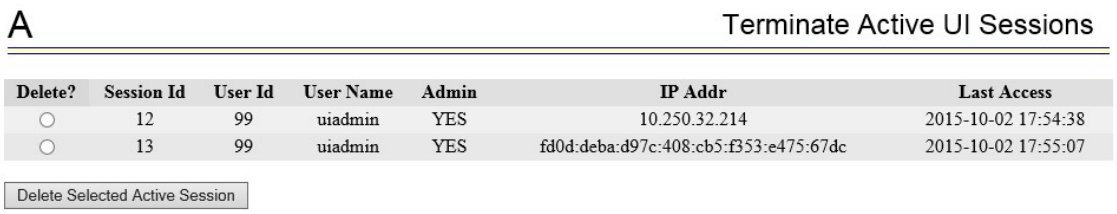
The enforcement of the checking for authorization status is immediate. The IP address of every message of every IP device using the GUI is checked as soon as the authorization status is enabled. The checking for authorized IPs does not occur only when devices log in.

3.2.8.4 Terminate UI Sessions

The User Administration / Terminate Active **UI** Sessions screen allows the administrator to selectively close individual active sessions. The **Terminate UI Sessions** menu option displays the active sessions with the client IP format same as the IP format used as URL to access the EPAP GUI.

The following figure shows the EPAP is configured in dual stack configuration and two EPAP GUI sessions have been opened, one using the IPv4 prov IP and other using the IPv6 prov IP. The client IP address is IPv4 for the IPv4 prov EPAP GUI session and IPv6 for the IPv6 prov EPAP GUI session.

Figure 3-103 Terminate Active UI Sessions



3.2.8.5 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.

3.2.9 Change Password

The Change Password screen provides **EPAP** users the capability to change their password. This basic action is available to all users and is accessible from the main menu (Figure 3-25).

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.

> **Note:**
>
> Unix account passwords cannot contain the `@` or `#` characters.

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.

3.2.10 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 3-25).

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.

4

Messages, Alarms, and Status Processing

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

4.1 EPAP Messages

This section includes Table 4-1. For alarm-related banner messages that appear on the UI browser screen in the Message Box described in EPAP GUI Main Screen. Refer to *Alarms and Maintenance Guide* for alarm recovery procedures.

EPAP Error Messages

Table 4-1 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 4-1 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*>
E1009	Active **PDBA** is not available.
E1010	This host is not an EPAP.
E1011	Cannot find EPAP <*A*|*B*> (host name <*host name*>)
E1012	Subscription (**SP**= <*subscription number*>) does not exist.
E1013	Subscription (SP= <*subscription number*>) already exists.
E1014	SP <*identifier*> does not exist.
E1015	**IMSI** <*identifier*> does not exist.
E1016	**DN** <*identifier*> does not exist.
E1017	**PDBI** error: <*error text*>
E1018	DN <*identifier*> already associated with IMSI <*identifier*>.
E1019	Device <*device*> unavailable.
E1020	Remote PDB unavailable.
E1021	IP address <*address*> is not authorized for PDB access.

Table 4-1 (Cont.) EPAP Error Messages

E1022	**RN** <*identifier*> does not exist.
E1023	Invalid value for <*prompt >: <value*>: Valid values are <*range*>. Hit the Escape key to abort the command.
E1024	**MTSU** error: <*error text*>
E1025	File lock failed: <*file name*>
E1026	Environment variable <*variable name*> not defined.
E1027	ssh error: <*error text*>
E1028	IP address <*IP address*> is already authorized for PDBI access.
E1029	IP address <*IP address*> is not authorized for PDBI access.
E1030	Operation timed out waiting for a response from the PDBA.
E1031	Operation timed out waiting for a response from the RTDB.
E1032	Operation aborted by user.
E1033	Unexpected response received from the PDBA: id=<*txid*>, return code=<*return code*>
E1034	Unexpected response received from the RTDB: id=<*txid*>, return code=<*return code*>
E1035	Script <*script name*> failed: status=<*status*>
E1036	EPAP configuration failed. Please use the configuration menu to manually configure the EPAP sync and **DSM** networks.
E1037	One or more EPAP software processes did not start
E1038	One or more EPAP software processes did not stop
E1039	Transaction log query failed: <*error text*>
E1040	Transaction log response file was not created.
E1041	Transaction log response file could not be parsed.
E1042	Transaction log export failed: <*error text*>
E1043	The specified EPAP was not available.
E1044	Remote EPAP software is running. You must stop the remote EPAP software before performing this operation.
E1045	RTDB copy operation failed.
E1046	Improperly encoded alarm string. Re-check source.
E1047	RTDB did not respond to query.
E1048	Invalid response received from RTDB.
E1049	Could not connect to <*device or process*>: <*error text*>
E1050	Secure shell **daemon** is not running on mate EPAP. Config files could not be synchronized !!!
E1051	No feature(s) specified.
E1052	Both **ELAP** and EPAP features specified.
E1053	This action may only be performed on the local EPAP.
E1054	Another user is currently performing this same action.
E1055	Missing mandatory parameter: <*parameter*>
E1056	Unexpected parameter was provided:<*parameter*>
E1057	The EPAP must be in Forced Standby mode for this operation.
E1058	An internal error in the <*parameter*> occurred: <*error text*>
E1059	The passwords did not match.

Table 4-1 (Cont.) EPAP Error Messages

E1060	The provisioning addresses for **MPS** A and B must be different.
E1061	The provisioning addresses for MPS A and B must be on the same network.
E1062	The default router must be on the same network as MPS A and MPS B.
E1063	The local and remote PDB addresses must be different.
E1064	This action may only be performed on EPAP A.
E1065	<*device or process*> must be configured.
E1066	The requested user <*user*> was not found.
E1067	The requested group <*group*> was not found.
E1068	The password entered was not correct.
E1069	The new password has been used too recently.
E1070	The provided password does not meet the security requirements. Reason: <*reason text*>
E1071	The specified group already exists.
E1072	This action may only be performed on EPAP B.
E1073	The file you have attempted to upload is larger than the <number> bytes of allocated storage space.
E1074	**LPU** batch failure: <*error text*>
E1075	This action must be done on the Active PDBA.
E1077	File system violation: <*error text*>
E1078	File '<*file name*>' was empty.
E1079	There are no PDBI connections available. Try again later.
E1080	The provisioning addresses for the main and backup networks must be different.
E1081	The specified IP already exists.
E1082	The specified IP does not exist.
E1083	The maximum number of authorized UI IPs has been reached.
E1084	This action may be performed only on a provisionable MPS.
E1085	The specified address is local to this MPS.
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 Blocklist Range).
E1093	The <*Provisioning Blocklist 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.
E1104	Both the entered IPs are same.
E1105	Invalid EMS Server name: <*Value*>. EMS Server name can contain only alphanumeric characters, hyphen and underscore! EMS Server name can contain a minimum of 5 and a maximum of 20 characters.

Table 4-1 (Cont.) EPAP Error Messages

E1106	Invalid Community String: <*Value*>. Only alphanumeric characters, hyphen and underscore are allowed. Community string length cannot exceed 127 characters.
E1107	Invalid value for Alarm feed variable: <*Value*>. Valid values are 'ON' or 'OFF'.
E1108	Maximum 5 EMS can be added.
E1109	The default router must be on the same network as MPS A.
E1110	The addresses for provisioning and GUI access must be different.
E1111	The addresses for provisioning and operations and maintenance must be different.
E1112	The addresses for GUI access and operations and maintenance must be different.
E1113	Invalid IP Address.
E1114	The specified IP already used for Local Network Configuration.
E1115	Remote PDB cannot be configured with %s as Local and Remote PDBA should be in the same IP format.

4.2 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 *Alarms and Maintenance Guide* 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, three LEDs correspond directly to alarm severities: critical, major, and minor. If more than one alarm level is active, all applicable LED lights are illuminated, not only the most severe alarm, until all alarms in that level are cleared.

4.2.1 Raising Alarms

This section details the steps to raise alarms for Long Wait on Write for PDBI Update and for NE count mismatch between PDB and RTDB.

4.2.1.1 Raising Alarm for Long Wait on Write for PDBI Update

Customers should complete the following steps in order to raise the " Long Wait on Write for PDBI Update" alarm. This will ensure the user is alerted to a PDBI write connection holding for too long:

1. Issue the uiEdit command "`PDBI_LONG_WAIT_ALARM_TIME`" `<time in seconds>` where <time in seconds> is the time value that a PDBI connection is allowed to hold a write connection before triggering the alarm.
2. Investigate the alarm banner on the EPAP GUI for the alarm text "Long wait on write for PDBI update"; or, identify the alarm bit 6000000000800000 from the connected EAGLE; or, find the alarm number 45121 from the SNMP NM server.
3. If the alarm is triggered, find the PDBI connection information by issuing the grep "`Throw alarm for connection`" `pdba.err.*` command in the `/usr/TKLC/epap/logs` directory.
4. Clear the alarm to release the PDBI write connection in question.

4.2.1.2 Raising Alarm for NE count mismatch between PDB and RTDB

Customer should schedule a cron job in "`/etc/cron.d/TS.EXAP`" for "`/usr/TKLC/appl/bin/checkNEsanity.pl`" in order to raise the alarm, when there is count mismatch between PDB and RTDB for Network Entity (NE).This will ensure that the user is alerted when there is any mismatch in NE count between PDB and RTDB. This cron will be scheduled only on the server having RTDB, hence don't schedule the cron on pdbonly server.

Customer can schedule the cron considering the following conditions:

- Cron should be scheduled once in a day.
- Server should not be involved in any other activity at the time when this cron is scheduled, to neglect any impact.
- It will be good to schedule the cron when the provisioning rate is very low or negligible.
- Cron should be scheduled at some specific time of the day when scheduling for once in a day.

For example: To schedule daily once at 05:00 , Sched="daily,1,05:00"

00 05 * * * epapdev /usr/TKLC/appl/bin/checkNEsanity.pl

Logs will be formed at /usr/TKLC/epap/logs directory.

On compact architecture, RTDB server:

`rtdbEpap17NEPrintCompact.log`

`rtdbEpap17NEPrintInorderCompact.log`

`checkNEsanity.log`

On extreme architecture RTDB server:

`rtdbEpap17NEPrintExtreme.log`

`rtdbEpap17NEPrintInorderExtreme.log`

`checkNEsanity.log`

On PDB server (compact/extreme):

`retrieveNEfromPDB.log` (to retrieve NE count from PDB)

If the alarm is triggered, follow the below mentioned recovery steps:

- When the alarm is observed, savelogs (application logs) is automatically taken for the first time but the customer will have to take the platform logs manually from the platcfg menu. Also, customer can retake the application logs, if more recent logs are needed.
- If we have other RTDBs connected to the same PDB and the DB on them is good, then the customer can restore the backup from one of the other connected RTDBs on this RTDB.
- If all RTDBs connected to the same PDB are show NE mismatch then restore both PDB and RTDB from backup taken from another site having the similar database.
- If the above two options are not feasible, then do a reload from PDB on this RTDB. This will reload the database from scratch on RTDB, from the connected PDB. This process will take time depending upon the total size of the database.

Alarms will be cleared once the mismatch is resolved.

4.2.2 Maintenance Blocks

MPS and **EPAP** have no direct means of accepting user input from or displaying output messages on EAGLE terminals. Maintenance, measurements, error, and status information are routed to EAGLE 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 *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 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. The information that is transferred is described in *Alarms and Maintenance Guide*.

4.2.3 Alarm Priorities

The **EPAP** sends the maintenance information, including the alarm data strings, to the **EAGLE** for interpretation. **Alarm** priorities determine which alarm category is displayed at the **EAGLE** terminal when multiple alarm levels exist simultaneously. **EAGLE** 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** terminal until any higher priority alarms are cleared.

4.2.4 Multiple Alarm Conditions

Critical, major and minor alarms appear repeatedly in each alarm delivery to the **EAGLE** 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** terminal when multiple alarms are reported, you can use the **EAGLE** `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** 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.

4.2.5 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.

4.3 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 installed memory size

4.3.1 Service Module Card Motherboard Verification

An SM8G-B card is required to support the **G-Flex**/ **G-Port**/**INP**/**EIR VSCCP** application on the **Service Module** card. **EAGLE** 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, as well as verifies the amount of memory in the SM card. 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.

4.3.2 Service Module Card Installed 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 installed memory both allocated and physically present on each Service Module card. See *Commands User's Guide* 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 installed memory. The 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**.

4.3.3 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 **Migration**application, **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 *Maintenance Guide*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** 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.

4.4 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. Refer to *Maintenance Guide* for EAGLE for additional information about LIM and Service Module cards.

- 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 improve the ratio (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 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.

  After an EAGLE database has been loaded, that database can be updated, if the system is not in an unstable Loading Mode. However, if an EAGLE update comes in during EAGLE database loading, the Service Module card aborts the current loading, issues a class 01D7 obit message (Figure 4-1), and reboots.

Figure 4-1 Obit Message for Abort of Card Loading

```
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
```

- 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.

4.5 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.

4.6 Commands

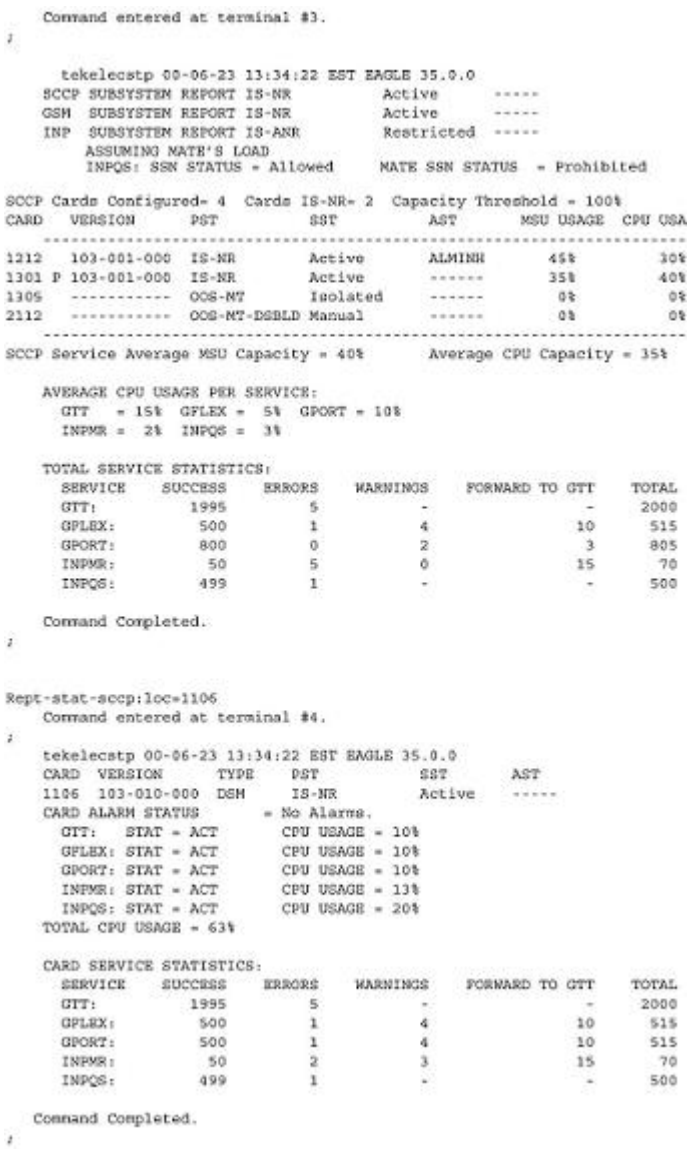
The commands described in this section report status information for the provisioning system.

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 4-2:

Figure 4-2 `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%  GFLEX =  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%
      GFLEX: STAT = ACT       CPU USAGE = 10%
      GPORT: STAT = ACT       CPU USAGE = 10%
      INPMR: STAT = ACT       CPU USAGE = 13%
      INPQS: STAT = ACT       CPU USAGE = 20%
    TOTAL CPU USAGE = 63%

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

   Command Completed.
;
```

rept-stat-db

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

Figure 4-3 `rept-stat-db` Command Report Example

```
   rept-stat-db:display=all:db=mps
   Command entered at terminal #4.

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

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

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

rept-stat-mps

The `rept-stat-mps` command reports the status of the provisioning system, including EPAP information.

There are two possible variants of this new command:

- `rept-stat-mps` - This produces a summary report showing the overall status of the G-Flex/G-Port/INP/EIR provisioning system and a moderate level of information for each 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 4-4:

Figure 4-4 rept-stat-mps Command Report Examples

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

    Integrat40 00-06-24 10:37:22 EST EAGLE 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.
;
```

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.

Figure 4-5 `rept-stat-trbl` Command Output Example

```
    rept-stat-trbl
    Command entered at terminal #10.
;
    eagle10605 99-06-24 14:34:08 EST EAGLE 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.
```

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.

Figure 4-6 `rept-stat-alm` Command Report Example

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

    eagle10605 99-06-24 23:59:39 EST EAGLE 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.
;
```

pass: cmd="Ping"

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

Figure 4-7 `pass: cmd="Ping"` Command Output Example

```
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)

;
```

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.

Figure 4-8 `pass: cmd="netstat"` Command Output Example

```
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
;
```

4.7 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.

Figure 4-9 Hourly Maintenance Report Output Example

```
    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"
;
```

4.8 Unsolicited Alarm and Information Messages

This section describes EPAP Unsolicited Alarm Messages (**UAMs**) and Unsolicited Information Messages (**UIMs**).

The EAGLE 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. The EAGLE controls and generates the alarm number, associated text, and formatting for alarms sent to EAGLE through the Maintenance Block mechanism.

Alarms and Maintenance Guide describes all EAGLE 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 *Alarms and Maintenance Guide*.

MPS platform and EPAP application alarms are reported in five 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.

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

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

Table 4-1 defines the application and platform alarms that are forwarded to EAGLE 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 *Alarms and Maintenance Guide*.

Table 4-2 EAGLE MPS Platform and Application Alarms

UAM #	Severity	Message Text
370	Critical	Critical Platform Failure(s)

Table 4-2 (Cont.) EAGLE MPS Platform and Application Alarms

UAM #	Severity	Message Text
372	Major	Major Platform Failure(s)
373	Major	Major Application Failure(s)
374	Minor	Minor Platform Failure(s)
375	Minor	Minor Application Failure(s)
250	Clearing	MPS Available

Figure 4-10 Alarm Output Example

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

Figure 4-11 MPS Available Alarm

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

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

4.8.1 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)

Figure 4-12 Service Module Card-EPAP Link Alarm Example

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

RTDB Audit Alarms

During an audit of the Service Module cards and the 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
123456789012345678901234567890123456789012345678901234567890123456789012345
67890
    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
123456789012345678901234567890123456789012345678901234567890123456789012345
67890
    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
123456789012345678901234567890123456789012345678901234567890123456789012345
67890
    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
123456789012345678901234567890123456789012345678901234567890123456789012345
67890
    station1234 99-09-30 16:28:08 EST EAGLE 35.0.0
    0012.0452   CARD 1108 VSCCP        RTDB reload complete
```

5
EPAP Software Configuration

This chapter describes how to configure the EPAP software.

5.1 Setting Up an EPAP Workstation

The customer workstation serving as a client PC, shown in Figure 3-1 must meet the criteria described below.

5.1.1 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.

5.1.2 Compatible Browsers

Chromium-based Microsoft Edge is supported and certified for use with the EPAP Graphical User Interface (GUI). Other browsers may be partially compatible with the EPAP GUI. When using these browsers, this message may be displayed when logging in to the EPAP GUI:

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

When an intranet site is used, the user must change the internet settings in order to be compatible. Complete the following steps:

1. Select **Tools** in the IE browser menu.
2. Select **Compatibility View Settings**.
3. Uncheck the **Display intranet sites in Compatibility View** option.

5.2 EPAP Configuration and Initialization

Before beginning to use EPAP for provisioning, the EPAP software must be configured and initialized. The EPAP configuration and initialization is performed through the EPAP text-based user interface.

Connect a local (optional) customer terminal to eth0 (port 0 on GB card 1) on the MPS frame at each EAGLE. Refer to *Application B Card Hardware and Installation Guide* for additional information. To begin the initialization, log in to EPAP A the first time as the `epapconfig` user. An automatic configuration is performed on both mated EPAPs.

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

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

> **Note:**
>
> The configuration procedure and differences in the Configuration Menu for Standalone PDB EPAP are provided in Standalone PDB EPAP .

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 is used in the configuration procedure.

5.2.1 Required Network Address Information

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

Table 5-1 Information for Provisionable MPSs at EAGLE A

Common Information			
MPS A Provisioning Network Address	.	.	.
MPS B Provisioning Network Address	.	.	.
Netmask	.	.	.
Default Router	.	.	.
Backup Provisioning Network Information (Optional)			
MPS A Backup Provisioning Net. Addr.	.	.	.
MPS B Backup Provisioning Net. Addr.	.	.	.
Backup Netmask	.	.	.
Backup Default Router	.	.	.
RTDB Homing			
Select one: *(local* **MPS** *A address)*			
Home to specific **PDB**	.	.	.
Active homing/allow alternate **PDB**			
Active homing/disallow alternate **PDB**			

Table 5-1 (Cont.) Information for Provisionable MPSs at EAGLE A

Common Information
External Information
MPS A Provisioning Network Address for **MPS** at **EAGLE** B (copy from Table 5-2) . . .
Port Forwarding and Static NAT Information (Optional)
MPS A Forwarded **HTTP** Port
MPS B Forwarded **HTTP** Port
MPS A Forwarded SuExec Port
MPS B Forwarded SuExec Port
MPS A Forwarded **PDBI** Port
MPS A Forwarded Banner Port
MPS B Forwarded Banner Port
MPS A Provisioning Static **NAT** Addr. . . .
MPS B Provisioning Static **NAT** Addr. . . .
MPS A Forwarded **HTTP** Port for **MPS** at **EAGLE** B (Copy from Table 5-2) . . .

Table 5-2 Information for Provisionable MPSs at EAGLE B

Common Information
MPS A Provisioning Network Address . . .
MPS B Provisioning Network Address . . .
Netmask . . .
Default Router . . .
Backup Provisioning Network Information (Optional)
MPS A Backup Provisioning Net. Addr. . . .
MPS B Backup Provisioning Net. Addr. . . .
Backup Netmask . . .
Backup Default Router . . .
RTDB Homing
Select one: *(local* **MPS** *A address)*
Home to specific **PDB** . . .
Active homing/allow alternate **PDB**
Active homing/disallow alternate **PDB**
External Information
MPS A Provisioning Network Address for **MPS** at **EAGLE** A (copy from Table 5-1) . . .
Port Forwarding and Static NAT Information (Optional)
MPS A Forwarded **HTTP** Port
MPS B Forwarded **HTTP** Port
MPS A Forwarded SuExec Port

Table 5-2 (Cont.) Information for Provisionable MPSs at EAGLE B

Common Information
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** A (Copy from Table 5-1) . . .

Table 5-3 Information for Non-Provisionable MPSs at EAGLE #1

Common Information
MPS A Provisioning Network Address . . .
MPS B Provisioning Network Address . . .
Netmask . . .
Default Router . . .
Backup Provisioning Network Information (Optional)
MPS A Backup Provisioning Net. Addr. . . .
MPS B Backup Provisioning Net. Addr. . . .
Backup Netmask . . .
Backup Default Router . . .
RTDB Homing
Select one:
Home to specific **PDB** . . .
Active homing/allow alternate **PDB**
Active homing/disallow alternate **PDB**
External Information
MPS A Provisioning Network Address for **MPS** at **EAGLE** A (copy from Table 5-1) . . .
MPS A Provisioning Network Address for **MPS** at **EAGLE** B (copy from Table 5-2) . . .
Port Forwarding and Static NAT Information (Optional)
MPS A Forwarded **HTTP** Port
MPS B Forwarded **HTTP** Port
MPS A Forwarded SuExec Port
MPS B Forwarded SuExec Port
MPS A Forwarded Banner Port
MPS B Forwarded Banner Port
MPS A Provisioning Static **NAT** Addr. . . .
MPS B Provisioning Static **NAT** Addr. . . .

Table 5-4 Information for Non-Provisionable MPSs at EAGLE #2

Common Information			
MPS A Provisioning Network Address	.	.	.
MPS B Provisioning Network Address	.	.	.
Netmask	.	.	.
Default Router	.	.	.
Backup Provisioning Network Information (Optional)			
MPS A Backup Provisioning Net. Addr.	.	.	.
MPS B Backup Provisioning Net. Addr.	.	.	.
Backup Netmask	.	.	.
Backup Default Router	.	.	.
RTDB Homing			
Select one:			
Home to specific **PDB**	.	.	.
Active homing/allow alternate **PDB**			
Active homing/disallow alternate **PDB**			
External Information			
MPS A Provisioning Network Address for **MPS** at **EAGLE** A (copy from Table 5-1)	.	.	.
MPS A Provisioning Network Address for **MPS** at **EAGLE** B (copy from Table 5-2)	.	.	.
Port Forwarding and Static NAT Information (Optional)			
MPS A Forwarded **HTTP** Port			
MPS B Forwarded **HTTP** Port			
MPS A Forwarded SuExec Port			
MPS B Forwarded SuExec Port			
MPS A Forwarded Banner Port			
MPS B Forwarded Banner Port			
MPS A Provisioning Static **NAT** Addr.	.	.	.
MPS B Provisioning Static **NAT** Addr.	.	.	.

5.2.2 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). The information in Table 5-5 is used for both internal customer network configuration and VPN access for support.

Table 5-5 Firewall Requirements

Server Interface	IP Address	TCP/IP Port	Inbound	Outbound	Use/Comments
EPAP Application Firewall Requirements:					
Port 1	Main/Backup provisioning IP configured on EPAP	22	Yes	Yes	SSH/SCP/SFTP
Port 1	NTP server IP(s) configured on EPAP	123	Yes	Yes	NTP - Needed for time-sync.
Port 1	Main/Backup provisioning IP configured on EPAP	80	Yes	No	APACHE - Needed for EPAP Web-based GUI.
Port 1	Main/Backup provisioning IP configured on EPAP	8001-8002	Yes	No	SUXEC (process) - Needed by EPAP Web-based GUI.
Port 1	Main/Backup provisioning IP configured on EPAP	8473	Yes	Yes	GUI server (process) - Needed by EPAP Web-based GUI.
Port 1	Main/Backup provisioning IP configured on EPAP	5871	Yes	No	Data download from PDBA to RTDB
Port 1	Main/Backup provisioning IP configured on MPS A and MPS B	5872	Yes	No	Data replication between Active and Standby PDBA
Port 1	Main/Backup provisioning IP configured on EPAP	5873	Yes	No	Used to send Provisioning data to the EPAP.
Port 1	Main/Backup provisioning IP configured on EPAP	5874	Yes	Yes	Used to send Provisioning data to the EPAP
Port 1	VIP configured on EPAP	5876	Yes	Yes	Used for provisioning from PDBA Proxy
Port 1	Main/Backup provisioning IP configured on EPAP	5883	Yes	Yes	Used to send provisioning data to EPAP through SOG Interface
Port 1	Main/Backup provisioning IP configured on EPAP	9696	Yes	Yes	PDBA (process) - PDB application manages the provisioning data.
MySQL port 3306	N/A	3306	Open	Open	Allows functionality between mated and provisioning sites

Table 5-5 (Cont.) Firewall Requirements

Server Interface	IP Address	TCP/IP Port	Inbound	Outbound	Use/Comments
EPAP Application Firewall Requirements:					
MySQL port 3307	N/A	3307	Open	Open	Allows functionality between mated and provisioning sites
RMM Firewall Requirements:					
RMM Port	RMM IP configured on EPAP	22	Yes	Yes	SSH/SCP/SFTP
RMM Port	RMM IP configured on EPAP	80	Yes	No	HTTP - Needed for RMM Web-based GUI.
RMM Port	RMM IP configured on EPAP	443	Yes	No	SSL (https) - Needed for RMM Web-based GUI secure connection (REQUIRED)
RMM Port	RMM IP configured on EPAP	623	Yes	Yes	RMCP

5.2.3 Configuration Menu Conventions

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

Menu Format

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

Figure 5-1 Configuration Menu 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
```

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.

5.3 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 5-2.

Figure 5-2 Initial Configuration Text Screen

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

             1. The mate MPS servers (MPS A and MPS B) must be powered on.
             2. "Initial Platform Manufacture" for the mate MPS servers
                must be complete.
             3. The sync network between the mate MPS servers must be
                operational.
             4. You must have the correct password for the EPAPdev user on
                the mate MPS server.
             5. You must be prepared to designate this MPS as provisionable
                or non-provisionable.

Press return to continue...
```

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

When the five criteria are met, press Return and the process resumes. Figure 5-3 shows the continuation of the screen information. The installer enters **y** if the installation is to continue.

Figure 5-3 Initial Configuration Continues

```
Are you sure you wish to continue? [N]: y
Password of epapdev:
Could not get authorized keys file from remote (mate).
Maybe it does not exist.  Continuing...
ssh is working correctly.
Password of root:
Could not get authorized keys file from remote (mate).
Maybe it does not exist.  Continuing...
ssh is working correctly.
Building the initial database on side A.
  Stopping local slave
  Stopping remote slave
EuiDB already exists.
  Starting local slave
  Starting remote slave
```

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

Next, the installer declares the MPS to be provisionable or non-provisionable, as shown in Figure 5-4. The example illustrates this MPS as a provisionable MPS.

Figure 5-4 Designating Provisionable or Non-Provisionable MPS

```
The provisioning architecture of the EPAP software allows for exactly 2
customer provisionable sites.  Additional sites that are to receive the data
provisioned to the provisionable sites should answer 'N' here.

If there are only 2 mated sites, it is safe to answer 'Y' here.

Is this site provisionable? [Y]: y
```

Next, the installer is prompted for the `epapdev` user password on the mate MPS server. Figure 5-5 shows sample output that is generated after the correct password is entered.

Figure 5-5 Entering the `epapdev` Password

```
Password for EPAPdev@mate:

Connecting to mate...
ssh is working correctly.

still OK.
still OK.
Building the initial database on side A.
  Stopping local slave
  Stopping remote slave
No preexisting EuiDB database was detected.
Enabling replication:
  deleting old binary logs on local server
  resetting local slave.
  deleting old binary logs on remote server
  resetting remote slave
  Starting local slave
  Starting remote slave
There was no epap.cfg file.  Using default configuration.
```

The Configuration Menu appears for the first time.

EPAP Configuration Menu

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

EPAP A 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                          |
|----|-----------------------------------|
| 10 | SNMP Configuration                |
|----|-----------------------------------|
| 11 | Configure Alarm Feed              |
|----|-----------------------------------|
| 12 | Configure Query Server            |
```

```
|----|---------------------------------|
| 13 | Configure Query Server Alarm Feed |
|----|---------------------------------|
| 14 | Configure SNMP Agent Community    |
|----|---------------------------------|
| 15 | DB Architecture Menu              |
|----|---------------------------------|
|  e | Exit                              |
\-----------------------------------/

Enter Choice:
```

EPAP B 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                          |
|----|---------------------------------|
| 10 | SNMP Configuration                |
|----|---------------------------------|
| 11 | Configure Alarm Feed              |
|----|---------------------------------|
| 12 | Configure Query Server            |
|----|---------------------------------|
| 13 | Configure Query Server Alarm Feed |
|----|---------------------------------|
| 14 | Configure SNMP Agent Community    |
|----|---------------------------------|
| 15 | DB Architecture Menu              |
|----|---------------------------------|
|  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**.

> **Note:**
>
> When exiting from `epapconfig` menu, the EPAP GUI will be terminated for a while and will be automatically restored.

Display Configuration

The Display Configuration option **1** displays a configuration of the EPAP. The following figure shows an example report:

Figure 5-6 Example of Configuration Report When the EPAP is Not Configured

```
EPAP A Provisioning Network IP Address    = Not configured
EPAP A Provisioning Network IP Address v6 = Not configured
EPAP B Provisioning Network IP Address    = Not configured
EPAP B Provisioning Network IP Address v6 = Not configured
Provisioning Network Netmask              = Not configured
Provisioning Network Prefix               = Not configured
Provisioning Network Default Router       = Not configured
Provisioning Network Default Router v6    = Not configured
EPAP A Backup Prov Network IP Address     = Not configured
EPAP A Backup Prov Network IP Address v6  = Not configured
EPAP B Backup Prov Network IP Address     = Not configured
EPAP B Backup Prov Network IP Address v6  = Not configured
Backup Prov Network Netmask               = Not configured
Backup Prov Network Prefix v6             = Not configured
Backup Prov Network Default Router        = Not configured
Backup Prov Network Default Router v6     = 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 IP Version                           = Not configured
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                    = Not configured
Remote Provisioning VIP                   = Not configured
Local PDBA Address                        = 0.0.0.0
Local PDBA Address v6                     = 0000:0000:0000:0000:0000:0000:0000:0000
Remote PDBA Address                       = 0.0.0.0
Remote PDBA B Address                     = Not configured
Time Zone                                 = America/New_York
PDB Database                              = None
Preferred PDB                             = 0.0.0.0
Allow updates from alternate PDB          = Yes
Auto DB Recovery Enabled                  = No
PDBA Proxy Enabled                        = No

Press return to continue...
```

Addresses that you choose should not conflict with your internal network addresses. The class C networks you choose should not conflict with the class C network used in your network scheme. Table 5-6 shows an example of IP addresses that could be used in the configuration process.

Table 5-6 Sample IP Addresses Used in Configuration

Provisioning Network Information	MPS EAGLE A (Local) IP Addresses	MPS EAGLE 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

5.3.1 Configure Network Interfaces Menu

The Configure Network Interfaces Menu option `2` of the Configuration Menu displays the submenu shown in Figure 5-7. It supports the configuration of all the network interfaces for the EPAP.

Figure 5-7 Configure Network Interfaces Menu

```
 /-----Configure Network Interfaces Menu----\
/--------------------------------------------\
|   1 | Configure Provisioning Network       |
|-----|--------------------------------------|
|   2 | Configure Sync Network               |
|-----|--------------------------------------|
|   3 | Configure DSM Network                |
|-----|--------------------------------------|
|   4 | Configure Backup Provisioning Network |
|-----|--------------------------------------|
|   5 | Configure Static NAT Addresses       |
|-----|--------------------------------------|
|   6 | Configure Provisioning VIP Addresses  |
|-----|--------------------------------------|
|   e | Exit                                 |
\--------------------------------------------/

Enter Choice:
```

Configure Provisioning Network

The Configure Provisioning Network option `1` of the Configure Network Interfaces Menu configures the EPAP provisioning network. With EPAP 16.1, the user is able to configure an IP address, net mask, and default router IP address when using an IPv4 address, and an IP address, Prefix and default router when using an IPv6 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. 0.0.0.0 is a valid IP address and can be used to reset the VIP/backup provisioning IP address.

> **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 5-8 for the option `1` configuration.

Figure 5-8 Configure Provisioning Network Menu

```
Entered the configMenuConfigProvNet Menu

MPS Side A:  hostname: epaprpi  hostid: a8c02d3d
             Platform Version: 4.0.10-5.5.1_75.20.0
             Software Version: EPAP 161.0.1-16.1.0_161.2.0
             Thu Apr  9 00:41:47 EDT 2015

 /-----Configure Provisiong Network Menu-\
/-----------------------------------------\
|   1 | IPv4 Configuration                |
|-----|-----------------------------------|
|   2 | IPv6 Configuration                |
|-----|-----------------------------------|
|   e | Exit                              |
\-----------------------------------------/

Enter Choice: 2

Verifying connectivity with mate...
EPAP A provisioning network IPv6 Address: 2606:b400:605:b80b:200:17ff:fe0f:2884
EPAP B provisioning network IPv6 Address: 2606:b400:605:b80b:200:17ff:fe0f:2885
EPAP provisioning network IPv6 prefix: 64
EPAP provisioning network IPv6 default router: 2606:b400:605:b80b::
```

> **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. 0.0.0.0 is a valid IP address and can be used to reset the VIP/backup provisioning IP address.

> **Note:**
>
> Unless there is a known network address conflict, the installer can bypass option `3`.

> **Note:**
>
> It is strongly advised not to change the DSM network subnet (IP addresses), if not absolutely necessary.

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 5-9 for the option `3` output.

Figure 5-9 Configure DSM Network

```
Verifying connectivity with mate ...
Enter the first 3 octets for the EPAP main DSM network [192.168.128]:
Enter the first 3 octets for the EPAP backup DSM network [192.168.129]:

Press Return to continue ...
```

> **Note:**
>
> Take care in configuring the IP information. Incorrect information will prevent the EPAP from communicating with the EAGLE.

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. With EPAP 16., the user is able to configure an IP address, net mask, and default router IP address when using an IPv4 address, and an IP address, Prefix and default router when using an IPv6 address. 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 5-10 for the option `4` output.

Figure 5-10 Configure Backup Provisioning Network

```
MPS Side A:  hostname: epaprpi  hostid: a8c02d3d
             Platform Version: 4.0.10-5.5.1_75.20.0
             Software Version: EPAP 161.0.1-16.1.0_161.2.0
             Thu Apr  9 00:51:38 EDT 2015

 /-----Configure Backup Provisioning Network Menu-\
/-------------------------------------------------\
|  1 | IPv4 Configuration                         |
|----|-------------------------------------------|
|  2 | IPv6 Configuration                         |
|----|-------------------------------------------|
|  e | Exit                                       |
\-------------------------------------------------/

Enter Choice: 2

Verifying connectivity with mate...
EPAP A backup provisioning network IPv6 Address: 2606:b400:605:b80b:200:17ff:fe0f:2886
EPAP B backup provisioning network IPv6 Address: 2606:b400:605:b80b:200:17ff:fe0f:2887
EPAP backup provisioning network prefix: 64
EPAP backup provisioning network default router: 2606:b400:605:b80b::
```

> **Note:**
>
> 127.0.0.1 is not a valid IP address for this operation. 0.0.0.0 is a valid IP address and can be used to reset the VIP/backup provisioning IP address.

> **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. 0.0.0.0 is a valid IP address and can be used to reset the VIP/backup provisioning IP address.

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

This information should be received from the customer for the MPS and recorded in Table 5-1 and Table 5-2 .

Configure Static NAT Addresses

The Configure Static **NAT** Addresses option 6 from the Configure Network Interfaces Menu provides the functionality to configure the static NAT addresses of the EPAP.

> **Note:**
>
> Only IPv4 is supported with Static NAT addresses.

Each numbered item of the Configure Static NAT Addresses menu allows the user to specify an IP Address used outside of the firewall for remote access to the MPS. The following Figure 5-11 shows an example of a resulting prompt.

> **Note:**
>
> 127.0.0.1 is not a valid IP address for this operation. 0.0.0.0 is a valid IP address and can be used to reset the VIP/backup provisioning IP address.

Figure 5-11 Configuring NAT Addresses Prompt

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

Configure Provisioning VIP Addresses

The Configure Provisioning VIP Addresses option 7 from the Configure Network Interfaces Menu provides the functionality to configure the **PDBA** Proxy feature.

The user must enter the VIP address for the local PDBA (MPS-A) and the remote PDBA using either an IPv4 or IPv6 address. The following figure shows an example of the option 7 output.

Figure 5-12 Configure Provisioning VIP Address

```
MPS Side A:  hostname: epaprpi  hostid: a8c02d3d
             Platform Version: 4.0.10-5.5.1_75.20.0
             Software Version: EPAP 161.0.1-16.1.0_161.2.0
             Thu Apr  9 01:03:37 EDT 2015

 /-----Configure Provisioning VIP address Menu-\
/-----------------------------------------------\
|  1 | IPv4 Configuration                       |
|----|-----------------------------------------|
|  2 | IPv6 Configuration                       |
|----|-----------------------------------------|
|  e | Exit                                     |
\-----------------------------------------------/

Enter Choice: 2

Verifying root connectivity with mate...
EPAP local provisioning Virtual IPv6 Address: 2606:b400:605:b80b:200:17ff:fe0f:2890
EPAP remote provisioning Virtual IPv6 Address: 2606:b400:605:b80b:200:17ff:fe0f:2891
```

> **Note:**
>
> 127.0.0.1 is not a valid IP address for this operation. 0.0.0.0 is a valid IP address and can be used to reset the VIP/backup provisioning IP address.

5.3.2 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 List of Time Zones for the option 3 output.

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 List of Time Zones 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 .

5.3.3 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 **EPAP**s. The **EPAP**s exchange encryption keys are required to run the secure shell.

The exchange normally occurs automatically during EPAP initialization. Use this menu item only if the exchange must be performed manually.

See Figure 5-22 for the option `4` output.

Figure 5-13 Exchange Secure Shell Keys Menu

```
 /-----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: 2

Are you sure you wish to exchange keys with remote? [N]: Y
Remote IP Address: 2606:b400:605:b80b:200:17ff:fe0f:2876
```

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 sub menu "Exchange Keys with Remote" allows the user to exchange keys with the remote server. The remote server IP will be either IPv4 or IPv6.

The `epapconfig` user must know the password for the `epapdev@mate`. The notification “ssh is working correctly” in the following figure confirms the “ssh” (i.e., secure shell) exchange of keys has completed successfully.

See Figure 5-23 for the Option **1** output.

Figure 5-14 Exchange Secure Shell Keys 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:
```

5.3.4 Change Password

The Change Password option `5` changes the text-based user interface password for the `epapconfig` login name for both MPS A and B.

See Figure 5-24 for the option 5 output.

Figure 5-15 Change Password

```
Verifying connectivity with mate...
Are you sure you wish to change the text UI password on MPS A and B? [N]: y
Enter new password for text UI user:
Re-enter new password:

Press return to continue...
```

5.3.5 Platform Menu

The **EPAP** Platform Option 6 accesses the Platform menu so that the epapconfig user can access and manage the platform functions shown in the menu. See Figure 5-16 for the option 6 output.

Figure 5-16 Platform Menu Output

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

Enter Choice:
```

Initiate Upgrade

The Initiate Upgrade option 1 of the **EPAP** Platform Menu initiates an upgrade on the selected **EPAP**. For upgrade output or procedures, contact Oracle Communications Technical Services; refer to My Oracle Support.

Reboot MPS

The Reboot **MPS** option 2 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.

MySQL Backup

The MySQL Backup option `3` 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 `4` 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 to "/var/TKLC/
epap/free/rtdbBackup_<hostname>_<timestamp>_v<RTDB version>.<No. of RTDB
files>.bkp.tar.gz"? [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 `5` of the EPAP Platform Menu backs up the PDB database. The output is shown below

```
Are you sure you want to backup the PDB to /var/TKLC/epap/free/
pdbBackup_<hostname>_<timestamp>_DBBirthdate_<birthdate>GMT_DBLevel_<dblevel>_
v<PDB version>.<No. of ibdata files in the backup>.bkp.tar.gz? [N]: Y

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

> **Note:**
>
> PDB only maintains a single copy of backup file. If the backup file is already present, the **PDB Backup already exists in free directory error message** is displayed. Therefore it is required to transfer PDB backup file to remote server using Configure File Transfer as described in section Configure File Transfer or manually by using sftp.

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.

5.3.6 Configure NTP Server Menu

The Configure **NTP** Server Menu option **7** allows for the display, addition, and removal of an external **NTP** server. As of EPAP 16.1, the user is able to add/remove external NTP servers using both IPv4 and IPv6 addresses.

- The user is allowed to configure IPv4 only remote system address
- The user is allowed to configure IPv6 only remote system address
- On dual stack - the user is allowed to configure IPv4 or IPv6 remote system address

See the following figure for the option **9** output:

Figure 5-17 Configure NTP Server Menu

```
MPS Side A:  hostname: epaprpi  hostid: a8c02d3d
             Platform Version: 4.0.10-5.5.1_75.20.0
             Software Version: EPAP 161.0.1-16.1.0_161.2.0
             Thu Apr  9 01:08:08 EDT 2015

 /-----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
```

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 following figure 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.

Figure 5-18 Add NTP Server Menu

```
MPS Side A:  hostname: epaprpi  hostid: a8c02d3d
             Platform Version: 4.0.10-5.5.1_75.20.0
             Software Version: EPAP 161.0.1-16.1.0_161.2.0
             Thu Apr  9 01:08:11 EDT 2015

 /-----Add External NTP Server Menu-\
/-------------------------------------\
|  1 | IPv4 Configuration             |
|----|--------------------------------|
|  2 | IPv6 Configuration             |
|----|--------------------------------|
|  e | Exit                           |
\-------------------------------------/

Enter Choice: 2

Verifying connectivity with mate...
Are you sure you wish to add new NTP Server? [N]: y
NTP Server IPv6 Address: 2606:b400:605:b80b:200:17ff:fe0f:2894
```

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.

5.3.7 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. Beginning with EPAP 16.1, the user is able to configure both IPv4 and IPv6 addresses for a PDB address. See Figure 5-19 for the option **8** output.

Figure 5-19 Configure PDB Menu

```
MPS Side A:  hostname: epaprpi  hostid: a8c02d3d
             Platform Version: 4.0.10-5.5.1_75.20.0
             Software Version: EPAP 161.0.1-16.1.0_161.2.0
             Thu Apr  9 01:10:19 EDT 2015

 /-----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
```

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. The following table shows Remote PDBA configuration use cases:

Table 5-7 Remote PDBA Configuration Use Cases

Site 1 Configuration	Site 2 Configuration		
	IPv4 Only	IPv6 Only	Dual Stack
IPv4 Only	Allowed	Not Allowed	Only IPv4 IP allowed for remote PDBA
IPv6 Only	Not allowed	Allowed	Only IPv6 IP allowed for remote PDBA
Dual Stack	Only IPv4 IP allowed for remote PDBA	Only IPv6 IP allowed for remote PDBA	IP version should be the same on both sites (either IPv4 or IPv6)*

* If both sites are configured in dual stack, the configuration must be kept consistent at both sites. The user is responsible for the maintenance of this configuration.

> **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.

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 5-20 shows the option **2** output.

Figure 5-20 RTDB Homing Menu

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

Enter Choice:
```

Configure Specific RTDB Homing

The Configure Specific RTDB Homing option **1** of the RTDB Homing Menu sets the RTDB homing policy to specific and configures the address of the preferred PDB.

This configuration cannot be completed until the PDB network has been configured. See Configure PDB Network. 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. When the EPAP is configured in a dual stack configuration, the PDBA also has both the IPs, one in IPv4 format and the other in IPv6 format. By default, the RTDB Homing Policy is set to the PDBA IPv6 IP. If the user wants to change the RTDB homing policy to the PDBA IPv4 IP, then the **Configure Specific RTDB Homing** menu option must be used.

Figure 5-21 RTDB Homing Policy Configuration

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

Enter Choice: 1

There are two configured PDBs for this MPS:
1. 192.168.55.82 (local)
2. 2606:B400:605:B80E:200:17FF:FE0E:A6A1 (local)
3. 2606:B400:605:B80B:200:17FF:FE0F:2884

Select the preferred PDB from which to receive updates [1]: 1

The RTDB Homing policy is set to 'specific' and will prefer
updates from 192.168.55.82

Press return to continue...
```

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. To complete this configuration, the user is prompted to configure the remote PDBA addresses from which the non-provisionable EPAP takes the updates. The user is allowed to specify either the IPv4 or the IPv6 address for the remote PDBA:

Figure 5-22 Configure PDB Network for Provisionable MPS

```
MPS Side A:  hostname: epaprpi  hostid: a8c02d3d
             Platform Version: 4.0.10-5.5.1_75.20.0
             Software Version: EPAP 161.0.1-16.1.0_161.2.0
             Thu Apr  9 01:10:22 EDT 2015

 /-----PDB Network Configuration Menu-\
/--------------------------------------\
|   1 | IPv4 Configuration              |
|-----|---------------------------------|
|   2 | IPv6 Configuration              |
|-----|---------------------------------|
|   e | Exit                            |
\--------------------------------------/

Enter Choice: 2

Verifying connectivity with mate...
This MPS is configured to be provisionable.  The EPAP local PDBA
address is currently set to 2606:b400:605:b80b:200:17ff:fe0f:2888
The EPAP local PDBA IP Address is 2606:b400:605:b80b:200:17ff:fe0f:2888
EPAP remote PDBA IPv6 Address: 2606:b400:605:b80b:200:17ff:fe0f:2889
EPAP remote PDBA B machine IPv6 Address: 2606:b400:605:b80b:200:17ff:fe0f:2889
```

Figure 5-23 Configure PDB Network for Non-Provisionable MPS

```
MPS Side A:  hostname: Recife-B  hostid: fa0a9633
             Platform Version: 4.0.10-5.5.1_75.20.0
             Software Version: EPAP 161.0.1-16.1.0_161.2.0
             Thu Apr  9 03:58:32 EDT 2015

 /-----PDB Network Configuration Menu-\
/--------------------------------------\
|  1 | IPv4 Configuration              |
|----|---------------------------------|
|  2 | IPv6 Configuration              |
|----|---------------------------------|
|  e | Exit                            |
\--------------------------------------/

Enter Choice: 2

This MPS is configured to be non-provisionable.  You will be prompted
for both of the remote PDBA addresses.  Order does not matter.

Enter one of the two PDBA IPv6 addresses: 2606:b400:605:b80b:200:17ff:fe0f:2895

Enter the other of the two PDBA IPv6 addresses: 2606:b400:605:b80b:200:17ff:fe0f:2896
```

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.

5.3.8 Security

Figure 5-24 EPAP Configuration Menu

The Security Menu option `9` provides access to configure the Idle Terminal Timeout and the password restrictions for EPAP system users. See Figure 5-25 for the option 8 output.

Figure 5-25 EPAP Configure Security Menu

```
 /-----EPAP Configure Security Menu-\
/-------------------------------------\
|   1 | Idle Terminal Timeout         |
|-----|-------------------------------|
|   2 | Password Restriction          |
|-----|-------------------------------|
|   3 | Configure Authorized IPs      |
|-----|-------------------------------|
|   e | Exit                          |
\-------------------------------------/

Enter Choice: 3
```

The submenu **Configure Authorized IPs** allows the user to configure the authorized IPs for the EPAP. The functionality of this menu is the same as the GUI menu **User Administration**, and then **Authorized IPs**.

Figure 5-26 EPAP Configure Authorized IPs Menu

```
 /-----Configure Authorized IPs Menu-\
/-------------------------------------\
|   1 | Display Authorized IPs         |
|-----|--------------------------------|
|   2 | Add Authorized IP              |
|-----|--------------------------------|
|   3 | Remove Authorized IP           |
|-----|--------------------------------|
|   e | Exit                           |
\-------------------------------------/

Enter Choice:
```

The **Add Authorized IP** menu option allows the user to add a new IP address, either in IPv4 or IPv6 format, to the list of the authorized IP addresses. The authorized IP version is independent of the EPAP network configuration. The authorized IP list can have a mix of the IPv4 and IPv6 IPs:

Figure 5-27 Add Authorized IP

```
 /-----Add Auth Ip Menu--\
/-------------------------\
|   1 | IPv4 Configuration |
|-----|--------------------|
|   2 | IPv6 Configuration |
|-----|--------------------|
|   e | Exit               |
\-------------------------/

Enter Choice: 2

Enter the Authorized IP to be added: 2606:B400:605:B80E:200:17FF:FE0E:A6A1

Authorized IP [2606:B400:605:B80E:200:17FF:FE0E:A6A1] added successfully.

Press return to continue...
```

The **Display Authorized IPs** menu option displays the list of authorized IPs. It displays all the configured IPs:

Figure 5-28 Display Authorized IPs

```
 /-----Configure Authorized IPs Menu-\
/-------------------------------------\
|  1 | Display Authorized IPs         |
|----|--------------------------------|
|  2 | Add Authorized IP              |
|----|--------------------------------|
|  3 | Remove Authorized IP           |
|----|--------------------------------|
|  e | Exit                           |
\-------------------------------------/

Enter Choice: 1

Authorized IP list:
1.1.1.1
2606:B400:605:B80E:200:17FF:FE0E:A6A1

Press return to continue...
```

The **Remove Authorized IP** screen allows the user to remove an IP address from the list of authorized IP addresses. The screen has no change for the IP version. The "IP to remove" field accepts both type of IPs, either IPv4 or IPv6:

Figure 5-29 Remove Authorized IP

```
 /-----Configure Authorized IPs Menu-\
/-------------------------------------\
|  1 | Display Authorized IPs         |
|----|--------------------------------|
|  2 | Add Authorized IP              |
|----|--------------------------------|
|  3 | Remove Authorized IP           |
|----|--------------------------------|
|  e | Exit                           |
\-------------------------------------/

Enter Choice: 3

Enter the Authorized IP to be removed: 2606:B400:605:B80E:200:17FF:FE0E:A6A1

Authorized IP [2606:B400:605:B80E:200:17FF:FE0E:A6A1] removed successfully.

Press return to continue...
```

Idle Terminal Timeout

The Idle Terminal Timeout, option **1** of the Figure 5-25 displays the submenu shown below. 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 will 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                                           |
\-----------------------------------------------------/
```

PDBI Idletimeout

The PDBI `idletimeout` parameter in Connect() request allows the client to specify the amount of time that the connection can remain idle before the PDBA terminates it.

This `idletimeout` parameter is configurable on EPAP via the uiEdit variable "PDBI_IDLE_TIMEOUT". The default value of this variable is zero (0) and the valid range is 0 to 2678400 (60*44640) seconds.

The `idletimeout` parameter in the PDBI Connect() request overrides the configured value on EPAP for that connection instance.

Password Restriction

The Password Restriction, option 2 of Figure 5-25 displays the submenu shown below. 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                                  |
\-----------------------------------------/
```

System Default

Option 1 of the above menu displays the submenu shown below.

In the below mentioned submenu, 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
|
\-------------------------------------------------------------------------------
/
```

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 below.

```
 /-----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 below mentioned submenu 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.

```
 /-----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 number 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 number 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 number 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

The **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 EPAP Configuration Menu. Linux PAM rules are not applicable while changing the password for the **epapconfig** user. Only the configured minimum password length applies.

> **Note:**
>
> If the password for the **appuser** or **epapconfig** user is changed by the root user, the **appuser** or **epapconfig** user will be prompted to change the password again.

5.3.9 SNMP Configuration Menu

The SNMP Configuration option **10** is used to support all configuration related to SNMPv2c and SNMPv3. See Figure 5-30 for the option `10` output.

Figure 5-30 EPAP SNMP Configuration Menu

```
 /-----EPAP SNMP Configuration Menu-\
/-------------------------------------\
|  1  | SNMP Global Mode              |
|-----|-------------------------------|
|  2  | View Configuration            |
|-----|-------------------------------|
|  3  | Group Configuration           |
|-----|-------------------------------|
|  4  | User Configuration            |
|-----|-------------------------------|
|  5  | EMS Configuration             |
|-----|-------------------------------|
|  e  | Exit                          |
\-------------------------------------/
```

SNMP Global Mode

EPAP supports three SNMP global modes: SNMPv2c, SNMPv3, and both. The EPAP user is able to update or view the global mode in the menu by choosing option **1**).

Figure 5-31 SNMP Global Mode Menu

```
 /-----EPAP SNMP Global Mode Menu-\
/-----------------------------------\
|  1 | Display Global Mode          |
|----|------------------------------|
|  2 | Update  Global Mode          |
|----|------------------------------|
|  e | Exit                         |
\-----------------------------------/
```

Update SNMP Global Mode Menu

The EPAP user is able to update the global mode using option 2.

Figure 5-32 Update SNMP Global Mode Menu

```
 /-----EPAP Update SNMP Global Mode Menu-\
/-----------------------------------------\
|  1 | SNMPv3                             |
|----|------------------------------------|
|  2 | SNMPv2c                            |
|----|------------------------------------|
|  3 | Both                               |
|----|------------------------------------|
|  e | Exit                               |
\-----------------------------------------/
```

If SNMPv2c (option **2**) mode is enabled, then EPAP only supports SNMPv2c:

- EPAP forwards SNMPv2c format traps only to the configured EMS(s) that support v2c.
- EPAP only allows the addition of any new EMS supporting v2c to be configured. Existing EMS(s) are prohibited from modification to support v3.
- Prior to the mode change to SNMPv3 only, all configured EMS(s) supporting v2c will be removed.

If SNMPv3 (option **1**) mode is enabled (recommended), then the EMS only supports SNMP version 3:

- EPAP forwards SNMPv3 format traps only to the configured EMS(s) that support v3.
- EPAP only allows the addition of any new EMS supporting v3 to be configured. Existing v3-supporting EMS(s) are prohibited modification to support v2c.
- Prior to the mode change to SNMPv2c ONLY, all configured EMS(s) supporting v3 will be removed.

If Both (option **3**) mode is enabled, then EPAP supports both SNMPv2c and SNMPv3.

- EPAP forwards traps to all the configured EMS(s) that support v2c or v3.
- EPAP allows the addition of new or updated EMS(s) supporting v2c or v3.

SNMPv3 Access View Configuration Menu

To support View-Based Access Control Mode for SNMPv3, **View Configuration**, option **2** under the SNMP Configuration menu, supports sub-menus **Add, Delete, Update, Display** in order to manage Access Views. The View menu is only accessible if SNMP Global Mode is configured as SNMPv3 ONLY or Both. If SNMPv2c only mode is enabled and the EPAP user tries to access the View menu, the "Error: SNMPv3 View must NOT be configured for SNMP v2c Mode" is displayed.

Figure 5-33 View Configuration Menu

```
 /-----EPAP View Configuration Menu-\
/-------------------------------------\
|  1  | Display SNMPv3 View           |
|-----|-------------------------------|
|  2  | Add SNMPv3 View               |
|-----|-------------------------------|
|  3  | Update SNMPv3 View            |
|-----|-------------------------------|
|  4  | Delete SNMPv3 View            |
|-----|-------------------------------|
|  e  | Exit                          |
\-------------------------------------/
```

The EPAP user is able to add a new View using option **2** under the **View Configuration** menu, as displayed in Figure 5-34. The default view is not be shown during add/update/delete, as no write operation is allowed on it.

Figure 5-34 Add SNMPv3 View

```
Enter Choice: 2

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

Enter View Name: snmpv3view
Enter OID: 1

snmpd.conf file is updated .Please start EPAP services to start snmp processes.

View Name [snmpv3view] has been added.

Press return to continue...
```

The EPAP user is able to display the configured View using option **1** of the **View Configuration** menu, as displayed in Figure 5-35:

Figure 5-35 Display SNMPv3 View

```
Enter Choice: 1


List of Configured Views.

View Name: resyncVarView
OID: 1.3.6.1.4.1.323.5.3.20.2.1.1

View Name: snmpv3view
OID: 1

Press return to continue...
```

The EPAP user is able to update the configured View using option **3** under the **View Configuration** menu, as displayed in Figure 5-36. The already configured OID associated with corresponding view name is shown in square brackets:

Figure 5-36 Update SNMPv3 View

```
Enter Choice: 3

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

List of Configured Views.

View Name: resyncVarView

View Name: snmpv3view

Enter View Name that needs to be updated: snmpv3view
Enter OID [2]: 1

snmpd.conf file is updated .Please start EPAP services to start snmp processes.

View Name [snmpv3view] has been updated.

Press return to continue...
```

The EPAP user is able to delete the view using option **4** under the **View Configuration** menu, as displayed in Figure 5-37:

Figure 5-37 Delete SNMPv3 View

```
Enter Choice: 4

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

List of Configured Views.

View Name: resyncVarView

View Name: snmpv3view2

View Name: snmpv3view

Enter View Name to be deleted: snmpv3view2

snmpd.conf file is updated .Please start EPAP services to start snmp processes.

View Name [snmpv3view2] has been deleted.

Press return to continue...
```

Note:

- View name is non-empty and unique.
- The length of View name cannot be more than 32 characters.
- View Name contains only alphanumeric characters and is case insensitive when being configured.
- OID to be associated with the View is mandatory.
- A View that is associated to any group cannot be deleted.

SNMPv3 Group Management

To support User-Based Security Mode for SNMPv3, **Group Configuration**, option **3** under the SNMP Configuration menu, supports sub-menus **Add, Delete, Update, Display** in order to manage Groups. The Group menu is only accessible if SNMP Global Mode is configured as SNMPv3 ONLY or Both. If SNMPv2c only mode is enabled and the EPAP user tries to access the Group menu, the "Error: SNMPv3 Group must NOT be configured for SNMP v2c Mode" is displayed.

Figure 5-38 Group Configuration Menu

```
 /-----EPAP Group Configuration Menu-\
/-------------------------------------\
|  1  | Display SNMPv3 Group           |
|-----|--------------------------------|
|  2  | Add SNMPv3 Group               |
|-----|--------------------------------|
|  3  | Update SNMPv3 Group            |
|-----|--------------------------------|
|  4  | Delete SNMPv3 Group            |
|-----|--------------------------------|
|  e  | Exit                           |
\-------------------------------------/
```

The EPAP user is able to add a new Groups using option **2** under the **Group Configuration** menu, as displayed in Figure 5-39. The default value of the security level "AuthPriv" is shown in square brackets:

Figure 5-39 Add SNMPv3 Group

```
Enter Choice: 2

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

Enter Group Name: snmpv3group
Enter Security Level[AuthPriv]: AuthNoPriv
Enter Read View: snmpv3view
Enter Write View: snmpv3view

snmpd.conf file is updated.Please start EPAP services to start snmp processes.

Group Name [snmpv3group] has been added.

Press return to continue...
```

The EPAP user is able to display the configured Group using option **1** of the **Group Configuration** menu, as displayed in Figure 5-40:

Figure 5-40 Display SNMPv3 Group

```
Enter Choice: 1


List of Configured Groups.
Group Name: snmpv3group
Security Level: AuthNoPriv
Read View Name: snmpv3view
Write View Name: snmpv3view


Group Name: snmpv3group2
Security Level: AuthPriv
Read View Name: snmpv3view
Write View Name: snmpv3view



Press return to continue...
```

The EPAP user is able to update the configured Groups using option **3** under the **Group Configuration** menu, as displayed in Figure 5-41. The already configured security level related to the corresponding Group is shown in square brackets; however, the read and write view is not shown in square brackets, as these are allowed to be empty:

Figure 5-41 Update SNMPv3 Group

```
Enter Choice: 3

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

List of Configured Groups.

Group Name: snmpv3group

Group Name: snmpv3group2

Enter Group Name that needs to be updated: snmpv3group
Enter Security Level [AuthNoPriv]: AuthPriv
Enter Read View: snmpv3view
Enter Write View: snmpv3view

snmpd.conf file is updated.Please start EPAP services to start snmp processes.

Group Name [snmpv3group] has been Updated.Users configured with this group must be reconfigured to match the new security level before restarting SNMP proces
s.

Press return to continue...
```

The EPAP user is able to delete the Groups using option **4** under the **Group Configuration** menu, as displayed in Figure 5-42:

Figure 5-42 Delete SNMPv3 Group

```
Enter Choice: 4

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

List of Configured Groups.

Group Name: snmpv3group

Group Name: snmpv3group2

Enter Group Name to be deleted: snmpv3group2

snmpd.conf file is updated.Please start EPAP services to start snmp processes.

Group Name [snmpv3group2] has been deleted.

Press return to continue...
```

Note:

- Group name is non-empty and unique.
- The length of Group name cannot be more than 32 characters.
- View Name must contain only alphanumeric characters and is case insensitive when configured; however, during update, Group name is case sensitive.
- Security Level is mandatory. Valid values are noAuthNoPriv, AuthNoPriv, and AuthPriv.
- Read View is optional. Specify the View name spelled exactly as configured in the View Menu if added.
- Read View is configured if it is to be added to the Group.
- Write View is optional. Specify the View name spelled exactly as configured in the View Menu if added.
- Write View is configured if it is to be added to the Group
- A Group that associated to any user cannot be deleted.

SNMPv3 User Management

To support User-Based Security Mode for SNMPv3, **User Configuration**, option **4** under the SNMP Configuration menu, supports sub-menus **Add, Delete, Update, Display** in order to manage Users. The User menu is only accessible if SNMP Global Mode is configured as SNMPv3 ONLY or Both. If SNMPv2c only mode is enabled and the EPAP user tries to access the User menu, the "Error: SNMPv3 User must NOT be configured for SNMP v2c Mode" is displayed.

Figure 5-43 User Configuration Menu

```
 /-----EPAP User Configuration Menu-\
/-------------------------------------\
|  1  | Display SNMPv3 User           |
|-----|-------------------------------|
|  2  | Add SNMPv3 User               |
|-----|-------------------------------|
|  3  | Update SNMPv3 User            |
|-----|-------------------------------|
|  4  | Delete SNMPv3 User            |
|-----|-------------------------------|
|  e  | Exit                          |
\-------------------------------------/
```

The User sub-menus are able to configure a user name, a group, and optional Privacy Protocol, Privacy Password, Authentication Protocol, and Authentication Password, depending on the security level configured for the chosen Group.

The EPAP services will be stopped through an interactive prompt menu every time the EPAP user initiates Add, Delete, or Update Group configuration.

The EPAP user is able to add a new User using option **2** under the **User Configuration** menu, as displayed in Figure 5-44. The password information is not visible to the EPAP user. The default value of the Authentication Protocol and Privacy Protocol will be shown in square brackets while adding a new User:

Figure 5-44 Add SNMPv3 User

```
Enter Choice: 2

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

Enter User  Name: snmpv3user
Enter Group name : snmpv3group
Enter Authentication Protocol [SHA]: SHA
Enter Authentication Password:
Re-enter Authentication Password:
Enter Privacy Protocol [DES]: DES
Enter Privacy Password:
Re-enter Privacy Password:

snmpd.conf file is updated.Please start EPAP services to start snmp processes.

User Name [snmpv3user] has been added.

Press return to continue...
```

The **Add SNMPv3 User** is configured based on Group configuration. First, the Group Name values are validated against the Group configured. If no valid Group is found, the Add step fails with a corresponding error message. If the Group entered is validated, then the menu lists only the valid fields corresponding to the Group entered. If the security level configured for the chosen group is 'noAuthNoPriv', then the input fields for Authentication Protocol, Authentication Password, Privacy Protocol, and Privacy password will not be displayed. If the security level

configured for the chosen group is 'AuthNoPriv', the input fields Priv Protocol and Priv Password will not be displayed. By default, DES is selected for the addition of a new User for an AuthPriv scenario.

The EPAP user is able to display the configured Users using option **1** of the **User Configuration** menu, as displayed in Figure 5-45. The password information for the authentication protocol and privacy protocol is not displayed:

Figure 5-45 Display SNMPv3 User

```
Enter Choice: 1


List of Configured Users.
User Name : snmpv3user
Group Name: snmpv3group
Authentication  Protocol: SHA
Privacy Protocol: DES

User Name : snmpv3user2
Group Name: snmpv3group
Authentication  Protocol: SHA
Privacy Protocol: DES


Press return to continue...
```

The EPAP user is able to update the configured Users using option **3** under the **User Configuration** menu, as displayed in Figure 5-46. The parameters already configured for the corresponding user will be shown in square brackets:

Figure 5-46 Update SNMPv3 User

```
Enter Choice: 3

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

List of Configured Users.

User Name : snmpv3user

User Name : snmpv3user2

Enter User  Name that needs to be updated: snmpv3user2
Enter Group Name  [snmpv3group]: snmpv3group2
Enter Authentication Protocol [SHA]: SHA
Enter Authentication Password:
Re-enter Authentication Password:
Enter Privacy Protocol [DES]: DES
Enter Privacy Password:
Re-enter Privacy Password:

snmpd.conf file is updated.Please start EPAP services to start snmp processes.

User Name [snmpv3user2] has been updated.

Press return to continue...
```

The EPAP user is able to delete the Usersroups using option **4** under the **User Configuration** menu, as displayed in Figure 5-47:

Figure 5-47 Delete SNMPv3 User

```
Enter Choice: 4

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

List of Configured Users.

User Name : snmpv3user

User Name : snmpv3user2

Enter User Name to be deleted: snmpv3user2

snmpd.conf file is updated.Please start EPAP services to start snmp processes.

User Name [snmpv3user2] has been deleted.

Press return to continue...
```

Note:

- Group name is non-empty and unique.
- The length of Group name cannot be more than 32 characters.
- User Name must contain only alphanumeric characters and is case insensitive when configured.
- Group must have been configured if it is to be added to the User.
- Group must be spelled in the exact case as configured in the Group menu.
- If the security level configured for the chosen group is 'noAuthNoPriv', then the input to Authentication Protocol, Authentication Password, Privacy Protocol and Privacy Password fields will not be displayed.
- If the security level configured for the chosen group is 'AuthNoPriv', then it is required to input the desired value for Authentication Protocol and provide a valid password in the Authentication Password field. The input to Privacy Protocol and Privacy Password fields are not required.
- If the security level configured for the chosen group is 'AuthPriv', then it is required to select the desired values for Authentication Protocol and Privacy Protocol fields and provide valid passwords in the Authentication Password and Privacy Password fields.
- Valid values for Auth Protocol is SHA as the default.
- Valid values for Priv Protocol are DES and AES; DES is the default.
- Auth and Priv password length must be between 8 and 255 inclusive.
- Auth and Priv password is stored in encrypted form in the DB.
- Only the following alphanumeric characters and special characters are allowed in Auth and Priv passwords: @, #, $, !
- A user associated to any EMS cannot be deleted.
- A default user "oracleuser" is for system use and will not be visible, added, edited, or deleted by customers through this menu.

5.3.9.1 Configure EMS Server

The EMS Configuration option `5` under the **EPAP SNMP Configuration Menu** allows the user to configure the EMS server using either an IPv4 or IPv6 address. The User Configuration sub-menus can be configured with an EMS host name, IP, Port, Heart Beat in seconds, and either Community or User, depending on the global mode set in SNMP Global Mode. If the Global Mode is SNMPv2c ONLY, the input field "User" will not be displayed.

The EPAP supports the configuration of maximum 5 EMS Servers. The EPAP supports the configuration of multiple EMS Servers with a mix of IPv4 and IPv6 IPs with which to interact to send the alarms to send as traps. See Figure 5-30 for the option `5` output.

Figure 5-48 Configure EMS Server

```
 /-----EPAP Configure EMS Server Menu-\
/--------------------------------------\
|  1 | Display EMS Server              |
|----|---------------------------------|
|  2 | Add EMS Server                  |
|----|---------------------------------|
|  3 | Update EMS Server               |
|----|---------------------------------|
|  4 | Delete EMS Server               |
|----|---------------------------------|
|  e | Exit                            |
\--------------------------------------/
```

Display EMS Server

Configure EMS Server Menu option **1** displays all configured EMS servers. For PROV/Non PROV EPAP, the display operation displays the values of the fields shown in Figure 5-49. For PDB_ONLY EPAP, all fields except the StatusB field are displayed:

Figure 5-49 Display EMS Configuration for PROV/Non-PROV Server

```
Enter Choice: 1


EMS IP Address: 192.168.59.32
EMS Server Name: snmpv3ems
EMS Port: 178
SNMP Version: SNMPv3
Username: snmpv3user
Heartbeat Interval: 80
StatusA: NORMAL
StatusB: NORMAL
Timestamp: 2016-07-31 23:16:08
```

Figure 5-50 Display EMS Configuration for PDBonly EPAP

```
Enter Choice: 1


EMS IP Address: 192.168.59.8
EMS Server Name: snmpv3ems
EMS Port: 172
SNMP Version: SNMPv3
Username: snmpv3user
Heartbeat Interval: 67
Status: NORMAL
Timestamp: 2016-08-02 02:37:51
```

Add EMS Server

Configuration EMS Server Menu option **2** allows the addition of EMS servers:

- The user is allowed to configure IPv4 only remote system address
- The user is allowed to configure IPv6 only remote system address
- On dual stack - the user is allowed to configure IPv4 or IPv6 remote system address

EMS IP Address
IP address of EMS to receive traps

EMS Server Name
A logical name for the EMS

EMS Port
Destination UDP port

EMS Community
SNMP community contained in traps

Heartbeat Interval [60]
Number of seconds between heartbeat traps (system alive message); the default is 60 seconds if not specified

Figure 5-51 and Figure 5-52 display examples of adding IPv4 SNMPv2c EMS servers:

> **Note:**
>
> IPv6 Configuration, menu option **2**, follows the same procedures as IPv4 for adding EMS servers.

Figure 5-51 Add IPv4 SNMPv2c EMS When Global Is Set to Both for PROV/Non-PROV EPAP

```
 /----- Add EMS Menu-----\
/-------------------------\
|  1 | IPv4 Configuration |
|----|--------------------|
|  2 | IPv6 Configuration |
|----|--------------------|
|  e | Exit               |
\-------------------------/

Enter Choice: 1

Verifying root connectivity with mate...
EPAP software is running.  Stop it? [N]: Y
EPAP software is running on mate MPS.  Stop it? [N]: Y

EMS SNMP Version(V2c/V3): V2c
EMS IP Address: 192.168.60.9
EMS Server Name: snmpv2cems
EMS Port: 167
EMS Community: public
Heartbeat Interval [60]: 50

EMS Server [192.168.60.9] has been added.
```

Figure 5-52 Add IPv4 SNMPv2c EMS When Global Mode Is Set to Both for PDBOnly EPAP

```
Enter Choice: 1

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

EMS SNMP Version(v2c/v3): v2c
EMS IP Address: 10.250.32.244
EMS Server Name: emsServer
EMS Port: 162
EMS Community: public
Heartbeat Interval [60]: 60

EMS Server [10.250.32.244] has been added.Please start EPAP services to start snmp processes.

Press return to continue...
```

and display examples of adding IPv4 SNMPv3 EMS servers:

Figure 5-53 Add IPv4 SNMPv3 EMS When Global Mode Is Set to Both for PROV/Non-PROV EPAP

```
Enter Choice: 1

Verifying root connectivity with mate...
EPAP software is running.  Stop it? [N]: Y
EPAP software is running on mate MPS.  Stop it? [N]: Y

EMS SNMP Version(V2c/V3): V3
EMS IP Address: 192.168.56.3
EMS Server Name: snmpv3ems
EMS Port: 176
EMS Username: snmpv3user
Heartbeat Interval [60]: 45

EMS Server [192.168.56.3] has been added.
```

Figure 5-54 Add IPv4 SNMPv3 EMS When Global Mode Is Set to Both for PDBOnly EPAP

```
Enter Choice: 1

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

EMS SNMP Version(v2c/v3): v3
EMS IP Address: 10.250.32.244
EMS Server Name: emsServer
EMS Port: 162
EMS Username: snmpv3user
Heartbeat Interval [60]: 30

EMS Server [10.250.32.244] has been added.Please start EPAP services to start snmp processes.

Press return to continue...
```

Update EMS Server

Configure EMS Server Menu option **3** allows the update of the EMS Server Name, EMS Port, EMS Community, and Heartbeat Interval fields for an EMS server IP address entered by the user, as displayed in .

Figure 5-55 Update EMS Configuration for PROV/Non-PROV EPAP When Global Mode Is SNMPv3

```
 /-----EMS Update Menu---\
/-------------------------\
|  1 | IPv4 Configuration |
|----|--------------------|
|  2 | IPv6 Configuration |
|----|--------------------|
|  e | Exit               |
\-------------------------/

Enter Choice: 1

Verifying root connectivity with mate...

EMS IP Address: 192.168.60.3
EMS Server Name: snmpv3ems
EMS Port: 162
SNMP Version: SNMPv3
Username: snmpv3user9
Heartbeat Interval: 60
StatusA: NORMAL
StatusB: NORMAL
Timestamp: 2016-09-01 05:20:57

EMS Server IP Address whose fields need to be updated : 192.168.60.3
EMS Server Name [snmpv3ems]:
EMS Port [162]: 163
EMS Username [snmpv3user9]:
Heartbeat Interval [60]: 45

EMS Server [192.168.60.3] has been updated.
```

Figure 5-56 Update EMS Configuration for PDBOnly EPAP When Global Mode Is Both

```
 /-----EMS Update Menu---\
/-------------------------\
|  1 | IPv4 Configuration |
|----|--------------------|
|  2 | IPv6 Configuration |
|----|--------------------|
|  e | Exit               |
\-------------------------/

Enter Choice: 1

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

EMS IP Address: 10.250.32.244
EMS Server Name: emsServer
EMS Port: 162
SNMP Version: SNMPv3
Username: snmpv3user
Heartbeat Interval: 30
Status: NORMAL
Timestamp: 2016-10-27 02:43:36

EMS Server IP Address whose fields need to be updated : 10.250.32.244
EMS SNMP Version(v2c/v3) [v3]: v3
EMS Server Name [emsServer]: EMSserverName
EMS Port [162]: 162
EMS Username [snmpv3user]: snmpv3user
Heartbeat Interval [30]: 60

EMS Server [10.250.32.244] has been updated.Please start EPAP services to start snmp processes.

Press return to continue...
```

Delete EMS Server

Configure EMS Server Menu option **4** allows the deletion of the EMS server, as displayed in.

Figure 5-57 Delete EMS Configuration for PROV/Non-PROV

```
Enter Choice: 4

Verifying root connectivity with mate...

EMS IP Address: 192.168.59.32
EMS Server Name: snmpv3ems
EMS Port: 178
SNMP Version: SNMPv3
Username: snmpv3user
Heartbeat Interval: 80
StatusA: NORMAL
StatusB: NORMAL
Timestamp: 2016-07-31 23:16:08

EMS Server IP Address to be deleted: 192.168.59.32

EMS Server [192.168.59.32] has been deleted.
```

Figure 5-58 Delete EMS Configuration for PDBonly EPAP

```
Enter Choice: 4

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

EMS IP Address: 1.2.3.4
EMS Server Name: emsServer
EMS Port: 162
SNMP Version: SNMPv3
Username: snmpv3user
Heartbeat Interval: 60
Status: NORMAL
Timestamp: 2016-10-27 02:13:52

EMS IP Address: 1.23.4.5
EMS Server Name: emsServer
EMS Port: 123
SNMP Version: SNMPv3
Username: snmpv3user
Heartbeat Interval: 60
Status: NORMAL
Timestamp: 2016-10-27 02:17:35

EMS IP Address: 10.250.32.244
EMS Server Name: EMSserverName
EMS Port: 167
SNMP Version: SNMPv2c
EMS Community: private
Heartbeat Interval: 30
Status: NORMAL
Timestamp: 2016-10-27 02:23:00

EMS Server IP Address to be deleted: 10.250.32.244

EMS Server [10.250.32.244] has been deleted.Please start EPAP services to start snmp processes.

Press return to continue...
```

Note:

- Name is the logic name for the EMS server with a valid length of 5 to 20 characters; Name is mandatory for both v3 and v2c configuration.
- Name must contain only alphanumeric characters (underscore is allowed) and is case insensitive when being configured.
- IP must be non-empty and unique. Both IPv4 and IPv6 EMS are supported.
- Port must be a valid value between range 1 to 65535, excluding the pre-defined ports.
- HeartBeat must be non-empty and in between a valid range of 0, 5 - 7200 for v3 configuration.
- Community String length cannot exceed 127 characters.
- Only alphanumeric characters, hyphen and underscore are allowed in Community.
- If Global Mode is set to SNMPv2c, the Community field is mandatory and the User field will not be displayed.
- If Global Mode is set to SNMPv3, the Community field will not be displayed and the User field is mandatory.
- User must be spelled in the exact case as it is configured in the User menu when being configured; If Global Mode is set to Both, either v2c or v3 "SNMP Version" will be selected. Community and User are mutually exclusive.

5.3.9.2 Autonomous Events Trap Forwarding

The EPAP SNMP agent forwards all autonomous events generated at the EPAP in the form of SNMP v2c traps to EMS(s) configured for SNMPv2c, or SNMPv3 traps to those configured for SNMPv3. One thread runs per EMS, which maintains its own head and tail to send the alarms to the SNMPv2c configured EMS or the SNMPv3 configured EMS. Trap forwarding from the EPAP to the SNMPv3 based EMS will remain the same, as in the case of SNMPv2c based EMS(s), except that the trap PDU will carry additional information related to USM entry for the EMS.

5.3.9.3 Connectivity Between EPAP and EMS

EPAP listens at the SNMP agent standard port "161" for SET/GET Message. On receiving GET/SET message, EPAP sends a response for the same at a configured destination port for EMS. EPAP sends SNMPv2c/SNMPv3 traps to the EMS at some port, which is configured by the user for that EMS server with the help of the `epapconfig` utility. A maximum of 5 EMSs can be connected to an EPAP.

5.3.9.4 Resynchronization

The resynchronization process is supported for both SNMPv2c and SNMPv3 EMS servers.

If any EMS (either SNMPv2c or SNMPv3) sends a SET request to EPAP (that sets object value of resyncVar to 1), then only that EMS will be resynchronized with EPAP. Incase all EMS(s) send a SET request to the EPAP, then resynchronization takes place for every EMS independently.

5.3.10 Configure Alarm Feed

The Configure Alarm Feed option `11` allows the user to configure the `Eagle Alarm Feed` and `SNMP Alarm Feed` parameters. For PROV/Non PROV EPAP (see Figure 5-59), the EPAP software is stopped in both the EPAP A and EPAP B servers before configuring the alarm feeds.

Figure 5-59 Alarm Feed Configuration Menu for PROV/Non PROV EPAP

```
Enter Choice: 11

Verifying root connectivity with mate...
Configure Eagle Alarm Feed [ON]:
Configure SNMP Alarm Feed [ON]:

Successfully configured Eagle Alarm Feed and SNMP Alarm Feed.

Press return to continue...
```

As shown in Figure 5-60, the `Eagle Alarm Feed` parameter is not configurable for PDB_ONLY EPAP. The EPAP software is stopped in the EPAP A server before configuring the alarm feed.

Figure 5-60 Alarm Feed Configuration Menu for PDB_ONLY EPAP

```
Enter Choice: 11

EPAP software is running.  Stop it? [N]: Y
Configure SNMP Alarm Feed [ON]:

Successfully configured SNMP Alarm Feed.

Press return to continue...
```

5.3.11 Configure Query Server

The Configure Query Server option `12` allows the user to configure the query server on EPAP, as shown in Figure 5-61, using either IPv4 or IPv6 addresses.

- The user is allowed to configure IPv4 only remote system address
- The user is allowed to configure IPv6 only remote system address
- On dual stack - the user is allowed to configure IPv4 or IPv6 remote system address

If no query server is configured, the MySQL `binlogs` are purged when the free disk space usage is more than the value set for `epap_binlogs_threshold`. The default value for `epap_binlogs_threshold` is 80%.

> **Note:**
>
> All Query Server related logs will be logged in the queryServer.log file @ /usr/TKLC/epap/logs. This logging includes configuration via the epapconfig menu, connectivity status of the Query Server, and alarms related to the Query Server on EPAP.

The following options are available in the epapconfig utility under the "Configure Query Server" tab:

1. Display Query Server Status
2. Add Query Server
3. Remove Query Server
4. Make Snapshot

Figure 5-61 Configure Query Server

```
MPS Side A:  hostname: epaprpi  hostid: a8c02d3d
             Platform Version: 4.0.10-5.5.1_75.20.0
             Software Version: EPAP 161.0.1-16.1.0_161.2.0
             Thu Apr  9 01:31:41 EDT 2015

 /-----EPAP Configure Query Server Menu-\
/----------------------------------------\
|   1 | Display Query Server Status      |
|-----|----------------------------------|
|   2 | Add Query Server                 |
|-----|----------------------------------|
|   3 | Remove Query Server              |
|-----|----------------------------------|
|   4 | Make Snapshot                    |
|-----|----------------------------------|
|   e | Exit                             |
\----------------------------------------/

Enter Choice: 2
```

Display Query Server Status

The Display Query Server Status option 1 displays the query server configured at the EPAP side, as shown in Figure 5-62.

Figure 5-62 Display Query Server Status

```
Enter Choice: 1

Query Server List

10.248.9.11


Press return to continue...
```

Add Query Server

The Add Query Server option 2 adds a query server at EPAP. As shown in Figure 5-63, the following parameters are configurable for a query server:

- IP address of the query server
- Password needed for replication user

Figure 5-63 Add Query Server

```
MPS Side A:  hostname: epaprpi  hostid: a8c02d3d
             Platform Version: 4.0.10-5.5.1_75.20.0
             Software Version: EPAP 161.0.1-16.1.0_161.2.0
             Thu Apr  9 01:31:46 EDT 2015

 /-----Add Query Server Menu-\
/-----------------------------\
|   1 | IPv4 Configuration     |
|----|------------------------|
|   2 | IPv6 Configuration     |
|----|------------------------|
|   e | Exit                   |
\-----------------------------/

Enter Choice: 2


Query Server IPv6 Address: 2606:b400:605:b80b:200:17ff:fe0f:2893
Query Server Password:
```

Remove Query Server

The Remove Query Server option 3 removes the query server configured at EPAP, as shown in Figure 5-64.

Figure 5-64 Remove Query Server

```
MPS Side A:  hostname: epaprpi  hostid: a8c02d3d
             Platform Version: 4.0.10-5.5.1_75.20.0
             Software Version: EPAP 161.0.1-16.1.0_161.2.0
             Thu Apr  9 01:34:15 EDT 2015

 /-----EPAP Configure Query Server Menu-\
/----------------------------------------\
|  1 | Display Query Server Status       |
|----|-----------------------------------|
|  2 | Add Query Server                  |
|----|-----------------------------------|
|  3 | Remove Query Server               |
|----|-----------------------------------|
|  4 | Make Snapshot                     |
|----|-----------------------------------|
|  e | Exit                              |
\----------------------------------------/

Enter Choice: 3

Query Server List

10.248.11.2
Replication User IP Address which needs to be deleted: 2606:b400:605:b80b:200:17ff:fe0f:2893
```

Make Snapshot

The Make Snapshort option `4` creates a snapshot of the EPAP PDB, as shown in Figure 5-65.

Figure 5-65 Make Snapshot

```
Enter Choice: 4


WARNING: This command may cause a brief interruption in traffic being sent
provisioning may be INTERRUPTED.

Do you want to continue? [Y/N]Y
Created snapinfo.sql file successfully.

Creating Snapshot...
```

5.3.12 Configure Query Server Alarm Feed

The Configure Query Server Alarm Feed option `13` allows the user to turn on or turn off the Query Server Alarm Feed, as shown in Figure 5-66.

Figure 5-66 Configure Query Server Alarm Feed

```
Enter Choice: 13

Configure Query Server Alarm Feed [ON]:

Successfully configured Query Server Alarm Feed.

Press return to continue...
```

When the Query Server Alarm Feed is set to ON, the **EPAP QS Replication Issue** and **EPAP QS Lagging behind** alarms can be raised in the system according to their alarm condition.

5.3.13 Configure SNMP Agent Community

The Configure SNMP Agent Community option `14` allows the user to configure the SNMP Read and Write Communities in the snmpd.conf file, as shown in Figure 5-67 and Figure 5-68. The default strings for the Read and Write communities in the snmpd.conf file are epapRdSnmp and epapWrSnmp.

Figure 5-67 Configure SNMP Agent Community Menu for PROV/Non PROV EPAP

```
Enter Choice: 14

SNMP Read Community: epapSnmpComm
SNMP Write Community: epapSnmpWComm

Read and Write Community updated in config file. SNMP Daemon started, now starting on mate server.

Press return to continue...

SNMP Agent Community configured on mate successfully.

Press return to continue...
```

Figure 5-68 Configure SNMP Agent Community Menu for PDB_ONLY EPAP

```
Enter Choice: 14

SNMP Read Community: epapRdComm
SNMP Write Community: epapWrComm

Read and Write Community updated in config file. SNMP Daemon started.

Press return to continue...
```

5.3.14 Configure Mate Disaster Recovery

Mate Disaster Recovery, menu option **15**, performs disaster recovery on Mixed/Non-prov EPAP. Choosing this option allows for the entire disaster recovery process to be an authenticated procedure. Instead of re-installing the EPAP on both servers and redoing the configuration steps, the EPAP user is able to IPM only the bad server, install EPAP on it, and perform disaster recovery from the mate.

> **Note:**
>
> - This menu option is not supported on PDBonly setup.
> - The menu option **15** does not work if VIP is configured on the server. To use this menu option remove the VIP configuration.

Figure 5-69 EPAP Configuration Menu on Server A

```
/-------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                          |
|----|-----------------------------------|
| 10 | SNMP Configuration                |
|----|-----------------------------------|
| 11 | Configure Alarm Feed              |
|----|-----------------------------------|
| 12 | Configure Query Server            |
|----|-----------------------------------|
| 13 | Configure Query Server Alarm Feed |
|----|-----------------------------------|
| 14 | Configure SNMP Agent Community    |
|----|-----------------------------------|
| 15 | Mate Disaster Recovery            |
|----|-----------------------------------|
|  e | Exit                              |
\---------------------------------------/
Enter Choice: 15
```

Figure 5-70 EPAP Configuration Menu on Server B

```
/-------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 | Security                         |
|----|----------------------------------|
|  9 | SNMP Configuration               |
|----|----------------------------------|
| 10 | Configure Alarm Feed             |
|----|----------------------------------|
| 11 | Configure SNMP Agent Community   |
|----|----------------------------------|
| 12 | Mate Disaster Recovery           |
|----|----------------------------------|
|  e | Exit                             |
\-------------------------------------/
Enter Choice: 12
```

> **Note:**
>
> Once the user initiates Disaster Recovery, all the services are stopped on EPAP.

After selecting menu option **15** from A Server or option **12** from B server, a prompt to confirm Mate Recovery will be displayed. On approval, the user will be asked to provide a password for key exchange, after which configuration for Mate Recovery will start:

```
Enter Choice: 12
WARNING: Are you sure you want to run Disaster Recovery on Mate? [N]: Y
Exchanging Keys with Mate...
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.
Password of admusr:
Could not get authorized keys file from remote (mate).
Maybe it does not exist. Continuing...
ssh is working correctly.
Password of root:
ssh is working correctly.
```

After completion, the user must reconfigure the cron jobs (autobackup, PDB/RTDB) that were previously set. This information will be lost during Disaster Recovery.

If Server A goes down on a mixed setup and the Query Server was configured before Disaster Recovery, the user must reconfigure the Query Server as well, as this information will be lost along with the PDB database.

> **Note:**
>
> If disaster recovery is performed on a server having a backup-prov IP, the syscheck may retain the backup-prov IP and throw the error “Could not ping IPv4/IPv6 host mate-prov-bkup”. To prevent this error, remove the configured backup-prov IP and reconfigure it with the same backup-prov IP after completing the disaster recovery procedure. This removes the default IP from /etc/hosts and clears the syscheck alarm.

5.3.15 DB Architecture Menu

The epapconfig menu supports a **DB Architecture** sub-menu, option `15`, which allows the DB Architecture to be changed from the default "Compact" to "eXtreme."

Figure 5-71 EPAP B 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                          |
|----|-----------------------------------|
| 10 | SNMP Configuration                |
|----|-----------------------------------|
| 11 | Configure Alarm Feed              |
|----|-----------------------------------|
| 12 | Configure Query Server            |
|----|-----------------------------------|
| 13 | Configure Query Server Alarm Feed |
|----|-----------------------------------|
| 14 | Configure SNMP Agent Community    |
|----|-----------------------------------|
| 15 | DB Architecture Menu              |
|----|-----------------------------------|
|  e | Exit                              |
\---------------------------------------/
```

```
Enter Choice:15



/-----DB Architecture Menu-------------\
/---------------------------------------\
|  1 | Display running DB Architecture   |
|----|-----------------------------------|
|  2 | Change DB Architecture to eXtreme |
|----|-----------------------------------|
|  e | Exit                              |
\---------------------------------------/
```

In the default "Compact" DB Architecture, the EPAP will run the version of RTDB and MAINT processes that are compatible with EAGLE 46.5 and 46.6.

> **Note:**
>
> The "PDB Capacity Menu" will not be displayed in the "Compact" DB Architecture.

Changing the DB Architecture from "Compact" to "eXtreme" requires the EPAP software to restart and run a new version of RTDB and MAINT process to support the capacity expansion. The connecting EAGLE must upgrade to the new release with SLIC cards running 64-bit SCCP applications in order to support this DB schema before the change. SM8G-B cards are not supported in the "eXtreme" DB architecture.

5.4 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 using 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 *Application B Card Hardware and Installation Guide*. Various internal configuration parameters are also set to their default values. The installer must perform initial configuration on MPS A on EAGLE A and MPS A on EAGLE B. The installer must also perform initial configuration on non-provisionable MPSs, if they are present.

See Standalone PDB EPAP for the procedure to configure Standalone PDB EPAPs.

5.4.1 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 A and MPS A side of EAGLE B. Attempting to perform initial configuration on MPS B of EAGLE 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 A and MPS A on EAGLE 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 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 B, the configuration software executing at EAGLE 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 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 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 B.

5.4.2 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** A, an **MPS** on **EAGLE** 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 5-8 Configuration Notations

Notation	Notation Description
A: MPS on EAGLE A:	This notation indicates installation instructions to be performed specifically for the **MPSs** (**MPS** A and **MPS** B) on **EAGLE** A.
B: MPS on EAGLE B:	This notation indicates installation instructions to be performed specifically for the **MPSs** (**MPS** A and **MPS** B) on **EAGLE** B.
N: Non-Provisionable MPS:	This notation indicates installation instructions to be performed specifically for any non-provisionable **MPSs**.

5.4.3 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 *Application B Card Hardware and Installation Guide* for the correct installation procedure.

5.4.4 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 A to configure it, then use `ssh` to connect to the MPS at EAGLE B and configure it.

After connecting to the MPS on EAGLE 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 value `n`.

```
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 B:

   The configuration software is now being executed on the MPSs on EAGLE B. While the MPSs on EAGLE 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 Configuration Terms and Assumptions.

4. Declare whether the MPS is provisionable or non-provisionable.

   This example shows this MPS as a provisionable MPS.
   A: MPS on EAGLE A:

   Answer `y` in this step.

   B: MPS on EAGLE 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 along with hostname, hostid, Platform Version, Software Version, and the date.

```
/-----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                          |
|----|-----------------------------------|
| 10 | SNMP Configuration                |
|----|-----------------------------------|
| 11 | Configure Alarm Feed              |
|----|-----------------------------------|
| 12 | Configure Query Server            |
|----|-----------------------------------|
| 13 | Configure Query Server Alarm Feed |
```

```
|----|----------------------------------|
| 14 | Configure SNMP Agent Community   |
|----|----------------------------------|
| 15 | DB Architecture Menu             |
|----|----------------------------------|
|  e | Exit                             |
\-----------------------------------------/

Enter Choice:1
```

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 A.

Figure 5-72 Example of Configuration Report When the EPAP is Not Configured

```
EPAP A Provisioning Network IP Address    = Not configured
EPAP A Provisioning Network IP Address v6 = Not configured
EPAP B Provisioning Network IP Address    = Not configured
EPAP B Provisioning Network IP Address v6 = Not configured
Provisioning Network Netmask              = Not configured
Provisioning Network Prefix               = Not configured
Provisioning Network Default Router       = Not configured
Provisioning Network Default Router v6    = Not configured
EPAP A Backup Prov Network IP Address     = Not configured
EPAP A Backup Prov Network IP Address v6  = Not configured
EPAP B Backup Prov Network IP Address     = Not configured
EPAP B Backup Prov Network IP Address v6  = Not configured
Backup Prov Network Netmask               = Not configured
Backup Prov Network Prefix v6             = Not configured
Backup Prov Network Default Router        = Not configured
Backup Prov Network Default Router v6     = 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 IP Version                           = Not configured
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                    = Not configured
Remote Provisioning VIP                   = Not configured
Local PDBA Address                        = 0.0.0.0
Local PDBA Address v6                     = 0000:0000:0000:0000:0000:0000:0000:0000
Remote PDBA Address                       = 0.0.0.0
Remote PDBA B Address                     = Not configured
Time Zone                                 = America/New_York
PDB Database                              = None
Preferred PDB                             = 0.0.0.0
Allow updates from alternate PDB          = Yes
Auto DB Recovery Enabled                  = No
PDBA Proxy Enabled                        = No

Press return to continue...
```

When the EPAP is configured in dual stack configuration, the "EPAP IP Version" is set to "IPv4v6". The **Display Configuration** option displays both the IPv4 and IPv6 network configurations:

Figure 5-73 Display Configuration of EPAP Configured in Dual Stack

```
EPAP A Provisioning Network IP Address    = 10.250.51.149
EPAP A Provisioning Network IP Address v6 = 2606:B400:605:B80D:200:17FF:FE0E:BF8B
EPAP B Provisioning Network IP Address    = 10.250.51.150
EPAP B Provisioning Network IP Address v6 = 2606:B400:605:B80D:200:17FF:FE0E:BF21
Provisioning Network Netmask              = 255.255.255.0
Provisioning Network Prefix               = 64
Provisioning Network Default Router       = 10.250.51.1
Provisioning Network Default Router v6    = FE80::226:98FF:FE1A:9AC1
EPAP A Backup Prov Network IP Address     = Not configured
EPAP A Backup Prov Network IP Address v6  = Not configured
EPAP B Backup Prov Network IP Address     = Not configured
EPAP B Backup Prov Network IP Address v6  = Not configured
Backup Prov Network Netmask               = Not configured
Backup Prov Network Prefix v6             = Not configured
Backup Prov Network Default Router        = Not configured
Backup Prov Network Default Router v6     = 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 IP Version                           = IPv4v6
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                    = Not configured
Remote Provisioning VIP                   = Not configured
Local PDBA Address                        = 10.250.51.149
Local PDBA Address v6                     = 2606:b400:605:b80d:200:17ff:fe0e:bf8b
Remote PDBA Address                       = 192.168.61.48
Remote PDBA B Address                     = 192.168.61.49
Time Zone                                 = America/New_York
PDB Database                              = Exists
Preferred PDB                             = 2606:b400:605:b80d:200:17ff:fe0e:bf8b
Allow updates from alternate PDB          = Yes
Auto DB Recovery Enabled                  = No
PDBA Proxy Enabled                        = No

Press return to continue...
```

In the IPv4 only configuration, the "EPAP IP Version" is set to IPv4. The **Display Configuration** option displays only the IPv4 network configuration. The IPv6 network configuration is be displayed as "Not configured."

Figure 5-74 Display Configuration of EPAP Configured as IPv4 Only

```
EPAP A Provisioning Network IP Address     = 192.168.61.35
EPAP A Provisioning Network IP Address v6 = Not configured
EPAP B Provisioning Network IP Address     = 192.168.61.36
EPAP B Provisioning Network IP Address v6 = Not configured
Provisioning Network Netmask               = 255.255.255.0
Provisioning Network Prefix                = Not configured
Provisioning Network Default Router        = 192.168.61.250
Provisioning Network Default Router v6     = Not configured
EPAP A Backup Prov Network IP Address      = Not configured
EPAP A Backup Prov Network IP Address v6   = Not configured
EPAP B Backup Prov Network IP Address      = Not configured
EPAP B Backup Prov Network IP Address v6   = Not configured
Backup Prov Network Netmask                = Not configured
Backup Prov Network Prefix v6              = Not configured
Backup Prov Network Default Router         = Not configured
Backup Prov Network Default Router v6      = 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 IP Version                            = IPv4
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                     = Not configured
Remote Provisioning VIP                    = Not configured
Local PDBA Address                         = 192.168.61.35
Local PDBA Address v6                      = 0000:0000:0000:0000:0000:0000:0000:0000
Remote PDBA Address                        = Not configured
Remote PDBA B Address                      = Not configured
Time Zone                                  = America/New_York
PDB Database                               = Exists
Preferred PDB                              = Standby
Allow updates from alternate PDB           = Yes
Auto DB Recovery Enabled                   = No
PDBA Proxy Enabled                         = No

Press return to continue...
```

In the IPv6 only configuration, the "EPAP IP Version" is set to IPv6. The **Display Configuration** option displays only the IPv6 network configuration. The IPv4 network configuration is be displayed as "Not configured."

Figure 5-75 Display Configuration of EPAP Configured as IPv6 Only

```
EPAP A Provisioning Network IP Address     = Not configured
EPAP A Provisioning Network IP Address v6  = 2606:B400:605:B80B:200:17FF:FE0F:2884
EPAP B Provisioning Network IP Address     = Not configured
EPAP B Provisioning Network IP Address v6  = 2606:B400:605:B80B:200:17FF:FE0F:2F2C
Provisioning Network Netmask                = Not configured
Provisioning Network Prefix                 = 64
Provisioning Network Default Router         = Not configured
Provisioning Network Default Router v6      = FE80::226:98FF:FE1A:9AC1
EPAP A Backup Prov Network IP Address       = Not configured
EPAP A Backup Prov Network IP Address v6    = Not configured
EPAP B Backup Prov Network IP Address       = Not configured
EPAP B Backup Prov Network IP Address v6    = Not configured
Backup Prov Network Netmask                 = Not configured
Backup Prov Network Prefix v6               = Not configured
Backup Prov Network Default Router          = Not configured
Backup Prov Network Default Router v6       = 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 IP Version                             = IPv6
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                      = Not configured
Remote Provisioning VIP                     = Not configured
Local PDBA Address                          = 0.0.0.0
Local PDBA Address v6                       = 2606:B400:605:B80B:200:17FF:FE0F:2884
Remote PDBA Address                         = 2606:B400:605:B80E:200:17FF:FE0E:A6A1
Remote PDBA B Address                       = 2606:B400:605:B80E:200:17FF:FE0E:A6A5
Time Zone                                   = America/New_York
PDB Database                                = Exists
Preferred PDB                               = Standby
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                           |
|----|------------------------------------|
| 10 | SNMP Configuration                 |
|----|------------------------------------|
| 11 | Configure Alarm Feed               |
|----|------------------------------------|
| 12 | Configure Query Server             |
|----|------------------------------------|
| 13 | Configure Query Server Alarm Feed  |
|----|------------------------------------|
| 14 | Configure SNMP Agent Community     |
|----|------------------------------------|
| 15 | DB Architecture Menu               |
|----|------------------------------------|
|  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 Static NAT Addresses       |
|----|--------------------------------------|
|  6 | 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. 0.0.0.0 is a valid IP address and can be used to reset the VIP/backup provisioning IP address.

Refer to the information recorded in Table 5-1 through Table 5-4 for the correct addresses.

> **Note:**
>
> No default value is provided for the EPAP provisioning network default router. This value must be received from the customer.

The display for the submenu for configuring communications networks 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. Enter option `2`, Configure Sync 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: 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 12 and 13 related to option 3, Configure DSM Network.

> **Note:**
>
> It is strongly advised not to change the DSM network subnet (IP addresses), if not absolutely necessary.

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 14 and 15.

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. 0.0.0.0 is a valid IP address and can be used to reset the VIP/backup provisioning IP address.

The address information should be received from the customer for the MPS. Refer to the information recorded in Table 5-1 through Table 5-4 for the correct addresses.

The IP address for this interface must be on a different class C subnet than the primary Provisioning Network address. 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 16 through 19 and proceed to 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:
```

> **Note:**
>
> The menu for changing the default value for HTTP and HTTP SuExec ports is not working as expected; the GUI may become inaccessible after the change.

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

    Refer to the information recorded in Table 5-1 and Table 5-2 for the correct information.
    A: MPS on EAGLE A:

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

    B: MPS on EAGLE 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 17 through 20 for configuring static NAT and continue with 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 |
|----|---------------------------------------|
|  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 A:**

    Options 1 and 3 are valid.

    B: MPS on EAGLE B:

    Option 2 is valid.

22. Enter a valid NAT IP address from Table 5-1 or Table 5-2.

    > **Note:**
    >
    > 127.0.0.1 is not a valid IP address for this operation. 0.0.0.0 is a valid IP address and can be used to reset the VIP/backup provisioning IP address.

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

23. Choose option `e` on theConfigure 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 24 through 26 and proceed to 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 Static NAT Addresses        |
|----|---------------------------------------|
|  6 | 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. 0.0.0.0 is a valid IP address and can be used to reset the VIP/backup provisioning IP address.

```
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 (5), skip menu option 3. Proceed to 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                          |
|----|-----------------------------------|
| 10 | SNMP Configuration                |
|----|-----------------------------------|
| 11 | Configure Alarm Feed              |
|----|-----------------------------------|
| 12 | Configure Query Server            |
|----|-----------------------------------|
| 13 | Configure Query Server Alarm Feed |
|----|-----------------------------------|
| 14 | Configure SNMP Agent Community    |
|----|-----------------------------------|
| 15 | DB Architecture Menu              |
|----|-----------------------------------|
|  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 B, List of Time Zones.

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 `1`, Exchange**Secure 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 28.

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                          |
|----|-----------------------------------|
| 10 | SNMP Configuration                |
|----|-----------------------------------|
| 11 | Configure Alarm Feed              |
|----|-----------------------------------|
| 12 | Configure Query Server            |
|----|-----------------------------------|
```

```
| 13 | Configure Query Server Alarm Feed |
|----|-----------------------------------|
| 14 | Configure SNMP Agent Community    |
|----|-----------------------------------|
| 15 | DB Architecture Menu              |
|----|-----------------------------------|
|  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 My Oracle Support 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 option`5` and proceed to 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                          |
|----|-----------------------------------|
| 10 | SNMP Configuration                |
|----|-----------------------------------|
| 11 | Configure Alarm Feed              |
|----|-----------------------------------|
| 12 | Configure Query Server            |
|----|-----------------------------------|
| 13 | Configure Query Server Alarm Feed |
|----|-----------------------------------|
| 14 | Configure SNMP Agent Community    |
|----|-----------------------------------|
| 15 | DB Architecture Menu              |
```

```
|----|----------------------------------|
|  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 an**NTP** server at this time, skip all steps related to option`7` and proceed to 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                          |
|----|----------------------------------|
| 10 | SNMP Configuration                |
```

```
|----|-----------------------------------|
| 11 | Configure Alarm Feed              |
|----|-----------------------------------|
| 12 | Configure Query Server            |
|----|-----------------------------------|
| 13 | Configure Query Server Alarm Feed |
|----|-----------------------------------|
| 14 | Configure SNMP Agent Community    |
|----|-----------------------------------|
| 15 | DB Architecture Menu              |
|----|-----------------------------------|
|  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. 0.0.0.0 is a valid IP address and can be used to reset the VIP/backup provisioning IP address.

B: MPS on EAGLE B:

Enter the same IP address for the NTP server that was previously added to the MPS A and B servers on EAGLE 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 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                          |
|----|-----------------------------------|
| 10 | SNMP Configuration                |
|----|-----------------------------------|
| 11 | Configure Alarm Feed              |
|----|-----------------------------------|
| 12 | Configure Query Server            |
|----|-----------------------------------|
| 13 | Configure Query Server Alarm Feed |
|----|-----------------------------------|
| 14 | Configure SNMP Agent Community    |
|----|-----------------------------------|
| 15 | DB Architecture Menu              |
|----|-----------------------------------|
|  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 5-1 through Table 5-4 for the information required to configure the PDB Network.

> **Note:**
>
> 127.0.0.1 is not a valid IP address for this operation. 0.0.0.0 is a valid IP address and can be used to reset the VIP/backup provisioning IP address.

- **Only for provisionable MPSs (MPS of EAGLE A or MPS of EAGLE B):**
  A: MPS on EAGLE A:

  You must have the IP address for the MPS A of EAGLE B (recorded in Table 5-2).

  B: MPS on EAGLE B:

  You must have the IP address for the MPS A of EAGLE A (recorded in Table 5-1).

  Option `1` requires you to provide the IP address of the MPS A on EAGLE A and the IP address for the MPS A on EAGLE 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 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 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 44.

- **Only for non-provisionable MPSs:**
  N: Non-Provisionable MPS:

  You must have the IP addresses for the MPS A of EAGLE A and MPS A of EAGLE B (recorded in Table 5-1 and Table 5-2).

  Option `1` requires you to provide the IP addresses for the MPS A on EAGLE A and the MPS A on EAGLE 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...
```

After 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 option`2`,RTDB Homing Menu, and proceed with 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 A, MPSs on EAGLE B, or any non-provisionable MPS pairs.

A: MPS on EAGLE A:

Proceed to 49.

N: Non-Provisionable MPS:

Proceed to 52.

B: MPS on EAGLE B:

Proceed to 55.

A: MPS on EAGLE A:

Perform 49 through 52 only for MPS A and B on EAGLE 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            |
|----|-----------------------------------|
|  9 | Security                          |
|----|-----------------------------------|
| 10 | SNMP Configuration                |
|----|-----------------------------------|
| 11 | Configure Alarm Feed              |
|----|-----------------------------------|
| 12 | Configure Query Server            |
|----|-----------------------------------|
| 13 | Configure Query Server Alarm Feed |
|----|-----------------------------------|
| 14 | Configure SNMP Agent Community    |
|----|-----------------------------------|
| 15 | DB Architecture 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 A:

The configuration of the MPSs on EAGLE A is not complete until its PDB is created. The MPSs on the EAGLE A PDB are created during the initial configuration of the MPS A on EAGLE B, which automatically replicates the PDB on the MPS on EAGLE A at the same time.

You have completed the initial configuration of MPSs on EAGLE A. You can begin the configuration of the MPSs on EAGLE B.

> **Caution:**
>
> Do not attempt to reboot the MPSs on EAGLE A at this point in the configuration. Rebooting the MPSs at EAGLE A and EAGLE B is performed concurrently when the configuration of the MPSs at EAGLE B is completed.

N: Non-Provisionable MPS:

Perform 52 and 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                         |
|----|----------------------------------|
| 10 | SNMP Configuration               |
|----|----------------------------------|
| 11 | Configure Alarm Feed             |
|----|----------------------------------|
| 12 | Configure Query Server           |
|----|----------------------------------|
| 13 | Configure Query Server Alarm Feed |
|----|----------------------------------|
| 14 | Configure SNMP Agent Community   |
|----|----------------------------------|
| 15 | DB Architecture Menu             |
|----|----------------------------------|
|  e | Exit                             |
\-------------------------------------/

Enter Choice:6
```

54. Proceed to 57.

    B: MPS on EAGLE B:

    Perform 55 only for MPS A and B on EAGLE 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.

> **Note:**
>
> While creating PDB database using the Create PDB option of the **EPAP Configuration Menu**, ensure that the value for remote PBD IP is set to 0.0.0.0.

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 B, if the time zone was not changed (27) the EPAP initial configuration of MPSs on EAGLE B is now complete.
- During configuration of MPSs on EAGLE B, if the Backup Provisioning Network (14) was not configured on either MPS, the EPAP initial configuration of MPSs on EAGLE B is now complete.
- Otherwise continue with 56 to reboot both MPS pairs on EAGLE A and on EAGLE 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                          |
|----|-----------------------------------|
| 10 | SNMP Configuration                |
|----|-----------------------------------|
| 11 | Configure Alarm Feed              |
|----|-----------------------------------|
| 12 | Configure Query Server            |
|----|-----------------------------------|
| 13 | Configure Query Server Alarm Feed |
|----|-----------------------------------|
| 14 | Configure SNMP Agent Community    |
|----|-----------------------------------|
| 15 | DB Architecture Menu              |
|----|-----------------------------------|
|  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 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 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                          |
|----|-----------------------------------|
| 10 | SNMP Configuration                |
|----|-----------------------------------|
| 11 | Configure Alarm Feed              |
|----|-----------------------------------|
| 12 | Configure Query Server            |
|----|-----------------------------------|
| 13 | Configure Query Server Alarm Feed |
|----|-----------------------------------|
| 14 | Configure SNMP Agent Community    |
|----|-----------------------------------|
| 15 | DB Architecture Menu              |
|----|-----------------------------------|
|  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 B:

The initial configuration of MPSs on EAGLE B is complete. Both MPSs on EAGLE 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.

5.4.5 Procedure for turning on EIRBLK

EIRBLK Expansion is a configurable feature that needs to be turned ON to provision more than 50,000 EIR Blocks. The PDBA limits EIR Block entries under 50,000 if the EIR_BLK_EXPANSION_200K feature is OFF.

1. Stop the EPAP and PDBA application:

```
$ systemctl stop Epap
$ systemctl stop Pdba
```

> **Note:**
>
> The provisioning will be interrupted when the application is stopped.

2. Enable EIR Block expansion:

```
$ uiEdit "EIR_BLK_EXPANSION_200K" ON
```

3. Start the EPAP and PDBA application:

```
$ systemctl start Epap
$ systemctl start Pdba
```

5.4.6 Procedure for turning on DNBLK

DNBLK Expansion is a configurable feature that needs to be turned ON to provision more than 100,000 EIR Blocks. The PDBA limits EIR Block entries under 100,000 if the DN_BLK_EXPANSION_400K feature is OFF.

1. Stop the EPAP and PDBA application:

```
$ systemctl stop Epap
$ systemctl stop Pdba
```

> **Note:**
>
> The provisioning will be interrupted when the application is stopped.

2. Enable EIR Block expansion:

```
$ uiEdit "DN_BLK_EXPANSION_400K" ON
```

3. Start the EPAP and PDBA application:

```
$ systemctl start Epap
$ systemctl start Pdba
```

5.4.7 Turning on the 240M DN and 240M IMSIs via Split Database Feature

The 240M DN and 240M IMSIs via Split Database (EPAP_DATA_SPLIT) feature must be turned on to support the expanded RTDB capacity. This feature must be turned on the EAGLE side.

See "Activating the EPAP Data Split and Dual ExAP Configuration Features" in *Database Administration - GTT User's Guide* for EAGLE for configuration.

Supported DB Capacity

As of Release 16.3, flexible provisioning of DN/IMSI/IMEI data with the available disk size and SM memory size is supported, allowing the maximum number of data provisioned to be irrespective of the type of data. The following DB capacities are supported:

> **Note:**
>
> The E5-SM8G-B card does NOT support the increased (480 M DN + 480 M IMSI + 600Mn IMEI) capacities - it supports only the existing capacities for EPAP 16.2/16.1, which is 240M DN + 240M IMSI + 48M IMEI.

Table 5-9 Supported DB Capacity

EPAP TYPE/Disk Size	EPAP Operation Mode	SM card type with "EPAP Data Split" feature status	DB Capacity and Configuration	DB Capacity limiting factor; Minimal memory size required to be available on SM (in Bytes)
E5APPB-02/480GB	Standalone PDB; Mixed EPAP	E5-SM8G-B (epap240M ON) with "EPAP Data Split" feature OFF	Total Max DB: 288M DN/IMSI/IMEI Current capacity NOT configurable in the Configuration menu.	E5-SM8G-B memory size
E5APPB-02/480GB	Standalone PDB; Mixed EPAP	E5-SM8G-B (epap240M ON) with "EPAP Data Split" feature ON	Total Max DB 528M: DN - 240M IMSI - 240M IMEI - 48M Current capacity NOT configurable in the Configuration menu.	E5-SM8G-B memory size
E5APPB-02/480GB	Standalone PDB	SLIC (EPAPX ON) with "EPAP Data Split" feature OFF	Total Max DB: 480M DN/IMSI/IMEI	None; 11,617,463,954
E5APPB-02/480GB	Standalone PDB	SLIC (EPAPX ON) with "EPAP Data Split" feature ON	Total Max DB 900M: DN - 420M (each DN is provisioned with all possible fields) IMSI/IMEI - 480M	E5APPB-02 Disk size; 10,148,933,426
E5APPB-02/480GB	Standalone PDB	SLIC (EPAPX ON) with "EPAP Data Split" feature ON	Total Max DB 1080M: DN - 480M (Standalone DNs associated with a Network Entity or a portability type; other fields such as asd, nsdn, cgbl, cdbl, should not be used) IMSI/IMEI - 600M	E5APPB-02 Disk size; 12,631,033,322
E5APPB-02/480GB	Standalone PDB	SLIC (EPAPX ON) with "EPAP Data Split" feature OFF or ON	Max DNBLK 400K; or 800K; or 1600K	None. Default Max DNBLK is 400K
E5APPB-02/480GB	Standalone PDB	SLIC (EPAPX ON) with "EPAP Data Split" feature OFF or ON	Max EIRBLK 100K; or 200K; or 800K	None. Default Max EIRBLK is 100K

> **Note:**
>
> With the "EPAP Data Split" feature ON, the data will be loaded only to EAGLE SM cards configured to be `data=DN/IMSI`.

The enhancement also supports DN Block capacity expansion from 200K to 400K, and optionally a max of 800K or 1600K DN Block is supported.

EIR Block capacity is optionally increased from 100K to configurable 200K or 800K.

6
Standalone PDB EPAP

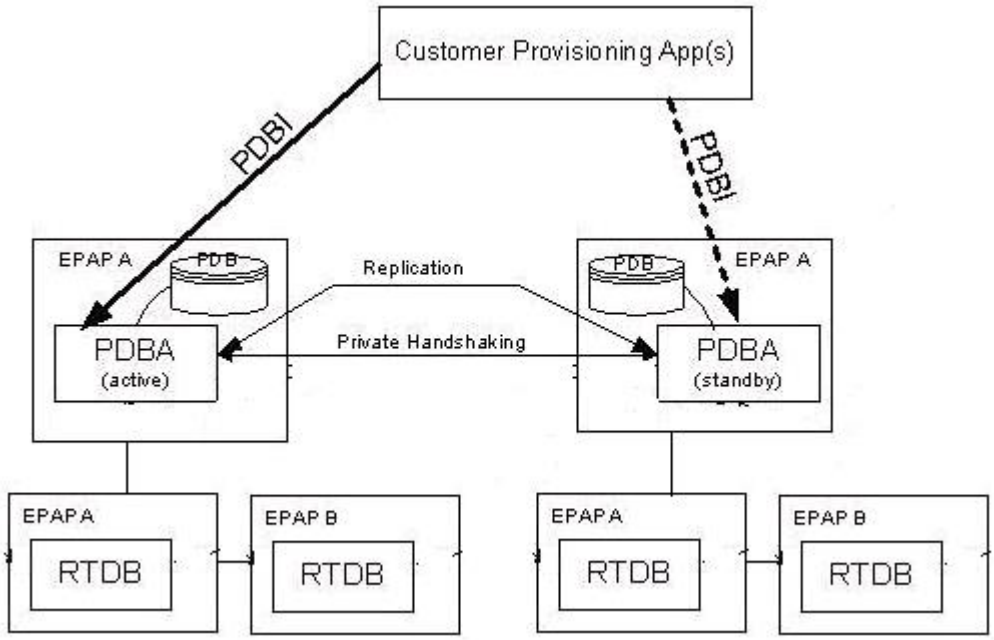
This chapter describes the Standalone PDB EPAP. The information in this chapter is specific to Standalone PDB EPAP. The content in other chapters may also apply to Standalone PDB EPAP unless the content includes Real Time Database (RTDB), Service Module Cards, EAGLE connections, or Mate servers.

6.1 General Description

This feature allows the EPAP users to build a new EPAP server that can be configured as a 'Standalone PDB' site. This is a single EPAP A server. No EPAP B is configured with it. Only PDB database will reside on the standalone PDB site. The RTDB database is not present on the standalone PDB server and therefore, it is not connected to the Eagle. The data to the Eagle is downloaded through the multiple non-provisionable EPAP servers connected to the standalone PDB site. The active standalone PDB site is connected to the standby PDBA for the PDB replication.

> **Note:**
>
> The information in this chapter is specific to Standalone PDB EPAP.

Figure 6-1 EPAP Standalone PDB Architecture



With this new functionality, the EPAP has the following architectures:

1. Standalone PDB - PDB only sites
2. Mixed EPAP - PDB and RTDB
3. Non-Provisionable EPAP - RTDB only sites

6.1.1 Standalone PDB Provisioning Performance

This section describes the Standalone PDB configurations for the database size of 60M, 240M, and 420M with respective provisioning performances. The first and second columns of the provisioning performance tables relate to database size. The third through fifth columns relate to the example operations. The final column lists the expected Commands per Second values for the specific combinations of configuration and operations. The provisioning performance values in this section are stated in Commands per Second (**CPS**), and apply to only the provisioning performance of the Standalone PDB with the stated configurations. Refer to EPAP Provisioning Performance for details about provisioning performance.

Provisioning Performance for DB Size 60M

- **Example Configuration 1**

  Table 6-1 shows the provisioning performance values associated with the following configuration:

  # of RTDB Clients = 4
  PDBI Statistics = ON
  Self Healing Feature = OFF
  Database Size: IMEI = 2M, Others = Full
  PDBI Sockets = 0
  Connection Type = Manual Import
  Provisioning Method= 1 File (1M Command per File)

Table 6-1 Provisioning Performance for Standalone PDB - Configuration 1

DB SIZE: DN	IMSI	OPERATIONS: Operation	Data Type	Associated Properties	CPS
60M	60M	dlt	2M DNs	Existing DNs with SP and NE attributes	700
58M	60M	add	2M DNs	Add DNs with SP and NE attributes	900
60M	60M	dlt	2M IMSIs	Existing IMSIs with no DNs	1000
60M	58M	add	2M IMSIs	Add IMSIs with no DNs	1250

- **Example Configuration 2**

  Table 6-2 shows the provisioning performance values associated with the following configuration:

  # of RTDB Clients = 4
  PDBI Statistics = ON
  Self Healing Feature = OFF
  Database Size: IMEI = 2M, Others = Full
  PDBI Sockets = 1
  Connection Type = Normal 4 commands by TXN
  Provisioning Method= Asynchronous

Table 6-2 Provisioning Performance for Standalone PDB - Configuration 2

DB SIZE: DN	IMSI	OPERATIONS: Operation	Data Type	Associated Properties	CPS
60M	60M	upd_sub	2M DNs	Existing DNs with SP and NE attributes	250
60M	60M	dlt_sub	2M DNs	Existing DNs with SP and NE attributes	450
58M	60M	ent_sub	2M DNs	Add DNs with SP and NE attributes	450
60M	60M	upd_sub	2M IMSIs	Existing IMSIs with no DNs	450
60M	60M	dlt_sub	2M IMSIs	Existing IMSIs with no DNs	450
60M	58M	ent_sub	2M IMSIs	Add IMSIs with no DNs	450

- **Example Configuration 3**
  Table 6-3 shows the provisioning performance values associated with the following configuration:

  # of RTDB Clients = 4
  PDBI Statistics = ON
  Self Healing Feature = OFF
  Database Size: IMEI = 2M, Others = Full
  PDBI Sockets = 1
  Connection Type = Single
  Provisioning Method= Asynchronous

Table 6-3 Provisioning Performance for Standalone PDB - Configuration 3

DB SIZE: DN	IMSI	OPERATIONS: Operation	Data Type	Associated Properties	CPS
60M	60M	upd_sub	2M DNs	Existing DNs with SP and NE attributes	300
60M	60M	dlt_sub	2M DNs	Existing DNs with SP and NE attributes	300
58M	60M	ent_sub	2M DNs	Add DNs with SP and NE attributes	400
60M	60M	upd_sub	2M IMSIs	Existing IMSIs with no DNs	300
60M	60M	dlt_sub	2M IMSIs	Existing IMSIs with no DNs	300
60M	58M	ent_sub	2M IMSIs	Add IMSIs with no DNs	400

Provisioning Performance for 240M

- **Example Configuration 4**
  Table 6-4 shows the provisioning performance values associated with the following configuration:

  # of RTDB Clients = 4
  PDBI Statistics = ON
  Self Healing Feature = OFF
  Database Size: DN = 240M, IMSI = 240M, IMEI = 48M, NE=50K, ASD = 1M, DN Block=200K, IMEI Block=100K
  DB Architecture = Compact
  PDBI Sockets = 1

Connection Type = Single/Normal/File Import
Provisioning Method= Synchronous
EAGLE Connected = Yes

Table 6-4 Provisioning Performance for Standalone PDB - Configuration 4

DB SIZE: DN	IMSI	Connection Type	OPERATIONS : Operation	Data Type	Associated Properties	CPS
240M	240 M	Single	ent_sub	200K DNs	Add DNs with SP and NE attributes	200
240M	240 M	Normal	ent_sub	200K DNs	Add DNs with SP and NE attributes	450
240M	240 M	File Import	ent_sub	200K DNs	Add DNs with SP and NE attributes	475
240M	240 M	Single	ent_sub	200K IMSIs	Add IMSIs with no DNs	275
240M	240 M	Normal	ent_sub	200K IMSIs	Add IMSIs with no DNs	600
240M	240 M	File Import	ent_sub	200K IMSIs	Add IMSIs with no DNs	725

Provisioning Performance for 420M

- **Example Configuration 5**
  Table 6-5 shows the provisioning performance values associated with the following configuration:

  # of RTDB Clients = 4
  PDBI Statistics = ON
  Self Healing Feature = OFF
  Database Size: DN = 510M, IMSI = 300M, IMEI = 800K, NE=50K, DN Block=800K, IMEI Block=200K
  DB Architecture = Extreme
  PDBI Sockets = 1
  Connection Type = Single/Normal/File Import
  Provisioning Method= Synchronous
  EAGLE Connected = Yes

Table 6-5 Provisioning Performance for Standalone PDB - Configuration 5

DB SIZE: DN	IMSI	Connection Type	OPERATIONS : Operation	Data Type	Associated Properties	CPS
510M	300 M	Single	ent_sub	200K DNs	Add DNs with SP and NE attributes	225
510M	300 M	Normal	ent_sub	200K DNs	Add DNs with SP and NE attributes	450
510M	300 M	File Import	ent_sub	200K DNs	Add DNs with SP and NE attributes	475
510M	300 M	Single	ent_sub	200K IMSIs	Add IMSIs with no DNs	275

Table 6-5 (Cont.) Provisioning Performance for Standalone PDB - Configuration 5

DB SIZE: DN	IMSI	Connection Type	OPERATIONS : Operation	Data Type	Associated Properties	CPS
510M	300 M	Normal	ent_sub	200K IMSIs	Add IMSIs with no DNs	600
510M	300 M	File Import	ent_sub	200K IMSIs	Add IMSIs with no DNs	725

- **Example Configuration 6**
  Table 6-6 shows the provisioning performance values associated with the following configuration:

  # of RTDB Clients = 4
  PDBI Statistics = ON
  Self Healing Feature = OFF
  Database Size: DN = 510M, IMSI = 300M, IMEI = 800K, NE=50K, DN Block=800K, IMEI Block=200K
  DB Architecture = Extreme
  PDBI Sockets = 1
  Connection Type = Single/Normal/File Import
  Provisioning Method= Synchronous
  EAGLE Connected = Yes

Table 6-6 Provisioning Performance for Standalone PDB - Configuration 6

DB SIZE: DN	IMSI	Connection Type	OPERATIONS : Operation	Data Type	Associated Properties	CPS
510M	300 M	Single	ent for 1 IMEI with 8 IMSIs and remaining 2 IMSIs using upd_eir command	200K IMEIs (each associated with 10 IMSIs)	Add DNs with SP and NE attributes	175
510M	300 M	Normal	ent for 1 IMEI with 8 IMSIs and remaining 2 IMSIs using upd_eir command	200K IMEIs (each associated with 10 IMSIs)	Add DNs with SP and NE attributes	325
510M	300 M	File Import	ent for 1 IMEI with 8 IMSIs and remaining 2 IMSIs using upd_eir command	200K IMEIs (each associated with 10 IMSIs)	Add DNs with SP and NE attributes	275

Provisioning Performance Limitations

The provisioning performance values are stated as an indication of possible CPS based on the key factors influencing the provisioning performance. For asynchronous provisioning systems, provisioning tool behavior plays a significant role in the actual performance.

The stated provisioning performance values for Standalone PDB are not valid for Mixed EPAP configurations, where RTDB and PDB are on the same EPAP servers.

Failure to achieve possible provisioning performance values does not constitute a breach of obligations by Oracle. Oracle assumes no liability with respect to the achievable CPS; no contractual obligations with Oracle are created by these provisioning performance values.

6.2 EPAP Configuration

This feature removes the epapconfig menus and sub-menus corresponding to the RTDB, Eagle, and EPAP B (mate).

Initial epapconfig User Login

The first time the epapconfig user logs in to the system, the initial configuration is performed. A caution is displayed and the user enters 'Y' to start the configuration. The EuiDB database is built. Unlike the standard EPAP configuration, the user is not asked to configure the EPAP as provisionable or non-provisionable, as the standalone PDB site is a provisionable site.

The user will be asked to enter System Number as the standalone PDB has their dedicated System Number.

The user will be prompted to set the Network Configuration Type to either single or segmented.

In 'Single' network configuration type, all IP interfaces are supported on one Ethernet port (IP address).

In 'Segmented' network configuration type, three different interfaces are used as follows:

- **eth01** - Provisioning interface (PDBI, SOG, PDB replication, PDBA clients, Data download to RTDB)
- **eth02** - EPAP GUI Access
- **eth03** - Operations and Maintenance (O&M) interface for SSH/SFTP
- **eth04** - Backup Provisioning Interface

```
Caution: This is the first login of the text user interface.

Press return to continue...
Are you sure you wish to ontinue? [N]: Y
Building the intitial database on side A.
Stopping local slave
EuiDB already exists on local.
Starting local slave
Set EPAP System Number:
Enter the Network Configuration Type (1 for Single, 2 for Segmented):
```

> **Note:**
>
> The user can choose the segmented network configuration and might not configure the GUI and Operations and Maintenance network. In that case, the EPAP initial configuration may be assumed as complete and the EPAP will behave as if in single network configuration.

Main Menu

The epapconfig main menu remains unchanged for the Standalone PDB site.

Figure 6-2 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                          |
|----|-----------------------------------|
| 10 | SNMP Configuration                |
|----|-----------------------------------|
| 11 | Configure Alarm Feed              |
|----|-----------------------------------|
| 12 | Configure Query Server            |
|----|-----------------------------------|
| 13 | Configure Query Server Alarm Feed |
|----|-----------------------------------|
| 14 | Configure SNMP Agent Community    |
|----|-----------------------------------|
| 15 | DB Architecture Menu              |
|----|-----------------------------------|
|  e | Exit                              |
\--------------------------------------/

Enter Choice:
```

Display Configuration Menu

The display configuration menu option 1, displays the EPAP configuration. On standalone PDB site, only the configuration related to EPAP A and PDB are displayed, as shown in Figure 6-3.

Please note that the parameter values displayed in the below figure are just examples. The values depend on the site configuration.

Figure 6-3 Single Network Configuration Display

```
Enter Choice: 1


MPS Side A:  hostname: PDbonly78  hostid: f80a4e0a
             Platform Version: 4.0.10-5.5.1_75.18.0
             Software Version: EPAP 160.0.13-16.0.0_160.13.0
             Sun Aug 23 21:40:37 EDT 2020

EPAP A Provisioning Network IP Address = 10.248.10.78
Provisioning Network Netmask           = 255.255.255.0
Provisioning Network Default Router    = 10.248.10.1
EPAP A Backup Prov Network IP Address  = Not configured
Backup Prov Network Netmask            = Not configured
Backup Prov Network Default Router     = Not configured
Network Configuration Type             = SINGLE
EPAP A HTTP Port                       = 80
EPAP A HTTP SuExec Port                = 8001
EPAP A Banner Connection Port          = 8473
EPAP A Static NAT Address              = Not configured
PDBI Port                              = 5873
Remote MPS A Static NAT Address        = Not configured
Remote MPS A HTTP Port                 = Not configured
Local PDBA Address                     = 10.248.10.78
Remote PDBA Address                    = 10.248.10.79
Time Zone                              = America/New_York
PDB Database                           = Exists
Auto DB Recovery Enabled               = Yes

Press return to continue...
```

Figure 6-4 Segmented Network Configuration Display

```
EPAP A Provisioning Network IP Address = 10.248.10.52
Provisioning Network Netmask           = 255.255.255.0
Provisioning Network Default Router    = 10.248.10.1
EPAP A Backup Prov Network IP Address  = Not configured
Backup Prov Network Netmask            = Not configured
Backup Prov Network Default Router     = Not configured
Network Configuration Type             = SEGMENTED
EPAP A GUI Network IP Address          = 10.248.9.52
GUI Network Netmask                    = 255.255.255.0
GUI Network Default Router             = 10.248.9.1
EPAP A O&M Network IP Address          = 10.248.8.52
O&M Network Netmask                    = 255.255.255.0
O&M Network Default Router             = 10.248.8.1
EPAP A HTTP Port                       = 80
EPAP A HTTP SuExec Port                = 8001
EPAP A Banner Connection Port          = 8473
EPAP A Static NAT Address              = Not configured
PDBI Port                              = 5873
Remote MPS A Static NAT Address        = Not configured
Remote MPS A HTTP Port                 = Not configured
Local PDBA Address                     = 10.248.10.52
Remote PDBA Address                    = 0.0.0.0
Time Zone                              = America/New_York
PDB Database                           = Exists
Auto DB Recovery Enabled               = No

Press return to continue...
```

Configure Network Interfaces Menu

The network interfaces configuration menu Option 2, does not provide the option to configure the DSM and sync interfaces because of the non-requirement of eagle and EPAP B (mate) connectivity, respectively. The menus for PDBA proxy are also be removed. The displayed menu options are dependent on the configured Network Configuration Type.

Figure 6-5 Single Network Interface Menu

```
Enter Choice: 2


MPS Side A:  hostname: PDbonly78  hostid: f80a4e0a
             Platform Version: 4.0.10-5.5.1_75.18.0
             Software Version: EPAP 160.0.13-16.0.0_160.13.0
             Sun Aug 23 21:44:41 EDT 2020

 /-----Configure Network Interfaces Menu----\
/-------------------------------------------\
|   1 | Configure Provisioning Network      |
|-----|-------------------------------------|
|   2 | Configure Backup Provisioning Network |
|-----|-------------------------------------|
|   3 | Configure Forwarded Ports           |
|-----|-------------------------------------|
|   4 | Configure Static NAT Addresses      |
|-----|-------------------------------------|
|   e | Exit                                |
\-------------------------------------------/

Enter Choice:
```

For the segmented configuration, the menu allows the user to configure all the interfaces separately. The IP version on the interfaces shall be independent of each other. This means that the user is able to configure any interface in the IPv4 only, IPv6 only or dual stack configuration.

Figure 6-6 Segmented Network Interface Menu

```
 /-----Configure Network Interfaces Menu-----------\
/-------------------------------------------------\
|   1 | Configure Provisioning Network              |
|-----|---------------------------------------------|
|   2 | Configure GUI Network                       |
|-----|---------------------------------------------|
|   3 | Configure Operations and Maintenance Network |
|-----|---------------------------------------------|
|   4 | Configure Backup Provisioning Network       |
|-----|---------------------------------------------|
|   5 | Configure Forwarded Ports                   |
|-----|---------------------------------------------|
|   6 | Configure Static NAT Addresses              |
|-----|---------------------------------------------|
|   e | Exit                                        |
\-------------------------------------------------/

Enter Choice:
```

For each menu selection, except Static NAT Addresses, the user must select whether the input is an IPv4 or IPv6 address. The Provisioning, GUI, Backup Provisioning and Operations and Maintenance Network configuration is configured the same way for a mixed EPAP.

Configure Provisioning Network Menu

The 'Configure provisioning network' menu configures the EPAP provisioning network for the standalone PDB site. Unlike the standard EPAP site, the user is not prompted for EPAP B (mate) parameters. On the standalone PDB site, the provisioning IP configured through this menu is used for the following operations: PDBI sockets, File imports for provisioning, Replication to the standby PDB and PDBA clients (RTDB).

Figure 6-7 Configure Provisioning Network

```
Entered the configMenuConfigProvNet Menu

MPS Side A:  hostname: epappri  hostid: f80a540a
             Platform Version: 4.0.10-5.5.1_75.20.0
             Software Version: EPAP 161.0.1-16.1.0_161.2.0
             Thu Apr  9 06:48:45 EDT 2015

 /-----Configure Provisiong Network Menu-\
/-----------------------------------------\
|  1 | IPv4 Configuration                 |
|----|------------------------------------|
|  2 | IPv6 Configuration                 |
|----|------------------------------------|
|  e | Exit                               |
\-----------------------------------------/

Enter Choice: 2

EPAP A provisioning network IPv6 Address: 2606:b400:605:b80b:200:17ff:fe0f:2894
EPAP provisioning network IPv6 prefix: 64
EPAP provisioning network IPv6 default router: 2606:b400:605:b80b::
```

Configure GUI Network Menu

The Configure GUI Network menu prompts the user for the standalone PDB GUI Network IP addresses. The user is allowed to access the EPAP GUI through the configured IP only. This menu is available only on the standalone PDB sites.

Figure 6-8 Configure GUI Network

```
MPS Side A:  hostname: epappri  hostid: f80a540a
             Platform Version: 4.0.10-5.5.1_75.20.0
             Software Version: EPAP 161.0.1-16.1.0_161.2.0
             Thu Apr  9 06:52:11 EDT 2015

 /-----Configure GUI Network Menu-\
/-----------------------------------\
|  1 | IPv4 Configuration           |
|----|------------------------------|
|  2 | IPv6 Configuration           |
|----|------------------------------|
|  e | Exit                         |
\-----------------------------------/

Enter Choice: 2

EPAP A GUI network IPv6 Address: 2606:b400:605:b80b:200:17ff:fe0f:3840
EPAP GUI network prefix: 64
EPAP GUI network route: 2606:b400:605:b80b::
```

Configure Operations and Maintenance Network Menu

The Configure Operations and Maintenance Network menu prompts the user for the standalone PDB O&M Network IP addresses. The user is allowed to access the EPAP CLI through the configured IP only. This menu is available only on the standalone PDB sites. The IP configured through this menu is used for the SSH operations.

Figure 6-9 Configure Operations and Maintenance Network Menu

```
MPS Side A:  hostname: epappri  hostid: f80a540a
             Platform Version: 4.0.10-5.5.1_75.20.0
             Software Version: EPAP 161.0.1-16.1.0_161.2.0
             Thu Apr  9 06:59:11 EDT 2015

 /-----Configure Operations and Maintenance Network Menu-\
/-------------------------------------------------------\
|  1 | IPv4 Configuration                               |
|----|--------------------------------------------------|
|  2 | IPv6 Configuration                               |
|----|--------------------------------------------------|
|  e | Exit                                             |
\-------------------------------------------------------/

Enter Choice: 2

EPAP A Operations and Maintenance network IPv6 Address: 2606:b400:605:b80b:200:17ff:fe0f:4870
EPAP Operations and Maintenance network prefix:64
EPAP Operations and Maintenance network route: 2606:b400:605:b80b::
```

Configure Backup Provisioning Network Menu

The Configure Backup Provisioning Network menu prompts the user for the standalone PDB Backup Provisioning Network IP addresses. This information allows the EPAP to communicate with the backup provisioning network. It is used when the main provisioning network

(configured on eth01) goes down. The behavior is same in both single and segmented network configuration.

```
EPAP A backup provisioning network IP Address [0.0.0.0]:
EPAP backup provisioning network netmask [0.0.0.0]:
EPAP backup provisioning network default route [0.0.0.0]:
```

> **Note:**
>
> In case the Provisioning Network goes down and the Backup Provisioning Network is configured, all connected Non-Provisioning Networks must be reconfigured to provide the Backup Provisioning IP for the PDB from which the Non-Provisioning Network will take updates.

Configure Forwarded Ports Menu

The Configure Forwarded Ports menu provides the functionality to configure the standalone PDB ports for the Web UI on EPAP A.

Figure 6-10 Forwarded Ports Configuration Menu

```
 /-----Configure Forwarded Ports Menu------\
/-----------------------------------------\
|  1 | Change EPAP A HTTP Port              |
|----|--------------------------------------|
|  2 | Change EPAP A HTTP SuExec Port       |
|----|--------------------------------------|
|  3 | Change EPAP A Banner Connection Port |
|----|--------------------------------------|
|  4 | Change PDBI Port                     |
|----|--------------------------------------|
|  5 | Change Remote MPS A HTTP Port        |
|----|--------------------------------------|
|  e | Exit                                 |
\-----------------------------------------/

Enter Choice:
```

Configure Static NAT Addresses Menu

The Configure Static NAT Addresses menu provides the functionality to configure the static NAT addresses of the standalone PDB site. Each of the configured IP Address is used outside of the firewall for remote access to the MPS.

Figure 6-11 Static NAT Addresses Menu

```
 /-----Configure Static NAT Addresses Menu---\
/--------------------------------------------\
|  1 | Change EPAP A Static NAT Address       |
|----|----------------------------------------|
|  2 | Change Remote MPS A Static NAT Address |
|----|----------------------------------------|
|  e | Exit                                   |
\--------------------------------------------/

Enter Choice:
```

Exchange Secure Shell Keys

The key exchange is facilitated with the remote PDBA server only.

Figure 6-12 Exchange Secure Shell Keys Menu

```
 /-----Exchange Secure Shell Keys Menu-\
/--------------------------------------\
|  1 | Exchange Keys with Remote       |
|----|---------------------------------|
|  e | Exit                            |
\--------------------------------------/

Enter Choice:
```

Platform Menu

The platform menu shall not provide the option for RTDB Backup.

Figure 6-13 EPAP Platform Menu

```
 /-----EPAP Platform Menu-\
/-------------------------\
|  1 | Initiate Upgrade   |
|----|--------------------|
|  2 | Reboot MPS         |
|----|--------------------|
|  3 | MySQL Backup       |
|----|--------------------|
|  4 | PDB Backup         |
|----|--------------------|
|  e | Exit               |
\-------------------------/

Enter Choice:
```

PDB Configuration Menu

The PDB Configuration menu does not provide the option to set RTDB Homing Policy, Change MPS Provisionable state and change PDBA Proxy State. The PDBA Proxy feature is not supported on the standalone PDB site as it is a single site with no EPAP B (mate).

Figure 6-14 Configure PDB Menu

```
/-----Configure PDB Menu-----------\
/-----------------------------------\
|  1 | Configure PDB Network         |
|----|-------------------------------|
|  2 | Configure PDB Capacity        |
|----|-------------------------------|
|  3 | Create PDB                    |
|----|-------------------------------|
|  4 | Change Auto DB Recovery State |
|----|-------------------------------|
|  e | Exit                          |
\-----------------------------------/
```

Configure PDB Network Menu

The Configure PDB Network menu prompts the user for the remote PDB IP address. Unlike the mixed EPAP, the standalone PDB site ask only for PDBA A IP address and not the PDBA B IP Address.

```
This MPS is configured to be provisionable.  The EPAP local PDBA
address is currently set to 10.250.51.130.
EPAP software and PDBA are running.  Stop them? [N]: Y
The EPAP local PDBA IP Address is 10.250.51.130.
EPAP remote PDBA IP Address [0.0.0.0]: 10.250.51.131
The server does not know of 10.250.51.131.
Will just exchange host keys for the name given!
Password of epapdev:
The server does not know of 10.250.51.131.
Will just exchange host keys for the name given!
ssh is working correctly.
```

6.3 EPAP GUI

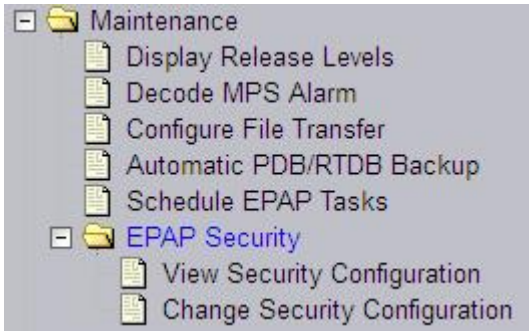
This feature removes the EPAP GUI menus and sub-menus corresponding to the RTDB, Eagle and EPAP B (mate). On the standalone PDB site, the GUI menus are as follows.

Figure 6-15 EPAP A GUI Main Menu

Maintenance sub-menu

The maintenance sub-menu no longer provides the option to activate the Force standby mode and the RTDB Audit. The option to take automatic backup configures the PDB backup on the Standalone PDB site and the RTDB backup is scheduled for all connected non-provisionable pairs.

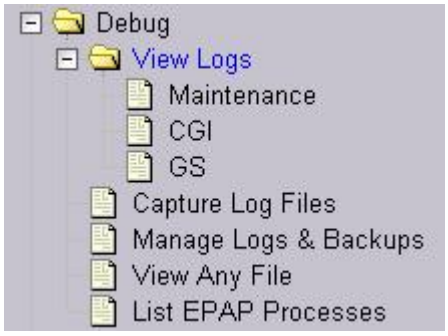
Figure 6-16 EPAP A Maintenance sub-menu



Debug sub-menu

The debug sub-menu provides the option to view only Maintenance, CGI and GS logs.

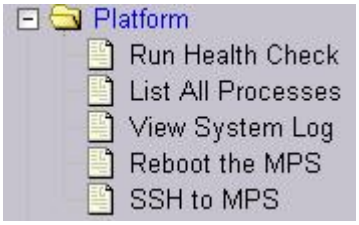
Figure 6-17 EPAP A Debug sub-menu



Platform sub-menu

The Platform sub-menu provides the following options:

Figure 6-18 EPAP A Platform sub-menu



PDBA sub-menu

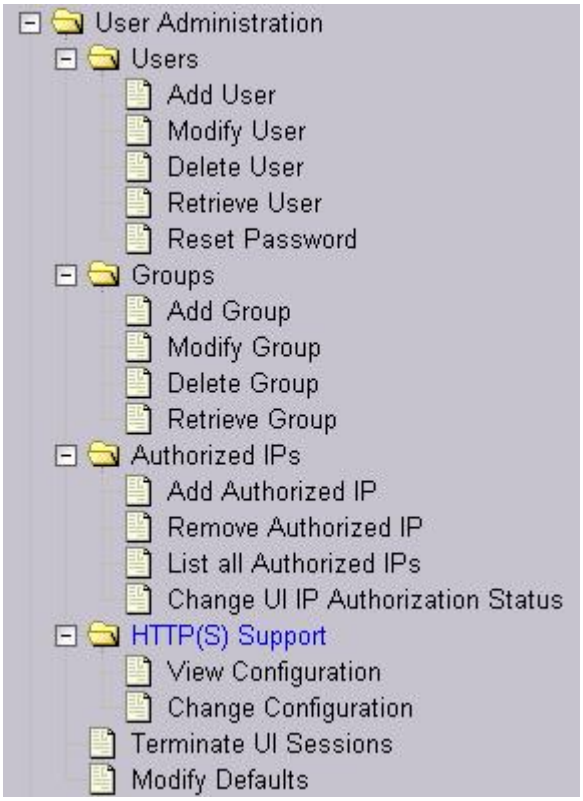
The PDBA sub-men remains unchanged.

Figure 6-19 EPAP A PDBA Main Menu

User Administration sub-menu

The User Administration sub-menu remains unchanged.

Figure 6-20 EPAP A User Administration Menu



6.4 EPAP GUI Banner Section

The banner frame containing EPAP A server information extends the entire width of the browser window.

The EPAP A areas contain information and displays to inform the user about the status and operation of the servers.

The Oracle Communications logo icon is located at the top left of the banner applet.

Figure 6-21 EPAP A GUI Banner Section

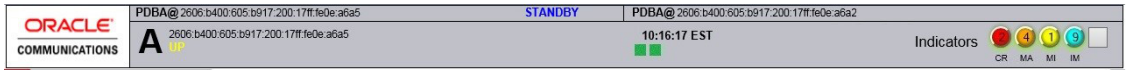
In the dual stack configuration, the EPAP GUI is accessible through both configured IPv4 and IPv6 IPs. The IP must be enclosed in the square brackets. Examples are displayed in the following figures:

Figure 6-22 Banner For Mixed EPAP With Watchers and No Remote PDBA

Figure 6-23 Banner for Mixed EPAP With Remote PDBA and No Watchers

Figure 6-24 Banner For Mixed EPAP With IPv6 Configuration With Watchers and Remote PDBA

Figure 6-25 Banner for PDBonly EPAP With Watchers and Remote PDBA



6.5 Standalone PDB EPAP Configuration Procedure

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 **EPAP**s 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.

> **Note:**
>
> RTDB-related executables will not be allowed to run from the CLI. Different error messages may be displayed if the user tries to execute any RTDB related executable.

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 A to configure it, then use `ssh` to connect to the MPS at EAGLE B and configure it.

After connecting to the MPS on EAGLE 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.
Press return to continue…
```

2. Press **Return** to continue.

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

> **Note:**
>
> Pressing **Return** accepts the default value `n`.

```
Are you sure you wish to continue? [N]: y
Building the initial database on side A.
  Stopping local slave
  EuiDB already exists.
  Starting local slave
Set EPAP System Number:
```

3. Enter a valid System Number and press **Return** .

   Enter the Network configuration Type (1 for Single, 2 for Segmented).

4. Enter the Network Configuration Type and press **Return** .

   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 along with hostname, `hostid`, Platform Version, Software Version, and the date.

```
MPS Side A:  hostname: SantosA  hostid: fa0a8233
             Platform Version: 4.0.10-5.5.1_75.18.0
             Software Version: EPAP 160.0.13-16.0.0_160.13.0
             Fri Aug 15 10:24:54 EDT 2014

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

```
|----|----------------------------------|
| 10 | SNMP Configuration               |
|----|----------------------------------|
| 11 | Configure Alarm Feed             |
|----|----------------------------------|
| 12 | Configure Query Server           |
|----|----------------------------------|
| 13 | Configure Query Server Alarm Feed |
|----|----------------------------------|
| 14 | Configure SNMP Agent Community   |
|----|----------------------------------|
|  e | Exit                             |
\-------------------------------------/

Enter Choice:
```

5. Choose option `1`, Display Configuration.

   This option provides a means of verifying EPAP A Provisioning Network IP address, the Time Zone, and other provisioning values for the MPS on EAGLE A.

Figure 6-26 Single Network Configuration Menu

```
Enter Choice: 1


MPS Side A:  hostname: PDbonly78  hostid: f80a4e0a
             Platform Version: 4.0.10-5.5.1_75.18.0
             Software Version: EPAP 160.0.13-16.0.0_160.13.0
             Sun Aug 23 21:40:37 EDT 2020

EPAP A Provisioning Network IP Address = 10.248.10.78
Provisioning Network Netmask           = 255.255.255.0
Provisioning Network Default Router    = 10.248.10.1
EPAP A Backup Prov Network IP Address  = Not configured
Backup Prov Network Netmask            = Not configured
Backup Prov Network Default Router     = Not configured
Network Configuration Type             = SINGLE
EPAP A HTTP Port                       = 80
EPAP A HTTP SuExec Port                = 8001
EPAP A Banner Connection Port          = 8473
EPAP A Static NAT Address              = Not configured
PDBI Port                              = 5873
Remote MPS A Static NAT Address        = Not configured
Remote MPS A HTTP Port                 = Not configured
Local PDBA Address                     = 10.248.10.78
Remote PDBA Address                    = 10.248.10.79
Time Zone                              = America/New_York
PDB Database                           = Exists
Auto DB Recovery Enabled               = Yes

Press return to continue...
```

Figure 6-27 Segmented Network Configuration Menu

```
EPAP A Provisioning Network IP Address = 10.248.10.52
Provisioning Network Netmask           = 255.255.255.0
Provisioning Network Default Router    = 10.248.10.1
EPAP A Backup Prov Network IP Address  = Not configured
Backup Prov Network Netmask            = Not configured
Backup Prov Network Default Router     = Not configured
Network Configuration Type             = SEGMENTED
EPAP A GUI Network IP Address          = 10.248.9.52
GUI Network Netmask                    = 255.255.255.0
GUI Network Default Router             = 10.248.9.1
EPAP A O&M Network IP Address          = 10.248.8.52
O&M Network Netmask                    = 255.255.255.0
O&M Network Default Router             = 10.248.8.1
EPAP A HTTP Port                       = 80
EPAP A HTTP SuExec Port                = 8001
EPAP A Banner Connection Port          = 8473
EPAP A Static NAT Address              = Not configured
PDBI Port                              = 5873
Remote MPS A Static NAT Address        = Not configured
Remote MPS A HTTP Port                 = Not configured
Local PDBA Address                     = 10.248.10.52
Remote PDBA Address                    = 0.0.0.0
Time Zone                              = America/New_York
PDB Database                           = Exists
Auto DB Recovery Enabled               = No

Press return to continue...
```

6. Press **Return** to return to the EPAP Configuration Menu.
7. Choose option 2, Configure Network Interfaces Menu.

```
Enter Choice 2:


MPS Side A:  hostname: PDbonly78  hostid: f80a4e0a
             Platform Version: 4.0.10-5.5.1_75.18.0
             Software Version: EPAP 160.0.13-16.0.0_160.13.0
             Sun Aug 23 10:24:54 EDT 2014

 /-----Configure Network Interfaces Menu----\
/-------------------------------------------\
|  1 | Configure Provisioning Network       |
|----|--------------------------------------|
|  2 | Configure Backup Provisioning Network |
|----|--------------------------------------|
|  3 | Configure Forwarded Ports            |
|----|--------------------------------------|
|  4 | Configure Static NAT Addresses       |
|----|--------------------------------------|
|  e | Exit                                 |
```

```
\-----------------------------------------/
Enter Choice:
```

```
 /-----Configure Network Interfaces Menu----------\
/-------------------------------------------------\
|  1 | Configure Provisioning Network               |
|----|----------------------------------------------|
|  2 | Configure GUI Network                        |
|----|----------------------------------------------|
|  3 | Configure Operations and Maintenance Network |
|----|----------------------------------------------|
|  4 | Configure Backup Provisioning Network        |
|----|----------------------------------------------|
|  5 | Configure Forwarded Ports                    |
|----|----------------------------------------------|
|  6 | Configure Static NAT Addresses               |
|----|----------------------------------------------|
|  e | Exit                                         |
\-------------------------------------------------/
Enter choice:
```

8. Choose option `1`, Configure Provisioning Network.

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

   > **Note:**
   >
   > 127.0.0.1 is not a valid IP address for this operation. 0.0.0.0 is a valid IP address and can be used to reset the VIP/backup provisioning IP address.

   Refer to the information recorded in Table 5-1 through Table 5-4 for the correct addresses.

   > **Note:**
   >
   > No default value is provided for the EPAP provisioning network default router. This value must be received from the customer.

   The display for the submenu for configuring communications networks appears.

```
EPAP A provisioning network IP Address [10.248.10.49]:
EPAP provisioning network netmast [255.255.255.0]:
EPAP provisioning network default router [10.248.10.1]:
```

9. Press the **Return** to return to the Configure Network Interfaces Menu. Choose `2`, Configure GUI Network.

The Configure GUI Network menu prompts the user for the standalone PDB GUI Network IP addresses. The user is allowed to access the EPAP GUI through the configured IP only. This menu is available only on standalone PDB sites.

```
EPAP A GUI network IP Address [192.168.3.10]:
EPAP GUI network netmast [255.255.255.0]:
EPAP GUI network route [192.168.3.1]:
```

10. Press **Return** to return to the Configure Network Interfaces Menu. Choose `3`, Configure Operations and Maintenance Network.

    The Configure Operations and Maintenance Network menu prompts the user for the standalone PDB O&M Network IP addresses. The user is allowed to access the EPAP CLI through the configured IP only. This menu is available only on the standalone PDB sites. The IP configured through this menu is used for the SSH operations.

    ```
    EPAP A Operations and Maintenance network IP Address [192.168.4.10]:
    EPAP Operations and Maintenance network netmask [255.255.255.0]:
    EPAP Operations and Maintenance network route [192.168.4.1]:
    ```

11. Press **Return** to return to the Configure Network Interfaces Menu. Choose `2` or `4` (depending on the Menu displayed by the Network Type Configuration), Configure Backup Provisioning Network.

    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 5-1 through Table 5-4 for the correct addresses.

    The IP address for this interface must be on a different class C subnet than the primary Provisioning Network address. 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.

    ```
    EPAP A backup provisioning network IP Address [0.0.0.0]:
    EPAP backup provisioning network netmask [0.0.0.0]:
    EPAP backup provisioning network default route [0.0.0.0]:
    ```

12. 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 13 through 16 and proceed to 20, Configure Forwarded Ports.

13. Choose option `3` or `5` (depending on the Menu displayed by the Network Type Configuration), Configure Forwarded Ports.

```
 /-----Configure Forwarded Ports Menu------\
/------------------------------------------\
|  1 | Change EPAP A HTTP Port              |
|----|--------------------------------------|
|  2 | Change EPAP A HTTP SuExec Port       |
|----|--------------------------------------|
|  3 | Change EPAP A Banner Connection Port |
|----|--------------------------------------|
|  4 | Change PDBI Port                     |
|----|--------------------------------------|
|  5 | Change Remote MPS A HTTP Port        |
|----|--------------------------------------|
|  e | Exit                                 |
\------------------------------------------/
Enter choice:
```

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

    Refer to the information recorded in Table 5-1 for the correct information.

15. Enter the appropriate port information.

    Press return to return to the Configure Forwarded Ports Menu.

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

16. 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 17 through 20 for configuring static NAT and continue with 24.

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

```
 /-----Configure Static NAT Addresses Menu---\
/--------------------------------------------\
|  1 | Change EPAP A Static NAT Address       |
|----|----------------------------------------|
|  2 | Change Remote MPS A Static NAT Address |
|----|----------------------------------------|
|  e | Exit                                   |
\--------------------------------------------/

Enter Choice:
```

18. 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**.

19. Enter a valid NAT IP address from Table 5-1.

> **Note:**
>
> 127.0.0.1 is not a valid IP address for this operation. 0.0.0.0 is a valid IP address and can be used to reset the VIP/backup provisioning IP address.

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

20. Choose option `e` on theConfigure Static NAT Addresses Menu to return to the Configure Network Interfaces Menu.
21. 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 (5), skip menu option 3. Proceed to 30.

22. 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                          |
|----|-----------------------------------|
| 10 | SNMP Configuration                |
|----|-----------------------------------|
| 11 | Configure Alarm Feed              |
|----|-----------------------------------|
| 12 | Configure Query Server            |
|----|-----------------------------------|
| 13 | Configure Query Server Alarm Feed |
```

```
|----|-----------------------------------|
| 14 | Configure SNMP Agent Community    |
|----|-----------------------------------|
|  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...
```

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

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

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

24. 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 B, List of Time Zones.

    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 MPS is rebooted.

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

> **Note:**
>
> Option `1`, Exchange**Secure 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 28.

25. Choose option `1` , Exchange Secure shell Keys.

```
 /-------Exchange Secure Shell Keys Menu-----\
/--------------------------------------------\
|  1 | Exchange Keys with Remote             |
|----|---------------------------------------|
|  e | Exit                                  |
\--------------------------------------------/
Enter Choice:
```

A prompt appears:

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

26. Enter `y`.

You are prompted for a Remote IP Address:

```
Temote IP Address:
```

27. Enter a valid IP address and Press **Return**.

```
Passord for EPAPdev@<above IP>:
```

You are prompted for the password of the remote. Contact My Oracle Support 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 option `5` and proceed to 36.

28. Enter option `5`, Change Password, to change the text-based user interface password for the `epapconfig` login name for the MPS A 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                         |
|----|----------------------------------|
| 10 | SNMP Configuration               |
|----|----------------------------------|
| 11 | Configure Alarm Feed             |
|----|----------------------------------|
| 12 | Configure Query Server           |
|----|----------------------------------|
| 13 | Configure Query Server Alarm Feed |
|----|----------------------------------|
| 14 | Configure SNMP Agent Community   |
|----|----------------------------------|
|  e | Exit                             |
\--------------------------------------/

Enter Choice: 5
```

You are prompted to confirm the action of changing the password for MPS A Server at this site.

```
Verifying connectivity with mate...
Are you sure you wish to change the text UI password on MPS A? [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.

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

> **Note:**
>
> If you do not want to add an**NTP** server at this time, skip all steps related to option`7` and proceed to 42.

30. 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                          |
|----|-----------------------------------|
| 10 | SNMP Configuration                |
|----|-----------------------------------|
| 11 | Configure Alarm Feed              |
|----|-----------------------------------|
| 12 | Configure Query Server            |
|----|-----------------------------------|
| 13 | Configure Query Server Alarm Feed |
|----|-----------------------------------|
| 14 | Configure SNMP Agent Community    |
|----|-----------------------------------|
|  e | Exit                              |
\-----------------------------------------/

Enter Choice: 7
```

31. 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. 0.0.0.0 is a valid IP address and can be used to reset the VIP/backup provisioning IP address.

The display shows the server verification occurring. A confirmation of a successful addition of the NTP server also appears.

32. Press **Return** to return to the EPAP Configure NTP Server Menu.
33. 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...
```

34. If the External NTP Server IP address is correct, press **Return** to return to the EPAP Configure NTP Server Menu.
35. 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
```

36. 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                       |
|----|--------------------------------|
| 10 | SNMP Configuration             |
|----|--------------------------------|
| 11 | Configure Alarm Feed           |
|----|--------------------------------|
| 12 | Configure Query Server         |
|----|--------------------------------|
| 13 | Configure Query Server Alarm Feed |
|----|--------------------------------|
| 14 | Configure SNMP Agent Community |
|----|--------------------------------|
|  e | Exit                           |
\-------------------------------------/

Enter Choice: 8


 /-----PDB Configuration Menu--------\
/-------------------------------------\
|  1 | Configure PDB Network          |
|----|--------------------------------|
|  2 | Create PDB                     |
```

```
|----|-------------------------------|
|  3 | Change Auto DB Recovery State  |
|----|-------------------------------|
|  e | Exit                          |
\-----------------------------------/
Enter Choice:
```

37. Enter option `1`, Configure PDB Network.

> **Note:**
>
> The Configure PDB Network menu prompts the user for the remote PDB IP Address. Unlike the mixed EPAP, the Standalone PDB site only asks for the PDBA A IP Address, not both A and B.

> **Note:**
>
> 127.0.0.1 is not a valid IP address for this operation. 0.0.0.0 is a valid IP address and can be used to reset the VIP/backup provisioning IP address.

38. Enter option `2`, Create PDB.

```
 /-----PDB Configuration Menu--------\
/-------------------------------------\
|  1 | Configure PDB Network          |
|----|-------------------------------|
|  2 | Create PDB                     |
|----|-------------------------------|
|  3 | Change Auto DB Recovery State  |
|----|-------------------------------|
|  e | Exit                          |
\-----------------------------------/
Enter Choice: 2
```

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 PDB, you are returned to the PDB Configuration Menu.

39. Enter option `3`, Change Auto DB Recovery, to enable the Automated Database Recovery feature.

```
 /-----PDB Configuration Menu--------\
/-------------------------------------\
|  1 | Configure PDB Network          |
|----|-------------------------------|
|  2 | Create PDB                     |
|----|-------------------------------|
|  3 | Change Auto DB Recovery State  |
|----|-------------------------------|
```

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

The following output appears.

```
Auto DB Recovery is currently DISABLED.
Do you want to ENABLE Auto DB Recovery? [N]: y
```

40. Enter option `e` to exit the PDB Configuration Menu and return to the EPAP Configuration Menu.
41. 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                          |
|----|-----------------------------------|
| 10 | SNMP Configuration                |
|----|-----------------------------------|
| 11 | Configure Alarm Feed              |
|----|-----------------------------------|
| 12 | Configure Query Server            |
|----|-----------------------------------|
| 13 | Configure Query Server Alarm Feed |
|----|-----------------------------------|
| 14 | Configure SNMP Agent Community    |
|----|-----------------------------------|
|  e | Exit                              |
\---------------------------------------/

Enter Choice: 6
```

```
/-----EPAP Platform Menu-\
/------------------------\
|  1 | Initiate Upgrade   |
```

```
|----|--------------------|
|  2 | Reboot MPS         |
|----|--------------------|
|  3 | MySQL Backup       |
|----|--------------------|
|  4 | PDB BACKUP         |
|----|--------------------|
|  e | Exit               |
\------------------------/
Enter Choice: 2
```

Enter option `2`, Reboot MPS.

The server is rebooted without further prompt.

6.6 Standalone PDB Capacity Configuration

Update the text as "With the 480GB disk on E5-APP-B-02, the maximum DB size of 1080M data entries can be supported in a Standalone PDB configuration. The 1110M data consists of 510M of DN and 600M of IMSI+IMEI.

The DB maximum capacity is configurable in the epapconfig menu only in the Standalone PDB running "eXtreme" DB architecture. See DB Architecture Menu.

The PDB Configuration Menu contains a **Configure PDB Capacity** sub-menu:

```
/-----PDB Capacity Menu--------------\
/-----------------------------------\
|  1 | Display current max Capacity   |
|----|--------------------------------|
|  2 | Set DN, IMSI/IMEI max Capacity |
|----|--------------------------------|
|  3 | Set DNBLK max capacity         |
|----|--------------------------------|
|  4 | Set EIRBLK max capacity        |
|----|--------------------------------|
|  e | Exit                           |
\-----------------------------------/
```

`Option 2`, **Set DN, IMSI/IMEI max Capacity**, allows users to input the following parameters in order to configure the PDB maximum Capacity:

1. To select if the EAGLE SM card type and EPAP Data Split feature status:

```
For Standalone PDB:
/-----SM card type--------------------\
|----|--------------------------------|
|  1 | SLIC with Data Split OFF       |
|----|--------------------------------|
|  2 | SLIC with Data Split ON        |
|----|--------------------------------|
|  e | Exit                           |
\-----------------------------------/
```

`Option 1` - Supported max Data size: Mixed - 480M DN/IMSI/IMEI

`Option 2` - Supported max Data size: 420M DN + 480M IMSI/IMEI, total 900M (Set this capacity if all fields are provisioned in DN);

`Option 2` - Supported max Data size: 510M DN + 600M IMSI/IMEI, total 1080M

2. Choose the supported data capacities after selecting the options in the previous step:

   If SLIC with Data Split OFF is selected (only available on Standalone PDB):

```
/-----Data Capacity ------------------\
/-------------------------------------\
|  1 | 510M DN/IMSI/IMEI               |
|----|---------------------------------|
|  e | Exit                            |
|----|---------------------------------|
```

   If SLIC with Data Split ON is selected (only available on Standalone PDB):

```
/-----Data Capacity ------------------\
/-------------------------------------\
|  1 | 420M DN + 480M IMSI/IMEI        |
|----|---------------------------------|
|  2 | 510M DN + 600M IMSI/IMEI        |
|----|---------------------------------|
|  e | Exit                            |
|----|---------------------------------|
```

3. Choose the supported DNBLK and EIRBLK capacities:
   - DNBLK: 400K, 800K, or 1600K
   - EIRBLK: 100K, 200K, or 800K

```
/----- DNBLK Capacity ----------------\
/-------------------------------------\
|  1 | 400K DNBLK                     |
|----|---------------------------------|
|  2 | 800K DNBLK                     |
|----|---------------------------------|
|  3 | 1600K DNBLK                    |
|----|---------------------------------|
|  e | Exit                           |
|----|---------------------------------|
```

```
/----- EIRBLK Capacity ---------------\
/-------------------------------------\
|  1 | 100K EIRBLK                    |
|----|---------------------------------|
|  2 | 200K EIRBLK                    |
|----|---------------------------------|
|  3 | 800K EIRBLK                    |
|----|---------------------------------|
```

```
|  e | Exit                           |
|----|--------------------------------|
```

The menu will verify the EAGLE SM card type and EPAP Data Split feature status.
The menu will also verify if the disk and DB partition is big enough to support the requested capacity.

A

E5-APP-B Card Removal

This appendix describes the procedure to shut down the EPAP prior to removing the E5-APP-B card.

A.1 Shutting Down the EPAP and Removing the E5-APP-B Card

The EPAP application must be shut down prior to removing an E5-APP-B card. Perform the following procedure to properly remove the card:

1. Stop the EPAP service.
2. Stop the PDBA service.
3. Execute the `shutdown` command.
4. Slide the front switch and remove the card once all LEDs turn off (see "Removing an E5-APP-B Card" in *Application B Card Hardware and Installation Guide*).

B
Time Zones

This appendix displays a list of time zones that are valid while configuring 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 default value for the time zone is “US/Eastern”.

B.1 List of Time Zones

```
Enter Choice: 3
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...
Verifying connectivity with mate...
Are you sure you wish to change the timezone for MPS A and B? [N]: Y
EPAP software and PDBA are running.  Stop them? [N]: Y
Enter a time zone: df
Time zone df does not exist
Valid time zones are:

Africa/Abidjan                  Africa/Accra
Africa/Addis_Ababa              Africa/Algiers
Africa/Asmara                   Africa/Asmera
Africa/Bamako                   Africa/Bangui
Africa/Banjul                   Africa/Bissau
Africa/Blantyre                 Africa/Brazzaville
Africa/Bujumbura                Africa/Cairo
Africa/Casablanca               Africa/Ceuta
Africa/Conakry                  Africa/Dakar
Africa/Dar_es_Salaam            Africa/Djibouti
Africa/Douala                   Africa/El_Aaiun
Africa/Freetown                 Africa/Gaborone
Africa/Harare                   Africa/Johannesburg
Africa/Juba                     Africa/Kampala
Africa/Khartoum                 Africa/Kigali
Africa/Kinshasa                 Africa/Lagos
Africa/Libreville               Africa/Lome
Africa/Luanda                   Africa/Lubumbashi
Africa/Lusaka                   Africa/Malabo
Africa/Maputo                   Africa/Maseru
Africa/Mbabane                  Africa/Mogadishu
Africa/Monrovia                 Africa/Nairobi
Africa/Ndjamena                 Africa/Niamey
Africa/Nouakchott               Africa/Ouagadougou
Africa/Porto-Novo               Africa/Sao_Tome
Africa/Timbuktu                 Africa/Tripoli
```

```
Africa/Tunis                        Africa/Windhoek
America/Adak                        America/Anchorage
America/Anguilla                    America/Antigua
America/Araguaina                   America/Argentina/Buenos_Aires
America/Argentina/Catamarca         America/Argentina/ComodRivadavia
America/Argentina/Cordoba           America/Argentina/Jujuy
America/Argentina/La_Rioja          America/Argentina/Mendoza
America/Argentina/Rio_Gallegos      America/Argentina/Salta
America/Argentina/San_Juan          America/Argentina/San_Luis
America/Argentina/Tucuman           America/Argentina/Ushuaia
America/Aruba                       America/Asuncion
America/Atikokan                    America/Atka
America/Bahia                       America/Bahia_Banderas
America/Barbados                    America/Belem
America/Belize                      America/Blanc-Sablon
America/Boa_Vista                   America/Bogota
America/Boise                       America/Buenos_Aires
America/Cambridge_Bay               America/Campo_Grande
America/Cancun                      America/Caracas
America/Catamarca                   America/Cayenne
America/Cayman                      America/Chicago
America/Chihuahua                   America/Coral_Harbour
America/Cordoba                     America/Costa_Rica
America/Creston                     America/Cuiaba
America/Curacao                     America/Danmarkshavn
America/Dawson                      America/Dawson_Creek
America/Denver                      America/Detroit
America/Dominica                    America/Edmonton
America/Eirunepe                    America/El_Salvador
America/Ensenada                    America/Fort_Nelson
America/Fort_Wayne                  America/Fortaleza
America/Glace_Bay                   America/Godthab
America/Goose_Bay                   America/Grand_Turk
America/Grenada                     America/Guadeloupe
America/Guatemala                   America/Guayaquil
America/Guyana                      America/Halifax
America/Havana                      America/Hermosillo
America/Indiana/Indianapolis        America/Indiana/Knox
America/Indiana/Marengo             America/Indiana/Petersburg
America/Indiana/Tell_City           America/Indiana/Vevay
America/Indiana/Vincennes           America/Indiana/Winamac
America/Indianapolis                America/Inuvik
America/Iqaluit                     America/Jamaica
America/Jujuy                       America/Juneau
America/Kentucky/Louisville         America/Kentucky/Monticello
America/Knox_IN                     America/Kralendijk
America/La_Paz                      America/Lima
America/Los_Angeles                 America/Louisville
America/Lower_Princes               America/Maceio
America/Managua                     America/Manaus
America/Marigot                     America/Martinique
America/Matamoros                   America/Mazatlan
America/Mendoza                     America/Menominee
America/Merida                      America/Metlakatla
America/Mexico_City                 America/Miquelon
America/Moncton                     America/Monterrey
```

America/Montevideo
America/Montreal
America/Montserrat
America/Nassau
America/New_York
America/Nipigon
America/Nome
America/Noronha
America/North_Dakota/Beulah
America/North_Dakota/Center
America/North_Dakota/New_Salem
America/Ojinaga
America/Panama
America/Pangnirtung
America/Paramaribo
America/Phoenix
America/Port-au-Prince
America/Port_of_Spain
America/Porto_Acre
America/Porto_Velho
America/Puerto_Rico
America/Punta_Arenas
America/Rainy_River
America/Rankin_Inlet
America/Recife
America/Regina
America/Resolute
America/Rio_Branco
America/Rosario
America/Santa_Isabel
America/Santarem
America/Santiago
America/Santo_Domingo
America/Sao_Paulo
America/Scoresbysund
America/Shiprock
America/Sitka
America/St_Barthelemy
America/St_Johns
America/St_Kitts
America/St_Lucia
America/St_Thomas
America/St_Vincent
America/Swift_Current
America/Tegucigalpa
America/Thule
America/Thunder_Bay
America/Tijuana
America/Toronto
America/Tortola
America/Vancouver
America/Virgin
America/Whitehorse
America/Winnipeg
America/Yakutat
America/Yellowknife
Antarctica/Casey
Antarctica/Davis
Antarctica/DumontDUrville
Antarctica/Macquarie
Antarctica/Mawson
Antarctica/McMurdo
Antarctica/Palmer
Antarctica/Rothera
Antarctica/South_Pole
Antarctica/Syowa
Antarctica/Troll
Antarctica/Vostok
Arctic/Longyearbyen
Asia/Aden
Asia/Almaty
Asia/Amman
Asia/Anadyr
Asia/Aqtau
Asia/Aqtobe
Asia/Ashgabat
Asia/Ashkhabad
Asia/Atyrau
Asia/Baghdad
Asia/Bahrain
Asia/Baku
Asia/Bangkok
Asia/Barnaul
Asia/Beirut
Asia/Bishkek
Asia/Brunei
Asia/Calcutta
Asia/Chita
Asia/Choibalsan
Asia/Chongqing
Asia/Chungking
Asia/Colombo
Asia/Dacca
Asia/Damascus
Asia/Dhaka
Asia/Dili
Asia/Dubai
Asia/Dushanbe
Asia/Famagusta
Asia/Gaza
Asia/Harbin
Asia/Hebron
Asia/Ho_Chi_Minh
Asia/Hong_Kong
Asia/Hovd
Asia/Irkutsk
Asia/Istanbul
Asia/Jakarta
Asia/Jayapura
Asia/Jerusalem
Asia/Kabul
Asia/Kamchatka

Asia/Karachi
Asia/Kashgar
Asia/Kathmandu
Asia/Katmandu
Asia/Khandyga
Asia/Kolkata
Asia/Krasnoyarsk
Asia/Kuala_Lumpur
Asia/Kuching
Asia/Kuwait
Asia/Macao
Asia/Macau
Asia/Magadan
Asia/Makassar
Asia/Manila
Asia/Muscat
Asia/Nicosia
Asia/Novokuznetsk
Asia/Novosibirsk
Asia/Omsk
Asia/Oral
Asia/Phnom_Penh
Asia/Pontianak
Asia/Pyongyang
Asia/Qatar
Asia/Qostanay
Asia/Qyzylorda
Asia/Rangoon
Asia/Riyadh
Asia/Saigon
Asia/Sakhalin
Asia/Samarkand
Asia/Seoul
Asia/Shanghai
Asia/Singapore
Asia/Srednekolymsk
Asia/Taipei
Asia/Tashkent
Asia/Tbilisi
Asia/Tehran
Asia/Tel_Aviv
Asia/Thimbu
Asia/Thimphu
Asia/Tokyo
Asia/Tomsk
Asia/Ujung_Pandang
Asia/Ulaanbaatar
Asia/Ulan_Bator
Asia/Urumqi
Asia/Ust-Nera
Asia/Vientiane
Asia/Vladivostok
Asia/Yakutsk
Asia/Yangon
Asia/Yekaterinburg
Asia/Yerevan
Atlantic/Azores
Atlantic/Bermuda
Atlantic/Canary
Atlantic/Cape_Verde
Atlantic/Faeroe
Atlantic/Faroe
Atlantic/Jan_Mayen
Atlantic/Madeira
Atlantic/Reykjavik
Atlantic/South_Georgia
Atlantic/St_Helena
Atlantic/Stanley
Australia/ACT
Australia/Adelaide
Australia/Brisbane
Australia/Broken_Hill
Australia/Canberra
Australia/Currie
Australia/Darwin
Australia/Eucla
Australia/Hobart
Australia/LHI
Australia/Lindeman
Australia/Lord_Howe
Australia/Melbourne
Australia/NSW
Australia/North
Australia/Perth
Australia/Queensland
Australia/South
Australia/Sydney
Australia/Tasmania
Australia/Victoria
Australia/West
Australia/Yancowinna
Brazil/Acre
Brazil/DeNoronha
Brazil/East
Brazil/West
CET
CST6CDT
Canada/Atlantic
Canada/Central
Canada/Eastern
Canada/Mountain
Canada/Newfoundland
Canada/Pacific
Canada/Saskatchewan
Canada/Yukon
Chile/Continental
Chile/EasterIsland
Cuba
EET
EST
EST5EDT
Egypt

```
Eire
Etc/GMT+0
Etc/GMT+10
Etc/GMT+12
Etc/GMT+3
Etc/GMT+5
Etc/GMT+7
Etc/GMT+9
Etc/GMT-1
Etc/GMT-11
Etc/GMT-13
Etc/GMT-2
Etc/GMT-4
Etc/GMT-6
Etc/GMT-8
Etc/GMT0
Etc/UCT
Etc/Universal
Europe/Amsterdam
Europe/Astrakhan
Europe/Belfast
Europe/Berlin
Europe/Brussels
Europe/Budapest
Europe/Chisinau
Europe/Dublin
Europe/Guernsey
Europe/Isle_of_Man
Europe/Jersey
Europe/Kiev
Europe/Lisbon
Europe/London
Europe/Madrid
Europe/Mariehamn
Europe/Monaco
Europe/Nicosia
Europe/Paris
Europe/Prague
Europe/Rome
Europe/San_Marino
Europe/Saratov
Europe/Skopje
Europe/Stockholm
Europe/Tirane
Europe/Ulyanovsk
Europe/Vaduz
Europe/Vienna
Europe/Volgograd
Europe/Zagreb
Europe/Zurich
GB-Eire
GMT+0
GMT0
HST
Iceland
Indian/Chagos
Etc/GMT
Etc/GMT+1
Etc/GMT+11
Etc/GMT+2
Etc/GMT+4
Etc/GMT+6
Etc/GMT+8
Etc/GMT-0
Etc/GMT-10
Etc/GMT-12
Etc/GMT-14
Etc/GMT-3
Etc/GMT-5
Etc/GMT-7
Etc/GMT-9
Etc/Greenwich
Etc/UTC
Etc/Zulu
Europe/Andorra
Europe/Athens
Europe/Belgrade
Europe/Bratislava
Europe/Bucharest
Europe/Busingen
Europe/Copenhagen
Europe/Gibraltar
Europe/Helsinki
Europe/Istanbul
Europe/Kaliningrad
Europe/Kirov
Europe/Ljubljana
Europe/Luxembourg
Europe/Malta
Europe/Minsk
Europe/Moscow
Europe/Oslo
Europe/Podgorica
Europe/Riga
Europe/Samara
Europe/Sarajevo
Europe/Simferopol
Europe/Sofia
Europe/Tallinn
Europe/Tiraspol
Europe/Uzhgorod
Europe/Vatican
Europe/Vilnius
Europe/Warsaw
Europe/Zaporozhye
GB
GMT
GMT-0
Greenwich
Hongkong
Indian/Antananarivo
Indian/Christmas
```

Indian/Cocos
Indian/Comoro
Indian/Kerguelen
Indian/Mahe
Indian/Maldives
Indian/Mauritius
Indian/Mayotte
Indian/Reunion
Iran
Israel
Jamaica
Japan
Kwajalein
Libya
MET
MST
MST7MDT
Mexico/BajaNorte
Mexico/BajaSur
Mexico/General
NZ
NZ-CHAT
Navajo
PRC
PST8PDT
Pacific/Apia
Pacific/Auckland
Pacific/Bougainville
Pacific/Chatham
Pacific/Chuuk
Pacific/Easter
Pacific/Efate
Pacific/Enderbury
Pacific/Fakaofo
Pacific/Fiji
Pacific/Funafuti
Pacific/Galapagos
Pacific/Gambier
Pacific/Guadalcanal
Pacific/Guam
Pacific/Honolulu
Pacific/Johnston
Pacific/Kiritimati
Pacific/Kosrae
Pacific/Kwajalein
Pacific/Majuro
Pacific/Marquesas
Pacific/Midway
Pacific/Nauru
Pacific/Niue
Pacific/Norfolk
Pacific/Noumea
Pacific/Pago_Pago
Pacific/Palau
Pacific/Pitcairn
Pacific/Pohnpei
Pacific/Ponape
Pacific/Port_Moresby
Pacific/Rarotonga
Pacific/Saipan
Pacific/Samoa
Pacific/Tahiti
Pacific/Tarawa
Pacific/Tongatapu
Pacific/Truk
Pacific/Wake
Pacific/Wallis
Pacific/Yap
Poland
Portugal
ROC
ROK
Singapore
Turkey
UCT
US/Alaska
US/Aleutian
US/Arizona
US/Central
US/East-Indiana
US/Eastern
US/Hawaii
US/Indiana-Starke
US/Michigan
US/Mountain
US/Pacific
US/Pacific-New
US/Samoa
UTC
Universal
W-SU
WET
Zulu