Oracle® Communications EAGLE Application Processor

Security Guide

Release 16.0

E54371 Revision 1

October 2014

Oracle® Communications Security Guide, Release 16.0

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

Topics:

This chapter contains general information such as an overview of the manual, how to get technical assistance, and where to find additional information.

Overview

This document provides guidelines and recommendations for configuring the Oracle Communications EAGLE Application Processor (EPAP) to enhance the security of the system. The recommendations herein are optional and should be considered along with the approved security strategies of your organization. Additional configuration changes that are not included herein are not recommended and may hinder the product's operation or Oracle's capability to provide appropriate support.

Scope and Audience

This guide is intended for administrators that are responsible for product and network security.

Documentation Admonishments

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

Table 1: Admonishments

Icon	Description
DANGER	**Danger**: (This icon and text indicate the possibility of *personal injury*.)
WARNING	**Warning**: (This icon and text indicate the possibility of *equipment damage*.)
CAUTION	**Caution**: (This icon and text indicate the possibility of *service interruption*.)
TOPPLE	**Topple**: (This icon and text indicate the possibility of *personal injury* and *equipment damage*.)

My Oracle Support (MOS)

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

Call the CAS 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:

1. Select **2** for New Service Request
2. Select **3** for Hardware, Networking and Solaris Operating System Support
3. Select **2** for Non-technical issue

You will be connected to a live agent who can assist you with MOS registration and provide Support Identifiers. Simply mention you are a Tekelec Customer new to MOS.

MOS is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at **1-800-223-1711** (toll-free in the US), or by calling the Oracle Support hotline for your local country from the list at *http://www.oracle.com/us/support/contact/index.html*. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

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

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

Related Publications

For information about additional publications that are related to this document, refer to the *Related Publications Reference* document, which is published as a separate document on the Oracle Technology

Network (OTN) site. See *Locate Product Documentation on the Oracle Technology Network Site* for more information.

Locate Product Documentation on the Oracle Technology Network Site

Oracle customer documentation is available on the web at the Oracle Technology Network (OTN) site, *http://docs.oracle.com*. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at *www.adobe.com*.

1. Log into the Oracle Technology Network site at *http://docs.oracle.com*.
2. Under **Applications**, click the link for **Communications**.
   The **Oracle Communications Documentation** window opens with Tekelec shown near the top.
3. Click **Oracle Communications Documentation for Tekelec Products**.
4. Navigate to your Product and then the Release Number, and click the **View** link (the **Download** link will retrieve the entire documentation set).
5. To download a file to your location, right-click the PDF link and select **Save Target As**.

Chapter 2

EPAP Security Overview

Topics:

This chapter describes basic security considerations and provides an overview of EPAP security.

Basic Security Considerations

The following principles are fundamental to using any application securely:

- **Keep software up to date.** This includes the latest product release and any patches that apply to it. Consult with your Oracle support team to plan for EPAP software upgrades.
- **Limit privileges as much as possible.** Users should be given only the access necessary to perform their work. User privileges should be reviewed periodically to determine relevance to current work requirements.
- **Monitor system activity.** Establish who should access which system components, and how often, and monitor those components.
- **Install software securely.** For example, use firewalls, secure protocols such as SSL, and strong passwords.
- **Learn about and use the EPAP security features.** See *Implementing EPAP Security* for more information.
- **Keep up to date on security information.** Oracle regularly issues security-related patch updates and security alerts. You must install all security patches as soon as possible. See the "Critical Patch Updates and Security Alerts" Web site: *http://www.oracle.com/technetwork/topics/security/alerts-086861.html*

Overview of EPAP Security

The 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)

The 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 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.

Recommended Deployment Configurations

The EPAP is deployed in the central office of the carrier and service provider, co-located with the EAGLE STP. The customer network should be secured via firewall, and making the EPAP provisioning network its own private network or VLAN is further recommended where possible. For a generic model of the deployment strategy, see *Figure 1: Generic EPAP Deployment Model*.

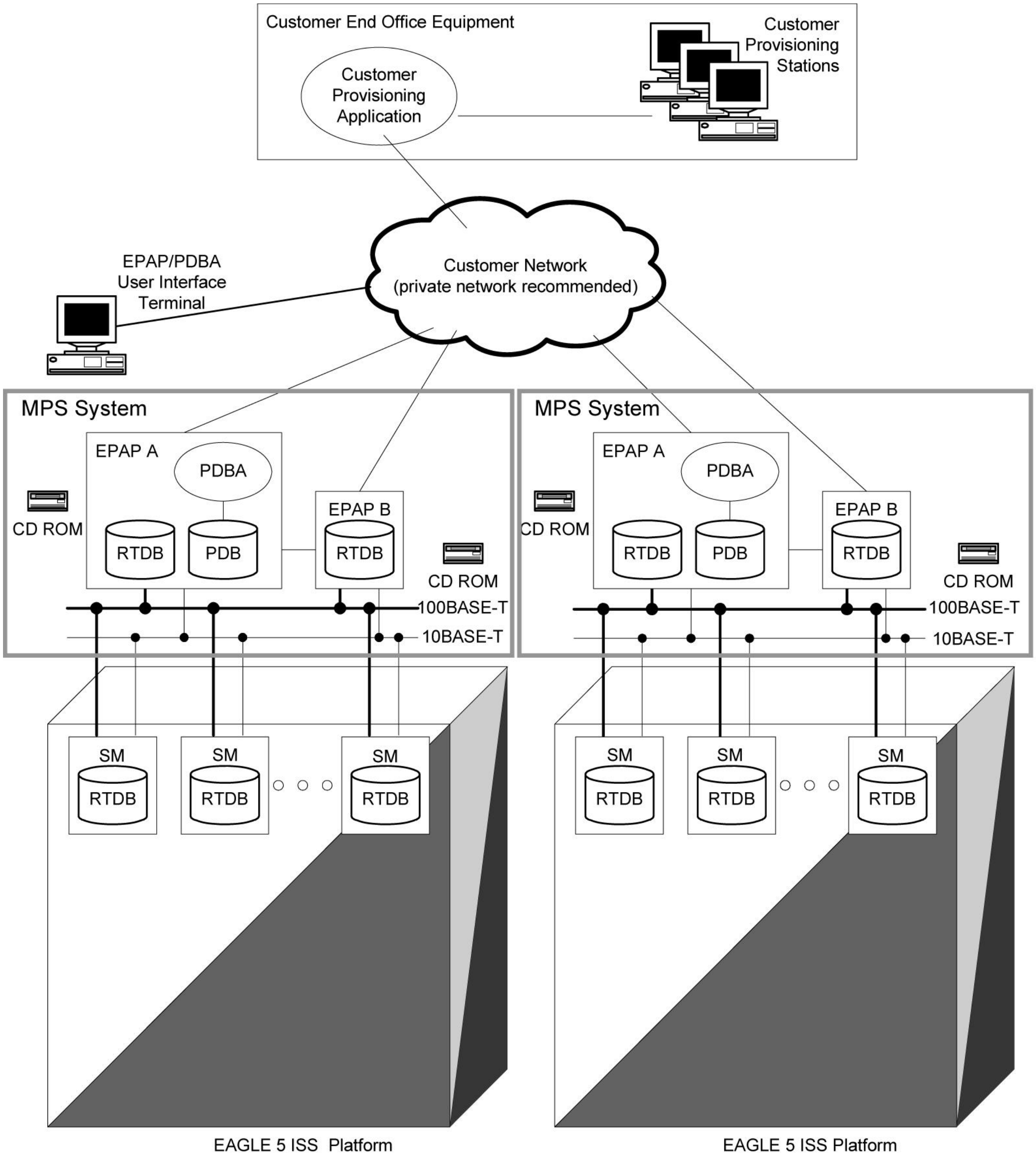

Figure 1: Generic EPAP Deployment Model

In addition to the firewalls, the EPAP system provides additional security capabilities that include application-specific remote IP address control.

Chapter 3

Implementing EPAP Security

Topics:

This chapter explains security related configuration settings that may be applied to the EPAP.

User and Group Administration

The EPAP user interface (UI) comes pre-defined with UI users to provide a seamless transition to the GUI. For instance, there is a pre-defined user that is used to access the **User Administration** menu, as shown in *Table 2: EPAP UI Logins*.

Table 2: 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 **User Administration** menu is used to set up and perform administrative functions for users and groups, and also to terminate active sessions and modify system defaults.

Establishing Groups and Group Privileges

Each user is assigned to a group, and permissions to a set of functions are assigned to the group. The permissions determine the functions and restrictions for the users belonging to the group. EPAP users can fall into one of the following default groups:

- maint
- database
- platform
- debug
- pdba
- admin
- readonly

The readonly group is the default group for new users. The readonly group contains only actions that view status and information.

The **User Administration** > **Groups** menu allows administrator access to group functions to add, modify, delete, and retrieve a group. For more information, see *Groups* under *User Administration Menu* in *Administration Guide*.

Creating Users and Assigning to Groups

Each user that is allowed access to the user interface is assigned a unique username. This username and associated password must be provided during login.

Prior to adding a user, determine which group the user should be assigned based on their operational role. The group assignment determines the functions that a user can access.

After determining the proper group for a user, use the **User Administration** > **Users** menu to add the user.

The **User Administration** > **Users** menu can also be used to modify, delete, and retrieve user accounts, and to reset passwords. For more information, see *Users* under *User Administration Menu* in *Administration Guide*.

User Authentication

Users are authenticated using login credentials. Each user that is allowed access to the UI is assigned a unique username. This username and associated password must be provided during login.

Password Restrictions

Before beginning to use EPAP for provisioning, the EPAP software must be configured and initialized. During configuration, default password restrictions such as password aging and minimum password size can be changed via the **EPAP Configuration** > **Security** menu. For more information, see *Security* under *EPAP Configuration Menu* in *Administration Guide*.

The UI 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. For information about modifying system-wide defaults, see *Modify Defaults* under *User Administration Menu* in *Administration Guide*. For information about user-specific settings, see *Users* under *User Administration Menu* in *Administration Guide*.

For information about topics such as password complexity, password aging, and password reuse, see *Change Password* under *EPAP Graphical User Interface Menus* in *Administration Guide*.

Changing Default Passwords for EPAP Administrative Account

As a security measure, the uiadmin and root passwords must be changed from their default values to user-defined values. For more information, see *Secure Turnover to Customer*.

Changing User Passwords

The **Change Password** screen of the EPAP GUI main menu provides all EPAP users with the capability to change their password. 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.

Password Change for System Users

The epapdev and appuser users can 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.

Modifying System Defaults

The **User Administration** > **Modify System Defaults** screen enables the administrator to manage system defaults. Use this screen to control settings such as maximum failed login attempts before disabling a user account, maximum account inactivity, maximum password age, and minimum password length. For more information, see *Modify Defaults* under *User Administration Menu* in *Administration Guide*.

SNMP Configuration

EPAP can use the industry-standard Simple Network Management Protocol (SNMP) interface to send alarms as trap messages to an EMS. EPAP sends SNMPv2c traps to the EMS if the configurable parameter SNMP Alarm Feed is set to **ON**. EPAP also supports GET and SET of the resyncVar MIB element.

The active EPAP server provides a single interface to SNMP data for the EPAP pair. For network configurations using the Stand-Alone PDBI feature, the PDBI provides its own SNMP interface directly with SNMP managers. The application sends SNMP traps to SNMP managers that are registered to receive traps.

Community Names / Strings

The default community names configured for Read and Write in the snmpd.conf file are epapRdSnmp and epapWrSnmp. You should change the default community names to prevent unauthorized access. Always use different names for the Read community and Write community.

For more information about SNMP Configuration, see *Administration Guide*.

Authorized IP Addresses

The **User Administration** > **Authorized IP** menu enables you to add, remove, and list authorized IP addresses, and to change the IP address authorization status. The IP addresses are authorized for both GUI and server access. For more information, see *EPAP Security Enhancements*, and *Authorized IPs* under *User Administration Menu*, in *Administration Guide*.

The PDBA maintains a list of IP addresses that are allowed to connect through the PDBI. Any connect request coming from an IP address that is not in the list is rejected. Each IP address in the list has either READ or READ/WRITE permission. The **PDBA** > **Authorized IP List** menu enables you to add, modify, remove, and list the IP addresses authorized to connect to the PDBA through the PDB. For more information, see *Authorized IP List* under *PDBA Menu* in *Administration Guide*.

Appendix A

Secure Deployment Checklist

Use the following security checklist to help secure EPAP and its components:

- Change default passwords
- Set strong password restrictions
- Restrict admin functions to the required administrator groups
- Utilize the Authorized IP addresses feature

Appendix B

Secure Turnover to Customer

Topics:

To ensure security of systems delivered to our customers and to satisfy Oracle policies, all passwords must be owned by the customer once transfer of ownership of systems has occurred.

Secure Turnover Process

Three key requirements address the fundamental principles of the secure turnover process:

- Oracle default passwords shall not remain on fielded systems.
- Oracle default passwords shall not be revealed to customers.
- Customer installed passwords shall not be known by Oracle.

Goals of the Secure Turnover Process

Following are the goals of the password handoff process:

1. Install the system securely with Oracle internal default passwords (passwords exclusively known and used by Oracle personnel).
2. Change the special account passwords during the installation process to a unique value (meeting password complexity rules required by the system).
3. Provide a non-repudiation process for the customer agent to set all special passwords.

Secure Turnover Procedure

Perform the following steps for secure system turnover:

1. System servers are installed by Oracle personnel using common ISO deliverables and installation procedures. The OS root password, OS admusr password, and the passwords for the default EPAP UI login accounts are from the build process, and are private and known only by Oracle.
2. Following installation, the Oracle installer performs a login to each server OS (real and virtual) as admusr and changes the password to a new unique secure password. The Oracle installer then switches user to root and changes the root password to a new unique password.
3. The Oracle installer uses a web browser to log in to the application on each relevant server using each default EPAP UI login name (such as uiadmin) and changes the password to a new unique password.
4. As a precursor to the official handoff of the system (all servers) to the customer, the Oracle installer ensures that the new unique passwords for root, admusr, and default EPAP UI login accounts have been securely given to the authorized customer agent.
5. The authorized customer agent is instructed to log in to each OS account on each server (real and virtual) and change the password for accounts admusr and root to the authorized operational setting for the customer.
6. The customer agent is instructed to use a web browser to log in to each relevant application server and change the password for the default EPAP UI login accounts to the authorized operational password for the customer.
7. Following the entry of the new passwords by the customer agent, the Oracle installer or authorized Oracle agent attempts to log in to each server using the previously known password. This should result in a failed login attempt verifiable in the server logs.
8. The customer agent again logs in to each OS account and the default EPAP UI login accounts using the new customer passwords to verify success with the new customer passwords.

Glossary

E

EMS

Element Management System

The EMS feature consolidates real-time element management at a single point in the signaling network to reduce ongoing operational expenses and network downtime and provide a higher quality of customer service.

EPAP

EAGLE Provisioning Application Processor

EPAP-related features

Features that require EPAP connection and use the Real Time Database (RTDB) for lookup of subscriber information.

- ANSI Number Portability Query (AINPQ)
- ANSI-41 AnalyzedInformation Query – no EPAP/ELAP (ANSI41 AIQ)
- Anytime Interrogation Number Portability (ATI Number Portability, ATINP)
- AINPQ, INP, G-Port SRI Query for Prepaid, GSM MAP SRI Redirect, IGM, and ATINP Support for ROP
- A-Port Circular Route Prevention (A-Port CRP)
- Equipment Identity Register (EIR)
- G-Flex C7 Relay (G-Flex)
- G-Flex MAP Layer Routing (G-Flex MLR)
- G-Port SRI Query for Prepaid

E

- GSM MAP SRI Redirect to Serving HLR (GSM MAP SRI Redirect)
- GSM Number Portability (G-Port)
- IDP A-Party Blacklist
- IDP A-Party Routing
- IDP Relay Additional Subscriber Data (IDPR ASD)
- IDP Relay Generic Routing Number (IDPR GRN)
- IDP Service Key Routing (IDP SK Routing)
- IDP Screening for Prepaid
- INAP-based Number Portability (INP)
- Info Analyzed Relay Additional Subscriber Data (IAR ASD)
- Info Analyzed Relay Base (IAR Base)
- Info Analyzed Relay Generic Routing Number (IAR GRN)
- Info Analyzed Relay Number Portability (IAR NP)
- INP Circular Route Prevention (INP CRP)
- IS41 Mobile Number Portability (A-Port)
- IS41 GSM Migration (IGM)
- MNP Circular Route Prevention (MNPCRP)
- MO-based GSM SMS NP
- MO-based IS41 SMS NP
- MO SMS Generic Routing Number (MO SMS GRN)
- MO- SMS B-Party Routing
- MO SMS IS41-to-GSM Migration
- MT-based GSM SMS NP
- MT-based GSM MMS NP
- MT-based IS41 SMS NP
- MTP Routed Messages for SCCP Applications (MTP Msgs for SCCP Apps)

E

- MTP Routed Gateway Screening Stop Action (MTPRTD GWS Stop Action)
- Portability Check for MO SMS
- Prepaid IDP Query Relay (IDP Relay, IDPR)
- Prepaid SMS Intercept Phase 1 (PPSMS)
- Service Portability (S-Port)
- S-Port Subscriber Differentiation
- Triggerless ISUP Framework Additional Subscriber Data (TIF ASD)
- Triggerless ISUP Framework Generic Routing Number (TIF GRN)
- Triggerless ISUP Number Portability (TIF NP)
- Triggerless ISUP Framework Number Substitution (TIF NS)
- Triggerless ISUP Framework SCS Forwarding (TIF SCS Forwarding)
- Triggerless ISUP Framework Simple Number Substitution (TIF SNS)
- Voice Mail Router (V-Flex)

M

MIB

Management Information Database

A database of network management information that is used and maintained by the SNMP protocol.

MPS

Multi-Purpose Server

The Multi-Purpose Server provides database/reload functionality and a variety of high capacity/high speed offboard database functions for applications. The MPS resides in the General Purpose Frame.

M

Messages Per Second

A measure of a message processor's performance capacity. A message is any Diameter message (Request or Answer) which is received and processed by a message processor.

P

PDB

Provisioning Database

PDBA

Provisioning Database Application

There are two Provisioning Database Applications (PDBAs), one in EPAP A on each EAGLE. They follow an Active/Standby model. These processes are responsible for updating and maintaining the Provisioning Database (PDB).

PDBI

Provisioning Database Interface

The interface consists of the definition of provisioning messages only. The customer must write a client application that uses the PDBI request/response messages to communicate with the PDBA.

S

SNMP

Simple Network Management Protocol.

An industry-wide standard protocol used for network management. The SNMP agent maintains data variables that represent aspects of the network. These variables are called managed objects and are stored in a management information base (MIB). The SNMP protocol

S

arranges managed objects into groups.

SSL

Secure Socket Layer (SSL) is an industry standard protocol for clients needing to establish secure (TCP-based) SSL-enabled network connections

STP

Signal Transfer Point

The STP is a special high-speed switch for signaling messages in SS7 networks. The STP routes core INAP communication between the Service Switching Point (SSP) and the Service Control Point (SCP) over the network.

Spanning Tree Protocol

U

UI

User Interface

V

VLAN

Virtual Local Area Network

A logically independent network. A VLAN consists of a network of computers that function as though they were connected to the same wire when in fact they may be physically connected to different segments of a LAN. VLANs are configured through software rather than hardware. Several VLANs can co-exist on a single physical switch.