# Oracle® Communications
# EAGLE LNP Application Processor

Security Guide

Release 10.0.1

**E57610 Revision 1**

November 2014

Oracle® Communications Security Guide, Release 10.0.1

# 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 LNP Application Processor (ELAP) 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**:<br>(This icon and text indicate the possibility of *personal injury*.) |
| WARNING | **Warning**:<br>(This icon and text indicate the possibility of *equipment damage*.) |
| CAUTION | **Caution**:<br>(This icon and text indicate the possibility of *service interruption*.) |
| TOPPLE | **Topple**:<br>(This icon and text indicate the possibility of *personal injury* and *equipment damage*.) |

## Manual Organization

This manual contains the following chapters:

- *Introduction* contains general information such as an overview of the manual, how to get technical assistance, and where to find more information.
- *ELAP Security Overview* describes basic security considerations and provides an overview of ELAP security.
- *Implementing ELAP Security* explains ELAP security features.
- *Secure Deployment Checklist* contains a security checklist to help secure ELAP.
- *Secure Turnover to Customer* describes the secure turnover process to ensure the security of delivered systems.

## 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 one of the following options:
   - For Technical issues such as creating a new Service Request (SR), Select **1**
   - For Non-technical issues such as registration or assistance with MOS, Select **2**

You will be connected to a live agent who can assist you with MOS registration and opening a support ticket.

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.

## Customer Training

Oracle University offers training for service providers and enterprises. Visit our web site to view, and register for, Oracle Communications training:

*http://education.oracle.com/communication*

To obtain contact phone numbers for countries or regions, visit the Oracle University Education web site:

*www.oracle.com/education/contacts*

## 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

# ELAP Security Overview

**Topics:**

This chapter describes basic security considerations and provides an overview of ELAP 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 ELAP 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 ELAP security features.** See *Implementing ELAP 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*

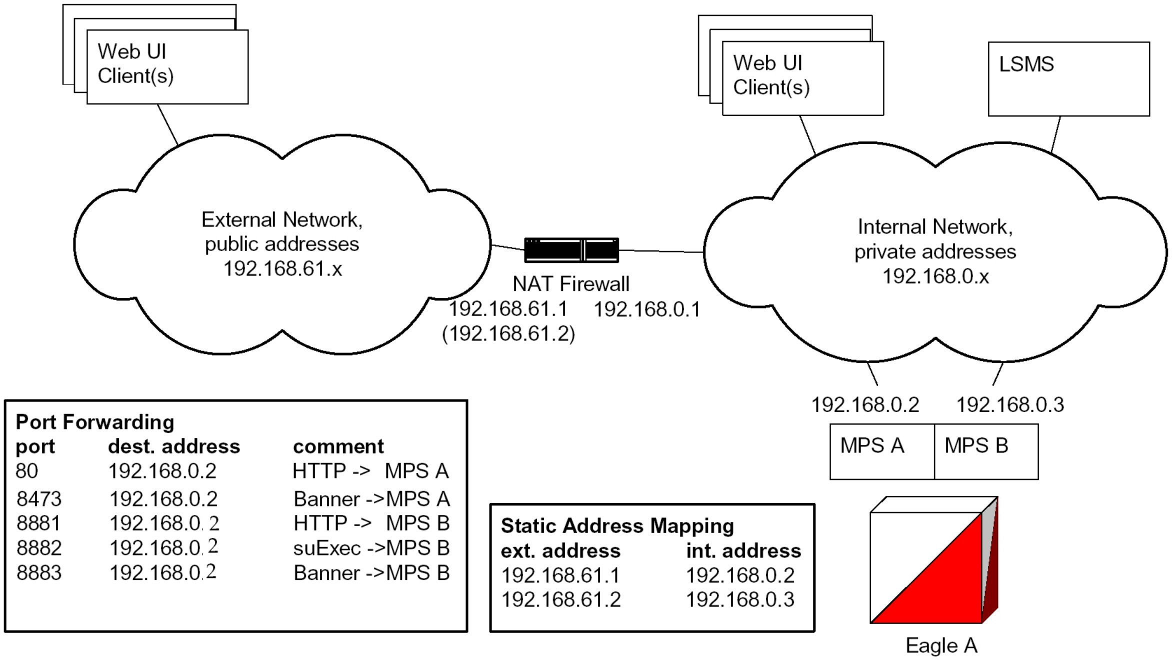
## Overview of ELAP Security

The main functions of the ELAP are:

- Accept and store data provisioned by the customer from LSMS over the provisioning network
- Update and reload provisioning data to the EAGLE Service Module cards

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

As shown in *Figure 1: Generic ELAP Deployment Model*, the MPS supports two types of network address translation (NAT), Port Forwarding and Static Address Mapping. In both cases, the MPS will have private IP addresses that are not available outside of the firewall-protected internal network. The firewall will translate particular addresses and port numbers to the internal addresses for the MPS.



**Port Forwarding**

| port | dest. address | comment |
|---|---|---|
| 80 | 192.168.0.2 | HTTP -> MPS A |
| 8473 | 192.168.0.2 | Banner ->MPS A |
| 8881 | 192.168.0.2 | HTTP -> MPS B |
| 8882 | 192.168.0.2 | suExec ->MPS B |
| 8883 | 192.168.0.2 | Banner ->MPS B |

**Static Address Mapping**

| ext. address | int. address |
|---|---|
| 192.168.61.1 | 192.168.0.2 |
| 192.168.61.2 | 192.168.0.3 |

**Figure 1: Generic ELAP Deployment Model**

**Note:** The addresses in *Figure 1: Generic ELAP Deployment Model* are examples. Addresses are not restricted to particular classes/ranges. Port assignments are shown in *ELAP Firewall Port Assignments*.

The ELAP provides two user interfaces (UIs):

- Text-based UI
- Graphical UI (GUI)

Before you can use the GUI, you must use the text-based UI to initialize and configure the ELAP software. For information, see *ELAP Initialization and First Configuration* and *ELAP Software Configuration* in *Administration and LNP Feature Activation Guide*.

**Note:** By default, ELAP supports both the standard HTTP protocol and the HTTP Secure (HTTPS) protocol. For important information about enabling the HTTPS protocol and disabling HTTP, see *ELAP Support for HTTPS on GUI*.

For more information about the overall design and functions of the ELAP, see the *ELAP Functional Description* in *Administration and LNP Feature Activation Guide*.

# Chapter 3

# Implementing ELAP Security

**Topics:**

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

## ELAP Support for HTTPS on GUI

The *ELAP Support for HTTPS on GUI* feature enables the use of the HTTPS protocol, which supports encryption of data exchanged between the web server and the browser. By default, ELAP also supports the standard HTTP protocol, which should be disabled since there is no encryption. For more information, see *ELAP Support for HTTPS on GUI* in *Administration and LNP Feature Activation Guide*.

## User and Group Administration

The ELAP 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: ELAP UI Logins*.

**Table 2: ELAP UI Logins**

| Login Name | Access Granted |
|---|---|
| elapmaint | Maintenance menu and all submenus |
| elapdatabase | Database menu and all submenus |
| elapdebug | Debug menu and all submenus |
| elapplatform | Platform menu and all submenus |
| uiadmin | User Administration menu |
| elapall | All of the above menus |
| elapconfig | Configuration menu and all submenus (text-based UI) |

The **User Administration** menu is used to set up and perform administrative functions for users and groups, and also to maintain an authorized IP address list, terminate active sessions, and modify system defaults.

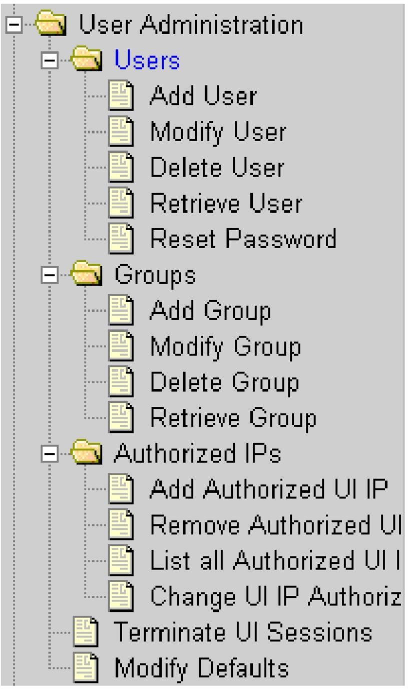


**Figure 2: User Administration Menu**

### 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. ELAP users can fall into one of the following default groups:

- maint
- database
- platform
- debug
- 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 Menu* under *User Administration Menu* in *Administration and LNP Feature Activation 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.

In addition to the group permissions that apply to a user, the administrator can set other user-specific permissions or restrictions for a specific user when adding 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 Menu* under *User Administration Menu* in *Administration and LNP Feature Activation Guide*.

## User Authentication

Users are authenticated through a unique username and password when logging in to the UI. The following rules govern passwords:

- Must be at least eight characters in length
- Must include at least one alpha character
- Must include at least one numeric character
- Must not contain three or more of the same alphanumeric character in a row
- Must not contain three or more consecutive ascending or descending alphanumeric characters in a row
- Must not contain the user account name or its reverse
- Must contain at least one of the following special punctuation characters: question mark (?), period (.), exclamation point (!), comma (,), or semi-colon(;)
- Must not use blank, null, or default passwords

The system administrator can change password-related default settings, such as maximum password age and password reuse limit. For information, see *Modifying System Defaults*.

### Changing Default Passwords

As a security measure, the passwords for the default ELAP UI users (for example, uiadmin) and operating system users (for example, root) 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 available from the ELAP GUI main menu provides all ELAP 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 elapdev 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 elapconfig uses the option provided in the ELAP Configuration Menu. Linux PAM rules are not applicable while changing the password for the elapconfig user. Only the configured minimum password length applies.

### Resetting a User Password

The **User Administration** > **Users** > **Reset Password** screen enables the system administrator to select a username and change the associated password.

## Modifying System Defaults

The **User Administration** > **Modify Defaults** screen enables the administrator to manage system defaults. Following are examples of the system defaults that you can modify from this screen:

- Maximum failed user login attempts before disabling a user account
- Maximum number of days that a user account can be inactive until it is automatically disabled
- Maximum number of days before a user password must be changed
- Number of unique passwords required before a previously used password can be reused

For a complete list and more information, see *Modify System Defaults* under *User Administration Menu* in *Administration and LNP Feature Activation Guide*.

## Authorized IP Addresses

ELAP security functions limit access to the ELAP GUI to specific IP addresses. The specified allowed IP addresses are kept in an ELAP list that can be added to, deleted from, and retrieved only by an authorized user. These functions also allow an authorized user to use the GUI to toggle authorized IP address checking to be on or off. The **User Administration** > **Authorized IPs** menu enables you to add, remove, and list authorized UI IP addresses, and to change the UI IP address authorization status.

For more information, see *ELAP Security Functions* and *Authorized IP Address Menu* under *User Administration Menu* in *Administration and LNP Feature Activation Guide*.

## Secure File Transfer Protocol

The ELAP supports secure File Transfer Protocol (FTPS) sessions with external servers for transfer of various files from the ELAP. The authentication process requires a self-signed digital certificate (user name & password only) for authenticating the sessions. The transfer of files is driven from the external server.

# Appendix A

# Secure Deployment Checklist

**Topics:**

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

- Change default passwords
- Configure ELAP firewall port assignments
- Enable HTTPS and disable HTTP
- Enforce strong password management
- Restrict admin functions to the required administrator groups
- Utilize the Authorized IP addresses feature

## ELAP Firewall Port Assignments

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

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

**Table 3: Firewall Requirements**

| Server Interface | IP Address | TCP/IP Port | Inbound | Outbound | Use/Comments |
|---|---|---|---|---|---|
| **ELAP Application Firewall Requirements:** | | | | | |
| Port 1 | Provisioning IP or VIP configured on ELAP | 22 | Yes | Yes | SSH/SCP/SFTP |
| Port 1 | NTP server IP(s) configured on ELAP | 123 | Yes | Yes | NTP - Needed for time-sync. |
| Port 1 | Provisioning IP or VIP configured on ELAP | 80 | Yes | No | APACHE - Needed for ELAP Web-based GUI. |
| Port 1 | Provisioning IP or VIP configured on ELAP | 8473 | Yes | Yes | GUI server (process) - Needed by ELAP Web-based GUI. |
| Port 1 | Provisioning IP or VIP configured on ELAP | 9691 | Yes | Yes | Used for HSOPD watcher. |
| Port 1 | Provisioning IP or VIP configured on ELAP | 1030 | Yes | Yes | Used for bulkdownload between LSMS and ELAP. |
| Port 1 | Provisioning IP or VIP configured on ELAP | 7483 | Yes | No | Used for download the normal provisioning data from LSMS to ELAP. |

# 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 ELAP 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 ELAP UI login name (such as uiadmin) and changes the password to a new unique password. For a list of the pre-defined ELAP UI login names, see *Table 2: ELAP UI Logins*.
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 ELAP 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 ELAP 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 ELAP UI login accounts using the new customer passwords to verify success with the new customer passwords.

# Glossary

## E

ELAP

EAGLE Local Number Portability Application Processor

The EAGLE LNP Application Processor (ELAP) platform provides capacity and performance required to support the ported number database.

## L

LNP

Local Number Portability

The ability of subscribers to switch local or wireless carriers and still retain the same phone number.

## M

MPS

Multi-Purpose Server

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

Messages Per Second

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

## N

NAT

Network Address Translation

## S

SSL

Secure Socket Layer (SSL) is an industry standard protocol for

| | |
|---|---|
| | **S** |
| | clients needing to establish secure (TCP-based) SSL-enabled network connections |
| | **U** |
| UI | User Interface |