

**Oracle® Communications
EAGLE**

Security Guide

Release 46.4

E79813 Revision 1

December 2016

Oracle Communications EAGLE Security Guide, Release 46.4

Copyright © 1993, 2016, Oracle and/or its affiliates. All rights reserved.

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 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 installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. 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 and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon 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, Opteron, the AMD logo, and the AMD Opteron 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.

Table of Contents

Chapter 1: Introduction.....	5
Overview.....	6
Scope and Audience.....	6
Documentation Admonishments.....	6
Manual Organization.....	7
My Oracle Support (MOS).....	7
Emergency Response.....	7
Related Specifications.....	8
Customer Training.....	8
Locate Product Documentation on the Oracle Help Center Site.....	8
Chapter 2: EAGLE Security Overview.....	10
Basic Security Considerations.....	11
Overview of EAGLE Security.....	11
Chapter 3: Performing a Secure EAGLE Installation.....	13
Pre-Installation Configuration.....	14
Installing EAGLE Securely.....	14
Post-Installation Configuration.....	14
Chapter 4: Implementing EAGLE Security.....	15
Managing User IDs and Passwords.....	16
EAGLE OA&M IP Security Enhancements.....	16
Network Security Enhancements.....	16
SS7 Firewall.....	17
Appendix A: Secure Turnover to Customer.....	18
Secure Turnover Process.....	19
Glossary.....	20

List of Tables

Table 1: Admonishments.....6

Chapter 1

Introduction

Topics:

- *Overview.....6*
- *Scope and Audience.....6*
- *Documentation Admonishments.....6*
- *Manual Organization.....7*
- *My Oracle Support (MOS).....7*
- *Emergency Response.....7*
- *Related Specifications.....8*
- *Customer Training.....8*
- *Locate Product Documentation on the Oracle Help Center Site.....8*

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 (EAGLE) 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 <i>personal injury</i> .)
 WARNING	Warning: (This icon and text indicate the possibility of <i>equipment damage</i> .)
 CAUTION	Caution: (This icon and text indicate the possibility of <i>service interruption</i> .)
 TOPPLE	Topple: (This icon and text indicate the possibility of <i>personal injury and equipment damage</i> .)

Manual Organization

This manual contains the following chapters/appendixes:

- *Introduction* contains general information such as an overview of the manual, how to get technical assistance, and where to find more information.
- *EAGLE Security Overview* describes basic security considerations and provides an overview of EAGLE security.
- *Performing a Secure EAGLE Installation* describes the process to ensure a secure installation of EAGLE.
- *Implementing EAGLE Security* explains EAGLE security features.
- *Secure Turnover to Customer* describes the secure password turnover process used to ensure security of systems delivered to our customers.

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 Specifications

For information about additional publications that are related to this document, refer to the Oracle Help Center site. See *Locate Product Documentation on the Oracle Help Center Site* for more information on related product publications.

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 Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) 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 <http://www.adobe.com>.

1. Access the Oracle Help Center site at <http://docs.oracle.com>.
2. Click **Industries**.
3. Under the Oracle Communications subheading, click the **Oracle Communications documentation** link.

The Communications Documentation page appears. Most products covered by these documentation sets will appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."

4. Click on your Product and then the Release Number.
A list of the entire documentation set for the selected product and release appears.

5. To download a file to your location, right-click the **PDF** link, select **Save target as** (or similar command based on your browser), and save to a local folder.

Chapter 2

EAGLE Security Overview

Topics:

- *Basic Security Considerations.....11*
- *Overview of EAGLE Security.....11*

This chapter describes basic security considerations and provides an overview of EAGLE 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.
- **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 the security log.
- **Install software securely.** For example, use firewalls, secure protocols using TLS (SSL), and strong passwords. See [Performing a Secure EAGLE Installation](#) for more information.
- **Learn about and use the EAGLE security features.** See [Implementing EAGLE 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>

When planning your EAGLE implementation, consider the following questions:

- Which resources need to be protected?
 - You need to protect customer data, such as routing data and network traffic.
 - You need to protect internal data, such as proprietary source code.
 - You need to protect system components from being disabled by external attacks or intentional system overloads.

- Who are you protecting data from?

For example, you need to protect your subscribers' data from other subscribers, but someone in your organization might need to access that data to manage it. You can analyze your work flows to determine who needs access to the data; for example, it is possible that a system administrator can manage your system components without needing to access the system data.

- What happens if protections on strategic resources fail?

In some cases, a fault in your security scheme is nothing more than an inconvenience. In other cases, a fault might cause great damage to you or your customers. Understanding the security ramifications of each resource will help you protect it properly.

Overview of EAGLE Security

EAGLE is a secure and reliable signaling platform that provides SS7-focused signal transfer point (STP) and signaling gateway (SG) services that help manage intelligent routing, screening services, number portability (NP), equipment identity register, and integrated performance/service management.

Secure Database Access Credentials

Only authorized personnel are allowed to access the database/admin commands, and a user ID and password are required. Provide minimum database access privileges to the operators so that unauthorized modifications can be avoided. For more information, see [Managing User IDs and Passwords](#).

Use SSH/SSL Connections

SSH/SSL is a robust, commercial-grade, and full-featured toolkit that implements the security and network encryption. SSH/SSL provides secure data transmission through encryption keys.

Encryption is strongly recommended for any remote connection to the EAGLE STP, and is available with the IPS application on an IPSM card. For more information, see [EAGLE OA&M IP Security Enhancements](#).

Use Message Verification

EAGLE's network security provides message verification options that can be turned on and off independently. Using these options enhances security by discarding messages that should not be received by the EAGLE. For more information, see [Network Security Enhancements](#).

Use the SS7 Firewall Feature

The SS7 Firewall feature provides an additional set of capabilities to monitor, throttle, and validate messages. For more information, see [SS7 Firewall](#).

Do Not Use Default Community Strings for SNMP Agent Implementation

SNMP is an industry-wide standard protocol used for network management. SNMP agents interact with Network Management Systems (NMSs) that are used to monitor and control the network. Community Names are used to validate commands sent from an NMS and traps sent to an NMS. You should not use the well-known default community strings, and instead consider using unique community strings (for example, for requests and traps). Unique community strings lessen the impact if a community string is compromised.

Chapter 3

Performing a Secure EAGLE Installation

Topics:

- [Pre-Installation Configuration.....14](#)
- [Installing EAGLE Securely.....14](#)
- [Post-Installation Configuration.....14](#)

This chapter describes the process to ensure a secure installation of EAGLE.

For information about installing EAGLE, see the *EAGLE Installation Guide*.

Pre-Installation Configuration

No pre-installation configuration regarding security is required.

Installing EAGLE Securely

System servers are securely installed by Oracle personnel with Oracle internal default passwords.

Post-Installation Configuration

The Oracle installer logs into each EAGLE OAM and changes the password to a unique and secure password, after which the customer logs in and sets their own authorized password. For details about the secure password change process, see [Secure Turnover to Customer](#).

For information about enabling user access to the database/admin commands, see [Managing User IDs and Passwords](#).

If OAM security features are not enabled by default during the installation process, see [EAGLE OA&M IP Security Enhancements](#).

For information about monitoring, throttling, and validating messages, see [SS7 Firewall](#).

Chapter 4

Implementing EAGLE Security

Topics:

- *Managing User IDs and Passwords.....16*
- *EAGLE OA&M IP Security Enhancements.....16*
- *Network Security Enhancements.....16*
- *SS7 Firewall.....17*

This chapter explains the EAGLE security features.

Managing User IDs and Passwords

The system administrator assigns user IDs and passwords. For information, see *Adding a User to the System* in *Database Administration - System Management User's Guide*.

Assign user IDs/passwords and privileges to each user only as needed.

Review the security defaults and modify them as appropriate for your installation. Develop a password scheme that results in strong user passwords, set password expiration limits, and disable inactive user IDs. For more information, see *Changing the Security Defaults* in *Database Administration - System Management User's Guide*.

If the non-configurable command classes are too broad, see *Configuring Command Classes* in *Database Administration - System Management User's Guide*.

These topics and others are all covered under *System Administration Procedures* in *Database Administration - System Management User's Guide*.

For further information about user ID and password administration rules, command classes, login security checks, and intrusion alert, see *System Security* in *Commands User's Guide*. The Command Class Management feature is described in *Previously Released Features*.

EAGLE OA&M IP Security Enhancements

The EAGLE OA&M IP Security Enhancements feature enables secure data transmission by using the Secure Shell (SSH) protocol to provide for secure remote login and other secure network services. After the EAGLE OA&M IP Security Enhancements feature is turned on, the EAGLE allows only secure connections from approved clients, and protects sensitive passwords and information while in transit between the EAGLE and a host.

If you need to activate this feature, see *Activating the Eagle OA&M IP Security Enhancement Controlled Feature* in *Database Administration - System Management User's Guide*. The EAGLE OA&M IP Security Enhancements feature is described in *Previously Released Features*.

Network Security Enhancements

The Network Security Enhancements feature enhances the EAGLE's network security by discarding messages that should not be received by the EAGLE. This feature is controlled by a centralized feature key and has STP command options to control activation of Enhanced MTP Security, Enhanced MTP Management Protection, and Enhanced SCCP Management Protection. For more information about the Network Security Enhancements feature, see *Previously Released Features*.

SS7 Firewall

The SS7 Firewall feature provides the following additional security options:

- Logging capability on the SCCP card

The logging engine logs events from an SCCP card, primarily containing the MTP, SCCP, TCAP, and MAP portions of a message. The SCCP card transfers all log events for the MSUs that trigger the SFLOG GTT action. Two IPS cards act as the primary and secondary logging cards.

- Egress throttling

For each SFTHROT GTT action, a threshold can be provisioned to limit the number of MSUs triggering the GTT action in a 30 second period, throttling such messages if the number of messages crosses the provisioned threshold.

- Map-Based Routing

Map-based routing provides enhancements to the existing FLOBR/TOBR/GTT Actions framework to allow additional MAP components to be used in the selection process.

- MAP SCCP validation

In certain MAP operations, some MAP parameters are expected to be the same as either the SCCP CdPA or CgPA. With SS7 Firewall, GTT Action SCPVAL will be used for this validation. This validation will be done only on MO-FSM and MT-FSM messages coming to the EAGLE.

For more information on the SS7 Firewall feature, see *Database Administration - GTT User's Guide*.

Appendix

A

Secure Turnover to Customer

Topics:

- [Secure Turnover Process.....19](#)

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 USB or tar file deliverables and installation procedures. The default user login *eagle* password used by manufacturing and operations is known only to Oracle. This user and default password may and should be removed.
2. Following installation, the Oracle installer performs a login to each EAGLE OAM as *eagle* and changes the password to a new unique secure password.
3. The authorized customer agent is instructed to log in to each EAGLE and change the password for accounts *eagle* to the authorized operational setting for the customer.
4. If the customer has the IPUI feature, the customer agent is instructed to access the IP terminals, log in to each relevant application, and change the default administrative account password to the authorized customer operational password.
5. 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.
6. The customer agent again logs in to each account using the new customer passwords to verify success with the new customer passwords.

N

NMS

Network Management System

An NMS is typically a standalone device, such as a workstation, that serves as an interface through which a human network manager can monitor and control the network. The NMS usually has a set of management applications (for example, data analysis and fault recovery applications).

NP

Number Plan

Numbering Plan

Number Portability

A capability that permits telecommunications users to maintain the same telephone access number as they change telecommunication suppliers.

O

OAM

Operations, Administration, and Maintenance. These functions are generally managed by individual applications and not managed by a platform management application, such as PM&C.

Operations – Monitoring the environment, detecting and determining faults, and alerting administrators.

Administration – Typically involves collecting performance statistics, accounting data for the purpose of billing, capacity planning, using usage data, and maintaining system reliability.

O

Maintenance – Provides such functions as upgrades, fixes, new feature enablement, backup and restore tasks, and monitoring media health (for example, diagnostics).

S

SG

Secure Gateway

Signaling Gateway

A network element that receives/sends SCN native signaling at the edge of the IP network. The SG function may relay, translate or terminate SS7 signaling in an SS7-Internet Gateway. The SG function may also be coresident with the MG function to process SCN signaling associated with line or trunk terminations controlled by the MG (for example, signaling backhaul). A Signaling Gateway could be modeled as one or more Signaling Gateway Processes, which are located at the border of the SS7 and IP networks. Where an SG contains more than one SGP, the SG is a logical entity and the contained SGPs are assumed to be coordinated into a single management view to the SS7 network and to the supported Application Servers.

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

S

(MIB). The SNMP protocol arranges managed objects into groups.

SS7

Signaling System #7

A communications protocol that allows signaling points in a network to send messages to each other so that voice and data connections can be set up between these signaling points. These messages are sent over its own network and not over the revenue producing voice and data paths. The EAGLE is an STP, which is a device that routes these messages through the network.

SSH

Secure Shell

A protocol for secure remote login and other network services over an insecure network. SSH encrypts and authenticates all EAGLE IPUI and MCP traffic, incoming and outgoing (including passwords) to effectively eliminate eavesdropping, connection hijacking, and other network-level attacks.

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

S

the Service Control Point (SCP)
over the network.

Spanning Tree Protocol

T

TLS

Transport Layer Security

A cryptographic protocol that provides security for communications over networks such as the Internet. TLS encrypts the segments of network connections at the transport layer end-to-end. TLS is an IETF standards track protocol.