

**Oracle® Communications  
EAGLE Query Server**

Security Guide

Release 1.0

**E83906 Revision 1**

February 2017

Oracle Communications EAGLE Query Server Security Guide, Release 1.0

Copyright © 2017, 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

<b>Chapter 1: Introduction.....</b>	<b>6</b>
Overview.....	7
Scope and Audience.....	7
Documentation Admonishments.....	7
Manual Organization.....	7
My Oracle Support (MOS).....	8
Emergency Response.....	8
Related Specifications.....	9
Customer Training.....	9
Locate Product Documentation on the Oracle Help Center Site.....	9
<b>Chapter 2: EAGLE Query Server Security Overview.....</b>	<b>10</b>
Basic Security Considerations.....	11
Overview of EAGLE Query Server Security.....	12
<b>Chapter 3: Performing a Secure EAGLE Query Server</b>	
<b>Installation.....</b>	<b>14</b>
Pre-Installation Configuration.....	15
Installing EAGLE Query Server Securely.....	15
Post-Installation Configuration.....	15
<b>Chapter 4: Implementing EAGLE Query Server Security.....</b>	<b>16</b>
Managing User Accounts.....	17
<b>Chapter 5: Security Considerations for Developers.....</b>	<b>18</b>
<b>Glossary.....</b>	<b>19</b>

# List of Figures

Figure 1: EAGLE Query Server Architecture.....12

# List of Tables

Table 1: Admonishments.....7

# Chapter 1

## Introduction

---

### Topics:

- [Overview.....7](#)
- [Scope and Audience.....7](#)
- [Documentation Admonishments.....7](#)
- [Manual Organization.....7](#)
- [My Oracle Support \(MOS\).....8](#)
- [Emergency Response.....8](#)
- [Related Specifications.....9](#)
- [Customer Training.....9](#)
- [Locate Product Documentation on the Oracle Help Center Site.....9](#)

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 manual describes how to ensure a secure installation of Oracle Communications EAGLE Query Server (EAGLE QS), and explains EAGLE QS security features.





## Scope and Audience

This manual is intended for system administrators that are installing and configuring an EAGLE QS.

## 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:

- [Introduction](#) contains general information such as an overview of the manual, how to get technical assistance, and where to find more information.
- [EAGLE Query Server Security Overview](#) describes basic security considerations and provides an overview of EAGLE QS security.
- [Performing a Secure EAGLE Query Server Installation](#) describes the process to ensure a secure installation of EAGLE QS.
- [Implementing EAGLE Query Server Security](#) explains EAGLE QS security features.
- [Security Considerations for Developers](#) provides guidelines for developers.

## 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 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](http://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 Query Server Security Overview

---

### Topics:

- *Basic Security Considerations.....11*
- *Overview of EAGLE Query Server Security.....12*

This chapter describes basic security considerations and provides an overview of EAGLE QS 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 those components.
- **Install software securely.** For example, use firewalls, secure protocols using TLS (SSL), and secure passwords. See *Performing a Secure EAGLE Query Server Installation* for more information.
- **Learn about and use the EAGLE QS security features.** See *Overview of EAGLE Query Server Security* and *Implementing EAGLE Query Server Security* for more information.
- **Use secure development practices.** For example, take advantage of existing database security functionality instead of creating your own application security. See *Security Considerations for Developers* 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 QS implementation, consider the following questions:

- Which resources need to be protected?
  - You need to protect customer data, such as telephone number (TN) information and associated data.
  - 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?

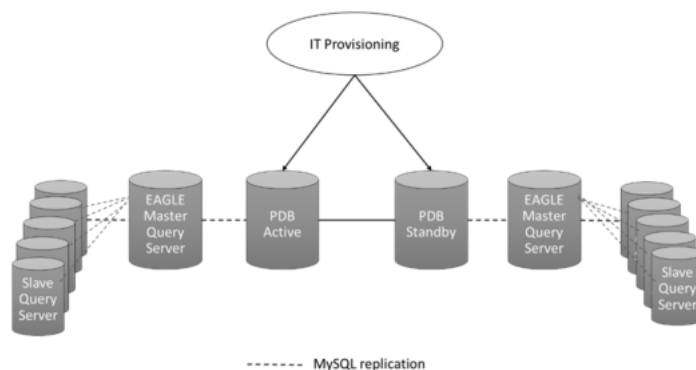
For example, you need to protect your subscribers' data from other subscribers, but someone in your organization might need to access that data to manage it. You can analyze your work flows to determine who needs access to the data; for example, it is possible that a system administrator can manage your 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 Query Server Security

The optional EAGLE QS enables offline query support into the Oracle Communications EAGLE Application Processor (EPAP) Provisioning Database (PDB). The EAGLE QS maintains a real-time copy of the EPAP PDB, enabling read access to the PDB and offloading this function from the EPAP Provisioning Database Interface (PDBI) and Provisioning Database Application (PDBA). A master EAGLE QS communicates directly with the EPAP (it can be either mixed EPAP or Standalone PDB), and a slave EAGLE QS communicates with the master EAGLE QS. IP-based connections are configured on the EPAP for establishing connection with the master QS, and replication between the master QS and slave QS is secured using an SSL connection. Each EAGLE QS supports up to 32 simultaneous connections from external applications to the QS database, excluding the Operations and Maintenance (O&M) connections. The basic EAGLE QS architecture is shown in [Figure 1: EAGLE Query Server Architecture](#).



**Figure 1: EAGLE Query Server Architecture**

### Operating System Security

The EAGLE QS was tested on the Oracle Sun Server X5-2 running version 6.8 of the 64-bit Oracle Linux operating system. Linux handles all operating system security for the EAGLE QS.

Set the Security Enhanced Linux (SELinux) mode to **Permissive** so that security logs can be created on the EAGLE QS (see [Security Logs](#)). For more information about Oracle Linux security, refer to the Oracle Linux *Security Guide for Release 6*.

### MySQL Query Client Security

The MySQL Query Client is used to query the ASCII database of the EAGLE QS. For establishing secure connections with the database, MySQL 5.7.12 or higher must be installed on the virtual machine (VM) where the EAGLE QS is to be installed.

### Secure Shell

The Secure Shell (SSH) service must be running on the EAGLE QS machine for securely connecting to EPAP(s) and the MySQL Query Client. All network elements should communicate with the EAGLE QS over secure connections to provide protection for the transported data. SSH is enabled by default for the Oracle Linux operating system. For another operating system, SSH installation might be required.

### MySQL Database Security

Only authorized personnel are allowed to access the database and a user ID and password are required. For more information, see [Managing User Accounts](#).

### Security Logs

The EAGLE QS logs all MySQL access and commands performed on the ASCII database in the `/var/QS/logs/db.cmd` log file. This log file is created on both the master and slave EAGLE QS. The logs are created by the MySQL application.

**Note:** For the log rotation to function, the SELinux mode must be set to either **Permissive** or **Disabled**; logs will not be rotated when the SELinux mode is set to **Enforcing**.

# Chapter 3

## Performing a Secure EAGLE Query Server Installation

---

### Topics:

- [Pre-Installation Configuration.....15](#)
- [Installing EAGLE Query Server Securely.....15](#)
- [Post-Installation Configuration.....15](#)

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

For step-by-step instructions to install an EAGLE Query Server, refer to EAGLE Query Server *Installation Guide*.

## Pre-Installation Configuration

Before installing the EAGLE QS, MySQL 5.7.12 or higher should be already installed on the virtual machine where the EAGLE QS is to be installed.

Before installing the EAGLE QS, create the /var/QS directory with a minimum available disk space of 500 GB.

Other security-related pre-installation configuration is set by Linux, and no additional user configuration regarding security is required. However, if another operating system is used, SSH installation might be required.

## Installing EAGLE Query Server Securely

Version 6.8 of the 64-bit Oracle Linux operating system running on an Oracle Sun Server X5-2 ensures a secure installation of the EAGLE QS application. For step-by-step instructions to install the EAGLE QS, refer to the EAGLE Query Server *Installation Guide*. The installation procedure assumes that version 6.8 of the 64-bit Oracle Linux operating system is running on an Oracle Sun Server X5-2.

## Post-Installation Configuration

There are no required post-installation configuration changes pertaining to Security.

For general information about configuring the QS, refer to EAGLE Query Server *User's Guide*.

# Chapter 4

## Implementing EAGLE Query Server Security

---

**Topics:**

- [Managing User Accounts.....17](#)

This chapter explains the EAGLE QS security features.



## Managing User Accounts

The EAGLE QS includes system users and MySQL users.

### System Users and Passwords

The following system users are required to operate the QS application and can be created using the functionality provided by the `updatePrivilegesForUser.sh` utility on the EAGLE QS:

- EAGLE QS admin user
- EAGLE QS configuration user

The system users can change their own passwords using the `passwd` command provided by the operating system. While changing a password using the `passwd` command, the Linux PAM credit rules are used. For more information, refer to the `passwd` manual page.

### MySQL Users and Passwords

The following MySQL users are available on the EAGLE QS. The length of passwords for MySQL users is 8 - 32 characters.

<b>epaprepl</b>	This user/password is created when configuring the master QS on the EPAP. The epaprepl user is used only for replication between Prov EPAP and the master EAGLE QS, and no change to the password should be required after initial configuration.
<b>epapslave</b>	This user/password is created when configuring the master QS on prov EPAP using the epapconfig menu. The epapslave user has replication privilege only, and no change to the password should be required after initial configuration.
<b>qsrepl</b>	This user/password is created when configuring the slave QS on the master QS. The qsrepl user is used for only replication of ASCII data between the master and slave query servers, and no change to the password should be required after initial configuration.
<b>root</b>	This user is the superuser used for MySQL login to any database; do not provide root access to an end user. The root user password is configured during MySQL installation/configuration and cannot be changed.
<b>dbroot</b>	This user is a restricted-privilege user with database read access only, which protects the integrity of the ASCII data. The dbroot user is used to query the ASCII database at both the master and slave EAGLE QS, and its password is set when configuring the MySQL Query Client. If the password for the dbroot user must be changed, delete the existing dbroot user and add a new dbroot user with a new password.

# Chapter 5

## Security Considerations for Developers

---

This chapter provides information for developers about how to create secure applications for EAGLE QS, and how to extend EAGLE QS without compromising security.

Consider the following guidelines:

- Use encrypted (hashed) passwords for user-accessible files.
- Delete or disable unused user accounts.
- Remove redundant code.

For more information, see *Client Programming Security Guidelines* in *MySQL 5.7 Reference Manual*.

## A

ASCII American Standard Code for Information Interchange

## E

EPAP EAGLE Application 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.

## Q

QS Query Server  
Query Service

## S

SSH Secure Shell

**S**

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

**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.

TN

Telephone Number

A 10-digit ported telephone number.

**V**

VM

Virtual Machine

Virtualized computation environment that behaves very much like a physical computer/server.

A VM has all its ingredients (processor, memory/storage, interfaces/ports) of a physical

V

computer/server and is generated by a Hypervisor, which partitions the underlying physical resources and allocates them to VMs. Virtual Machines are capable of hosting a VNF Component (VNFC).