Oracle® Communications

Local Service Management System Query Server Security Guide



Release 14.1
G63397-01
October 2026

ORACLE

Oracle Communications Local Service Management System Query Server Security Guide, Release 14.1

G63397-01

Copyright © 2003, 2026, Oracle and/or its affiliates.

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

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

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

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

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

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

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

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

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Oracle customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

Contents

1 Introduction

1.1 Overview 1
1.2 Scope and Audience 1
1.3 Documentation Admonishments 1
1.4 Manual Organization 1
1.5 Related Publications 2
1.6 Locate Product Documentation on the Oracle Help Center Site 2

2 LSMS Query Server Security Overview

2.1 Basic Security Considerations 1
2.2 Overview of LSMS Query Server Security 2

3 Performing a Secure LSMS Query Server Installation

3.1 Pre-Installation Configuration 1
3.2 Installing LSMS Query Server Securely 1
3.3 Post-Installation Configuration 1

4 Implementing LSMS Query Server Security

4.1 Managing User Accounts 1
4.2 Configurable MySQL Port 1

5 Security Considerations for Developers

Copyright © 2003, 2026, Oracle and/or its affiliates.

My Oracle Support

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

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

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

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

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

Copyright © 2003, 2026, Oracle and/or its affiliates.

What's New in This Guide

Release 14.1 - G63397-01, October 2026

There are no updates in this document in this release.

Copyright © 2003, 2026, Oracle and/or its affiliates.

1 Introduction

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

1.1 Overview

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

1.2 Scope and Audience

This manual is intended for system administrators that are installing and configuring an **LSMS** Query Server.

1.3 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 1-1 Admonishments

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

1.4 Manual Organization

This manual contains the following chapters:

Copyright © 2003, 2026, Oracle and/or its affiliates.

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

1.5 Related Publications

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.

1.6 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.

Copyright © 2003, 2026, Oracle and/or its affiliates.

2

LSMS Query Server Security Overview

This chapter describes basic security considerations and provides an overview of **LSMS** Query Server security.

2.1 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 LSMS Query Server Installation for more information.
- **Learn about and use the LSMS Query Server security features.** See Implementing LSMS 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 LSMS Query Server 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?

Copyright © 2003, 2026, Oracle and/or its affiliates.

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.

2.2 Overview of LSMS Query Server Security

The optional LSMS Query Server enables automatic access to real time Local Number Portability (**LNP**) data through a standard **API**. Customers can perform customized, high volume, automated data queries for use by internal office and support systems such as service assurance, testing, service fulfillment, and customer care.

Operating System Security

An LSMS Query Server is hosted by a dedicated Oracle SPARC server running the Oracle Linux 10/11 operating system. Linux handles all operating system security for the LSMS Query Server, and the LSMS Query Server *Installation and Upgrade Guide* assumes that servers already have SPARC Linux 10/11 installed. Make sure you always have the latest SPARC Linux software/patches installed on your machines.

Database Security

The following security considerations apply to the MySQL database:

- Secure Database Access Credentials
  Only authorized personnel are allowed to access the database and a user ID and password are required.

  Provide minimum privileges to the user so that unauthorized modifications can be avoided.

  For more information, see Managing User Accounts.
- Use **IPsec** Connections for Data Downloads
  Configure an **IPsec** connection to download data to customer servers or devices.

  IP Security (**IPsec**) secures Internet Protocol (IP) communications by encrypting and/or authenticating all IP packets. **IPsec** provides security at the network layer for connections configured for specified addresses.
- 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 an LSMS Query Server. For more information about using keys, refer to the *Configuration Guide*.

Secure Network Management

LSMS Query Server can interact with LSMS using TLS 1.2 encryption. For more information, see *LSMS Query Server on Linux Installation and Upgrade Guide*.

Copyright © 2003, 2026, Oracle and/or its affiliates.

3

Performing a Secure LSMS Query Server Installation

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

For step-by-step instructions to install an LSMS Query Server, refer to the LSMS Query Server *Installation and Upgrade Guide*.

3.1 Pre-Installation Configuration

All pre-installation configuration is set by Linux 10/11. No additional user configuration regarding security is required.

3.2 Installing LSMS Query Server Securely

The Oracle Linux 10/11 operating system running on an Oracle SPARC server ensures a secure installation of the LSMS Query Server application. For step-by-step instructions to install the LSMS Query Server, refer to the LSMS Query Server *Installation and Upgrade Guide*. The installation procedure assumes that servers already have SPARC Linux 10/11 installed. Make sure you always have the latest SPARC Linux software/patches installed on your machines.

3.3 Post-Installation Configuration

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

For general information about configuring the Query Server, refer to the *Configuration Guide*.

Copyright © 2003, 2026, Oracle and/or its affiliates.

4

Implementing LSMS Query Server Security

This chapter explains the **LSMS** Query Server security features.

4.1 Managing User Accounts

The system administrator assigns user names and passwords.

Other than the platform-installed users, the only application and therefore the only users for the LSMS Query Server are MySQL users.

The MySQL admin user should limit additional users to only those privileges required. Refer to the Oracle *MySQL Reference Manual* for further details.

4.2 Configurable MySQL Port

The master port configuration on the LSMS Query Server must match the port configured in the LSMS GUI for the corresponding, mated LSMS pair. For information about setting the master port on the Query Server, refer to the LSMS Query Server *Installation and Upgrade Guide*.

The optional Configurable MySQL Port feature enhances the security of LSMS Query Server databases by enabling the system administrator to change the MySQL port. The port can be changed in the `my.cnf` file and the same port should be set for the corresponding Query Server IP address through the LSMS GUI. The MySQL port can be configured to ports 1024-65535.

Copyright © 2003, 2026, Oracle and/or its affiliates.

5

Security Considerations for Developers

This chapter provides information for developers about how to create secure applications for LSMS Query Server, and how to extend LSMS Query Server without compromising security.

Consider the following guidelines:

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

Copyright © 2003, 2026, Oracle and/or its affiliates.