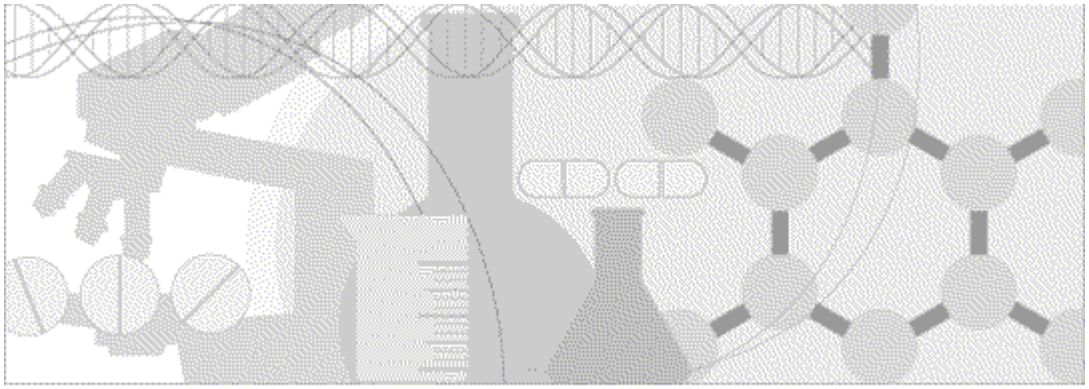
Secure Configuration Guide

Oracle® Health Sciences LabPas
Release 3.1



ORACLE

Part Number: E48667-02

Contents

About this guide

In this preface

Overview of this guide

The *Secure Configuration Guide* provides essential secure configuration considerations for the LabPas application.

Audience

This guide is for everyone who installs and configures the Oracle® Health Sciences LabPas application.

Documentation

The product documentation is available from the following locations:

- **My Oracle Support** (https://support.oracle.com)—*Release Notes* and *Known Issues*.
- **Oracle Technology Network** (http://www.oracle.com/technetwork/documentation)—The most current documentation set, excluding the *Release Notes* and *Known Issues*.

All documents may not be updated for every LabPas release. Therefore, the version numbers for the documents in a release may differ.

Item	Description	Last updated
Release Notes	The *Release Notes* document presents information about new features, enhancements, and updates for the current release.	3.1
Known Issues	The *Known Issues* document presents information about known issues for the current release.	3.1
User Guide	The *User Guide* provides online access to all tasks you can perform from the LabPas application, as well as supporting concepts and reference information. You can access the *User Guide* from the Help button in the LabPas application.	3.1
Administration Guide	This guide provides a roadmap for configuring and setting up the LabPas application, setting up the LabPas Recruiting module, and viewing and printing reports. This guide contains step-by-step instructions and field definitions you can use to perform tasks such as setting up roles and permissions; setting up various aspects of a facility, such as instruments, samples, and vessels; and configuring the LabPas user interface and messaging.	3.1
Clinical Trial Design and Resource Management Guide	This guide provides a roadmap and step-by-step instructions for a variety of tasks, such as creating clinics, creating studies, planning clinic schedules, planning staff assignments, configuring and setting up the LabPas application, designing a clinical trial and recruitment, and viewing and printing reports and labels.	3.1
Recruiting User Guide	This guide provides step-by-step instructions for setting up and managing recruitment, including adding and contacting volunteers, scheduling, managing advertising campaigns, and performing other related operations. It also includes instructions for screening volunteers in a clinical trial.	3.1
Sample Management Guide	This guide provides step-by-step instructions for processing and tracking samples in the lab.	3.1
Clinical Data Entry Guide	This guide describes how to use the LabPas application to accomplish the typical tasks you would perform while gathering data during a clinical trial. It contains step-by-step instructions and field definitions you can use to perform data entry while capturing data about doses, samples, tests, adverse events, and other observations.	3.1

Item	Description	Last updated
Data Qualification Guide	This guide provides step-by-step instructions for reviewing data that is collected in LabPas CT studies.	3.1
Installation Guide	This guide provides step-by-step instructions for installing the LabPas application.	3.1
Secure Configuration Guide	This guide provides essential secure configuration considerations for the LabPas application.	3.1
Ad Hoc Reports Database Views Guide	This document provides details of the database views used in ad hoc reports. The descriptions include the details of each view as well as corresponding fields where you can verify data.	3.1
Specification for the HL7 Lab Data Interface	This document provides the information that is needed to set up jobs and exchange files automatically between LabPas facilities and the labs that process their samples.	3.1
Specification for the Mortara E-Scribe Interface	This document provides the information needed to set up jobs and import Mortara ECG files.	3.1
Third Party Licenses and Notices	This document includes licenses and notices for third party technology that may be included in or distributed with the LabPas software.	3.1

If you need assistance

Oracle customers have access to support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info, or if you are hearing impaired, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs.

CHAPTER 1

Security overview

In this chapter

Overview

To ensure security in the LabPas application, carefully configure all system components, including the following third-party components:

- Web browsers.
- Firewalls.
- Load balancers.
- Virtual Private Networks (VPNs).

General security principles

Require complex and secure passwords

Each password should meet the following requirements:

- Contains a minimum of eight characters.
- Contains at least one upper case character, and at least one number or special character.
- Expires after 90 days.
- Does not contain a common word, name, or any part of the user name.

Keep passwords private and secure

Tell users never to share passwords, write down passwords, or store passwords in files on their computers.

Lock computers to protect data

Encourage users entering data to lock computers left unattended.

Provide only the necessary permissions to perform an operation

Assign roles to users so that they can perform only the tasks necessary for their jobs.

Protect sensitive data

- Collect the minimum amount of sensitive data needed.
- Tell users not to send sensitive information over email.
- Provide access to sensitive data only to users who need it for their jobs.

CHAPTER 2

Secure installation and configuration

In this chapter

Installation overview

This chapter outlines principles for a secure installation. For information about installing and configuring the LabPas application, see the *Installation Guide*.

Secure Sockets Layer (SSL)

Oracle recommends using a Secure Sockets Layer (SSL) connection to encrypt pages. For instructions, see the *Installation Guide*.

Tomcat HTTP-only configuration

The Tomcat HTTP-only configuration prevents JavaScript from examining the contents of the Tomcat session cookie.

You can enable the HTTP-only functionality for all web applications in conf/context.xml:

```
<Context useHttpOnly="true">
...
</Context>
```

Remove the Apache Tomcat version from HTTP error messages

By default, the Apache Tomcat version number appears in the HTTP error messages that Apache Tomcat displays. For security purposes, remove the version information so that it does not appear in these messages.

Follow these steps to remove the Tomcat version string from HTTP error messages. You must perform these steps on all application servers.

1 Stop the Apache Tomcat service.

2 Unpack the catalina.jar file.

```
cd $CATALINA_HOME/lib
jar xf catalina.jar org/apache/catalina/util/ServerInfo.properties
```

3 In the ServerInfo.properties file, replace server.info with server.info=Apache Tomcat, and then repack the catalina.jar file.

```
jar uf catalina.jar org/apache/catalina/util/ServerInfo.properties
```

4 Remove the $CATALINA_HOME/lib/org directory created when you extracted the ServerInfo.properties file.

```
rmdir /S org
```

5 Restart the Apache Tomcat service.

Change ownership of Apache Tomcat files to a least-privileged user

After installing the Apache Tomcat software, you should change ownership of the Apache Tomcat files to a least-privileged user.

1 Create a user and group to serve, with minimal permissions, as the owner of the Apache Tomcat and LabPas files.

```
groupadd <tomcat_group>
useradd -g <tomcat_group> -s /sbin/nologin -m -d <login_directory>
<tomcat_user>
```

2 Change ownership of the Apache Tomcat files to the least-privileged user that you created. The following commands are suggested.

Command	Notes
chown -R <*tomcat_user*>:<*tomcat_group*> <*home_directory*>	Change the owner and group of the <*home_directory*> to the user of least permission.
chmod -R 500 <*home_directory*>	Grant read and execute permission on the <*home_directory*>.
chmod -R 740 <*home_directory*>/logs	Grant read, write, and execute permissions on the <*home_directory*>/logs directory. If you want to give system administrators read access to log files, make them members of the <*tomcat_group*>. This allows them to view the files without having to log in as a user with super user privileges.
chmod -R 700 <*home_directory*>/work/Catalina/localhost	Grant read, write, and execute permissions on the <*home_directory*>/work/Catalina/localhost directory.

Configure strong user passwords

The LabPas application can use LDAP or Active Directory authentication. You can specify the authentication method when you install the application. LabPas does not store passwords or user information other than the user name and the user ID.

Note: Make sure that user passwords conform to Oracle standards.

Configure strong database passwords

LabPas 3.1 uses the Oracle Wallet to encrypt and store the LabPas database password. The Oracle Wallet is a container on the server where database credentials are stored securely in an encrypted form.

For more information, see the *Installation Guide*.

- Before upgrading to LabPas 3.1 from a previous 3.0.x version, you must change the database password to a known password, and then add it to an Oracle Wallet.
- For new LabPas installations, you must preconfigure a LabPas database user, add the user password to an Oracle Wallet on the server, and use it to connect to the database.

Note: Make sure that database passwords conform to Oracle standards.

Configure the sqlnet.ora file to secure database access

The sqlnet.ora file contains configuration parameters for the Oracle Net networking stack used in communications between the database server and clients. You can use the sqlnet.ora file to enforce encryption for database communication.

Update the sqlnet.ora file

The sqlnet.ora file is located at:

```
%ORACLE_HOME%\NETWORK\ADMIN\sqlnet.ora
```

Open the sqlnet.ora file with a text editor and add the following lines:

```
SQLNET.AUTHENTICATION_SERVICES = (AUTHENTICATION_SERVICE)
SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER = (CRYPTO_CHECKSUM_TYPE)
SQLNET.ENCRYPTION_SERVER = (ENCRYPTION_SERVER)
SQLNET.CRYPTO_SEED = ('CRYPTO_SEED')
SQLNET.ENCRYPTION_TYPES_SERVER = (ENCRYPTION_TYPE_SERVER)
ADR_BASE = (ADR_BASE)
SQLNET.CRYPTO_CHECKSUM_SERVER = (CRYPTO_CHECKSUM_SERVER)
```

To enforce encryption, use the following values.

Parameter	Description	Recommended value
AUTHENTICATION_SERVICE	Native OS authentication service	nts
CRYPTO_CHECKSUM_TYPE	Checksum cryptographic hash function	sha1
ENCRYPTION_SERVER	Enforces encryption for connections	required
CRYPTO_SEED	String used to generate the cryptographic key	a 10 to 70 characters long string
ENCRYPTION_TYPE_SERVER	List of encryption algorithms used by the database server	AES256
ADR_BASE	Base directory into which tracing and logging incidents are stored when ADR is enabled	• C:\app\<username> in Windows • /u01/app/<username> in Linux
CRYPTO_CHECKSUM_SERVER	Enforces checksum-based data integrity verification for connections	required

Note: You must restart the listener for the changes to take effect. To restart the listener, from the command line, run **lsnrctl stop** and then **lsnrctl start**.

Close all unused ports

Keep only the minimum number of ports open. Close all ports not in use.

Ports required for Apache Tomcat are set in $CATALINA_HOME/conf/server.xml as connectors. Use a port above 1024, because the root user owns those below 1024.

The default port for connecting to the Oracle database is 1521. If you use a different value, open the configured port on the application servers to connect to the database. The port is referenced in the $TNS_ADMIN/tnsnames.ora alias connection information. Oracle Wallet uses the configured alias to connect the application server to the database.

If you use the lab interface utility, make sure the port configured for connecting to an SFTP server is open.

Disable unused daemons

Disable all unused daemons.

The LabPas application uses the following daemons:

- **Apache Tomcat daemon**—For web pages. A least-privileged user should run this daemon.
- **LabPas daemon**—For LabPas jobs. A least-privileged user should run this daemon.

Post-installation configuration

Restrict access to LabPas files

Enforce the following restrictions:

- Allow access to $LABPAS_HOME only to least-privileged users.
- Allow access to $LABPAS_HOME/Logs only as necessary for troubleshooting purposes.
- Remove global read and write permissions on all LabPas files.
- Restrict remote access to the server.
- Disable or delete unnecessary users.
- Restrict read and write access to $LABPAS_HOME/<*lab_import base directory*>.

Revoke database privileges granted during installation

Make sure you revoke the following roles from the LabPas database user:

- REVOKE CREATE VIEW FROM <*LabPasUser*>;
- REVOKE CREATE TRIGGER FROM <*LabPasUser*>;
- REVOKE CREATE PROCEDURE FROM <*LabPasUser*>;
- REVOKE CREATE SEQUENCE FROM <*LabPasUser*>;
- REVOKE CREATE ROLE FROM <*LabPasUser*>;
- REVOKE DROP ANY ROLE FROM <*LabPasUser*>;
- REVOKE CREATE USER FROM <*LabPasUser*>;
- REVOKE GRANT ANY ROLE FROM <*LabPasUser*>;
- REVOKE SELECT ON SYS.DBA_USERS FROM <*LabPasUser*>;
- REVOKE SELECT ON SYS.DBA_ROLES FROM <*LabPasUser*>;
- REVOKE DROP USER FROM <*LabPasUser*>;
- REVOKE GRANT ANY PRIVILEGE FROM <*LabPasUser*>.

Restrict access to directories for each lab

If you exchange files with labs using the HL7 interface, make sure you provide access to only the required directories. The LabPas application can create these directories automatically, or you can create them manually.

If the lab import and export feature is set up, the LabPas application creates the following directories as needed, unless they were created manually.

- Base directory
- Directories for each lab
- Import and export directories
- Error directories

For information about the directory structure, see the *Installation Guide*.

The system administrator manages accounts for outside labs, and ensures that each lab has access to the appropriate directories and has only the necessary privileges. For example, labs need access to read from the export directory and write to the import directory.

Restrict access to directories for multiple servers

If you exchange files with labs using the HL7 interface and you use multiple servers, make sure all servers in the server farm have only the necessary access to the export and import directories.

If the directories are on the LabPas application server running the LabPas service and the server fails, when you start the LabPas service on the secondary server, the application creates a new set of directories on the secondary server. In this case, edit the sql.properties files on the remaining servers with the new directory path and properly restrict lab access to the new directories.

Edit authentication filtering parameters

For authentication filtering, edit the parameters in the $LABPAS_HOME/bin/sql.properties directory to use the following LDAP filtering strings:

```
ATTRIBUTES_USERS = uid, cn
SEARCH_STRING_USERS = (objectClass=inetorperson)
```

Authentication filtering parameters use the following Active Directory strings:

```
ATTRIBUTES_USERS = sAMAccountName,displayName
SEARCH_STRING_USERS = (&(objectClass=person)(objectCategory=user))
```

Configure LabPas user roles

Security roles define a set of permissions that allow a user to perform certain functions or access specific pages or data.

- The Administrator role is the only security role that is installed by default.
- One administrator role must be assigned to each facility.

Users are assigned to roles on the Users page. When users are assigned to a role, they acquire the permissions associated with that role. All users assigned to the same role have the same permissions.

The administrator configures rights and assigns roles to users so that the users can perform only the tasks necessary for their jobs.

Configure study access

Both internal and external users are granted access to studies on a study by study basis. You can grant a user access to all studies when appropriate.

CHAPTER 3

Security features

In this chapter

User security features

Login security

Users must enter their user names and passwords to log in.

If either a user name or a password is incorrect, an error message appears, but does not tell the user which value is incorrect. Therefore, the message confirms neither a user name nor a password, in case an unauthorized individual is attempting to log in.

Note: LabPas logs failed login attempts if you set the application logging level to INFO or a lower value in the sql.properties file.

For more information, see the *Installation Guide*.

No data loss after a session transaction

Studies are configured to require users to re-enter their user names and passwords after a defined period of inactivity. The user can log in within a period of inactivity (typically, 15 to 60 minutes) and continue working without losing data.

Automatically locked user accounts

You should configure your authentication system (LDAP or Active Directory) to allow a defined number of login attempts. When the user exceeds the number of allowed login attempts, the application locks the user account, and prevents the user from logging in.

Application security features

For more information, see the *Administration Guide*.

Permissions assigned to roles

The application comes with a single default Administrator role and a set of permissions. The list of available permissions is the same in every study.

Permissions grant access to different parts of the application and allow users to perform tasks relevant to their jobs.

The Administrator can create additional roles or change the permissions that are assigned to each role to suit the needs of an organization or individual study.

Users assigned to roles

After you review the permissions that are assigned to roles and make any necessary changes, you can assign users to roles. A user assigned to a role has the permissions that are granted to that role. All users assigned to the same role have the same permissions. Changes to a role are immediately applied to all users assigned to the role.

Users assigned to facilities

Users can only access the facilities they are assigned to. Users can have access to multiple facilities and can be assigned different user roles in each facility.

Data security features

Restricted viewing of sensitive data

You can use roles and permissions to control access to LabPas modules and to individual pages in certain modules.

External users can be added to individual studies. They access the LabPas application through the LabPas DQ module. The external authentication method is set during LabPas installation. LDAP and Active Directory authentication can be filtered in the same way as internal access, using Auth2 parameters in the sql.properties file.

Note: Assign only the appropriate external users to the appropriate study. Do not assign external users to studies to which they should not have access.