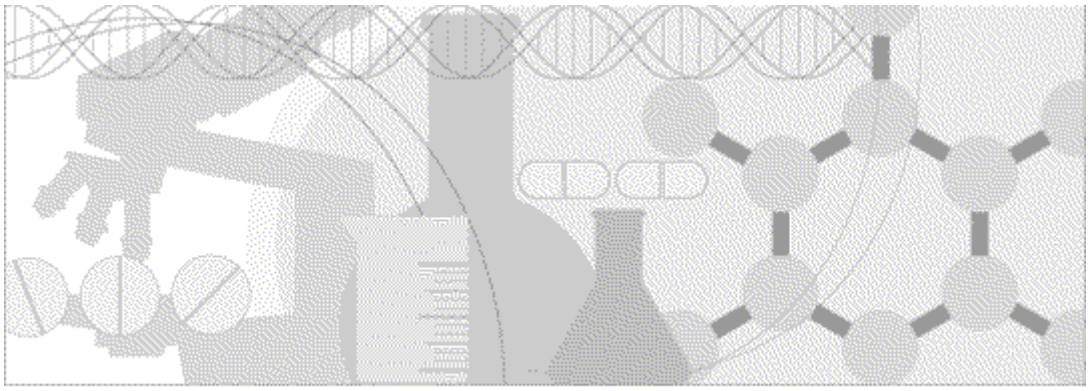
Secure Configuration Guide

Oracle® Health Sciences InForm CRF Submit Release 3.1.2



ORACLE

Part Number: E40032-01

Contents

About this guide

In this preface

Overview of this guide

The *Secure Configuration Guide* provides an overview of the security features provided with the Oracle® Health Sciences CRF Submit application, including details about the general principles of application security, and how to install, configure, and use the CRF Submit application securely.

Audience

This guide is for users who install and configure the CRF Submit application.

Related information

Documentation

All documentation is available from the Oracle Software Delivery Cloud (https://edelivery.oracle.com) and the Download Center (https://extranet.phaseforward.com).

All documents may not be updated for every CRF Submit release. Therefore, the version numbers for the documents in a release may differ. For a complete list of the documents in this CRF Submit release, their release version numbers, and part numbers, see the *Release Notes*.

Title	Description
Release Notes	The *Release Notes* document describes enhancements introduced and problems fixed in the current release, upgrade considerations, release history, and other late-breaking information.
Known Issues	The *Known Issues* document provides detailed information about the known issues in this release, along with workarounds, if available. The most current list of known issues is available on the Extranet. To sign in to the Extranet, go to https://extranet.phaseforward.com.
Installation Guide	The *Installation Guide* describes how to install the CRF Submit software and the CRF Submit Adapter server. This document is also available from the Documentation CD.
User Guide and online Help	The *User Guide* and online Help provide an overview of the CRF Submit application, step-by-step instructions for using the CRF Submit application to generate PDF files of study data, and a detailed description of the user interface. This document is also available from the Documentation CD and the CRF Submit user interface.
Secure Configuration Guide	The *Secure Configuration Guide* provides an overview of the security features provided with the Oracle® Health Sciences CRF Submit application, including details about the general principles of application security, and how to install, configure, and use the CRF Submit application securely.
PDF Quick Reference	The *PDF Quick Reference* provides an overview of the PDFs generated by the CRF Submit software and instructions for viewing PDFs.

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

Application security overview

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

- Web browsers
- Firewalls
- 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.

For more information, see *Password configuration for user and application security* (on page 4).

Keep passwords private and secure

All users should change their passwords when they log in for the first time.

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

Lock computers to protect data

Encourage users to lock computers that are left unattended.

Provide only the necessary rights to perform an operation

Choose membership in the CRF Submit User Group and the CRF Submit Admin Group so that users 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.

For more information, see *Data security—Restricted viewing of sensitive data* (on page 4).

Security features

Password configuration for user and application security

Access to the CRF Submit application is controlled by the Windows login id. Passwords should follow good security guidelines, including the following.

- Password complexity—Number of the following additional requirements a password must meet. Recommended setting is 3.
  - Password must contain one or more alphabetical (A-Z, a-z) and numeric (0-9) characters.
  - Password must contain at least one non-alphanumeric character.
  - Password must contain one or more upper case [A-Z] and lower case [a-z] characters.
- Minimum length of passwords. Recommended setting is 8.
- Password reuse limit. Recommended setting is 3.
- Number of consecutive failed login attempts allowed. Recommended setting is 3.
- Number of days before the password expires. Recommended setting is 90 days.

User security—Granting access to the CRF Submit application

Access to the CRF Submit software is controlled by Windows user groups. The following groups are created during installation. You must add users to the following groups to grant them access.

- **CRF Submit User Group**—Windows user group that defines the users who can access the CRF Submit application on a user level.
- **CRF Submit Admin Group**—Views existing work order details, maintains configuration settings, and manages adapters and studies.

For more information on user administration, see the Microsoft documentation.

If you use different names for your user groups, you must update the **PhaseForward.CRFS.Enterprise.config.xml** file. For more information, see the *User Guide*.

Data security—Restricted viewing of sensitive data

You can use Windows user group membership to restrict the data that users can view.

Work orders should specify that the generated PDFs are password protected.

- Use passwords that follow the *guidelines for complexity listed in this document* (on page 4).
- For details on the options for protecting PDFs, see the *User Guide*.

CHAPTER 2

Secure installation and configuration

In this chapter

Installation overview

Use the information in this chapter to ensure the CRF Submit application is installed and configured securely. For information about installing and configuring the CRF Submit application, see the *Installation Guide*.

Use SSL to communicate with CRF Submit servers

Configure your environment so that the CRF Submit application servers are hosted behind a firewall and all communication through the firewall is over HTTPS.

Configure strong database passwords

During the CRF Submit installation, you are prompted for two database usernames and passwords, one for the CRF Submit database, the other for an existing admin database user. Ensure that these database passwords are strong passwords.

Close all unused ports

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

The CRF Submit application always uses the following ports:

- **Port 1521**—Default connection to the Oracle database.
- **Port 80**—For the client connection (HTTP).
- **Port 443**—For the client connection (HTTPS).

Disable all unused services

Disable all unused services.

The CRF Submit application uses the following services:

- COM+ System Application.
- Distributed Transaction Coordinator.
- DNS Client.
- IIS Admin Service.
- Oracle MTS Recovery Service.
- Oracle TNS Listener.
- World Wide Web Publishing Service.
- ASP.NET State Service.

Post-installation configuration

Restrict access to CRF Submit server machines

Allow only the necessary user accounts access to the CRF Submit server machine.

Limit the number of users with access to the server machine. Disable or delete any unnecessary users.

Configure strong user passwords

Configure password options to require a secure level of complexity. For example, a minimum required password length of 8 characters requires users to create more secure and complex passwords than a minimum required password length of 6 characters.

For more information, see *General security principles* (on page 3).

Configure roles and rights

Limit membership in the Windows Users Group. For more information, see *General security principles* (on page 3).

Place PDF output on a secure machine

The PDF output location is specified in the work order options. See the *User Guide* for detailed instructions.