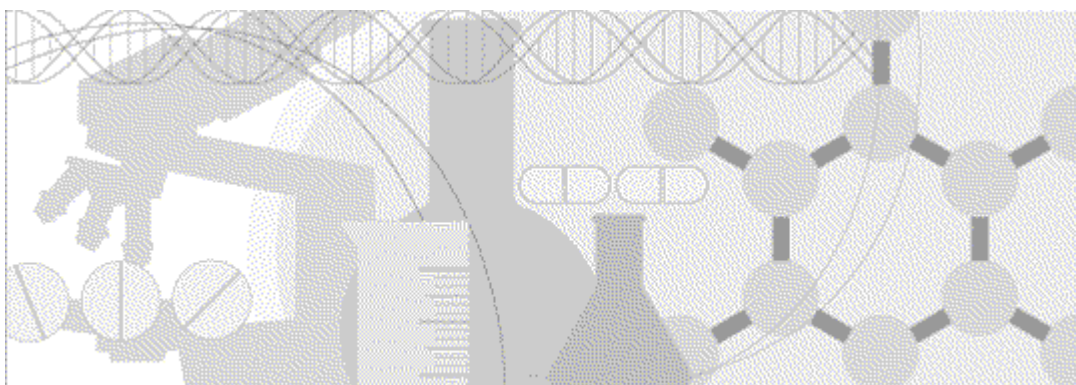


# Secure Configuration Guide

Oracle<sup>®</sup> Health Sciences InForm CRF Submit  
Release 3.1.6



ORACLE<sup>®</sup>

Part Number: E78513-01

Copyright © 2012, 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, 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.

This documentation may include references to materials, offerings, or products that were previously offered by Phase Forward Inc. Certain materials, offerings, services, or products may no longer be offered or provided. Oracle and its affiliates cannot be held responsible for any such references should they appear in the text provided.

# Contents

<b>Chapter 1 Security overview</b>	<b>1</b>
Application security overview .....	2
General security principles.....	3
Security features .....	4
Password configuration for user and application security.....	4
User security—Granting access to the CRF Submit application.....	4
Data security—Restricted viewing of sensitive data .....	4
<b>Chapter 2 Secure installation and configuration</b>	<b>5</b>
Installation overview .....	6
Use SSL to communicate with CRF Submit servers.....	6
Configure strong database passwords .....	6
Close all unused ports .....	6
Disable all unused services .....	6
Post-installation configuration .....	7
Restrict access to CRF Submit server machines.....	7
Configure strong user passwords.....	7
Configure roles and rights .....	7
Place PDF output on a secure machine.....	7
<b>About the documentation</b>	<b>9</b>
Where to find the product documentation.....	9
Documentation accessibility.....	9
Access to Oracle Support .....	9
Documentation .....	9



# CHAPTER 1

## Security overview

### In this chapter

Application security overview .....	2
General security principles .....	3
Security features .....	4

## 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 to create and work with work orders.
- **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 .....	6
Post-installation configuration.....	7

## 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.



# About the documentation

## Where to find the product 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/hsgbu-154445.html>)—The most current documentation set, excluding the *Release Notes* and *Known Issues*.

If the software is available for download, the complete documentation set is available from the Oracle Software Delivery Cloud (<https://edelivery.oracle.com>).

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

## Documentation accessibility

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>.

## Access to Oracle Support

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

## Documentation

Title	Description	Part Number	Last Updated
<i>Release Notes</i>	The <i>Release Notes</i> document describes enhancements introduced and problems fixed in the current release, upgrade considerations, release history, and other late-breaking information.	E78059-01	3.1.6
<i>Known Issues</i>	The <i>Known Issues</i> document provides detailed information about the known issues in this release, along with workarounds, if available.	E78060-01	3.1.6

Title	Description	Part Number	Last Updated
<i>Installation and Maintenance Guide</i>	The <i>Installation and Maintenance Guide</i> describes how to install the CRF Submit software and the CRF Submit Adapter server.	E78511-01	3.1.6
<i>User Guide</i> and online Help	The <i>User Guide</i> 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 CRF Submit user interface.	E78512-01	3.1.6
<i>Secure Configuration Guide</i>	The <i>Secure Configuration Guide</i> provides an overview of the security features provided with the CRF Submit application, including details about the general principles of security, and how to install, configure, and use the CRF Submit application securely.	E78513-01	3.1.6
<i>PDF Quick Reference</i>	The <i>PDF Quick Reference</i> provides an overview of the PDFs generated by the CRF Submit software and instructions for viewing PDFs.	E40031-01	3.1.2
<i>Third Party Licenses and Notices</i>	The <i>Third Party Licenses and Notices</i> document includes licenses and notices for third party technology that may be included with the InForm software.	E78514-01	3.1.6