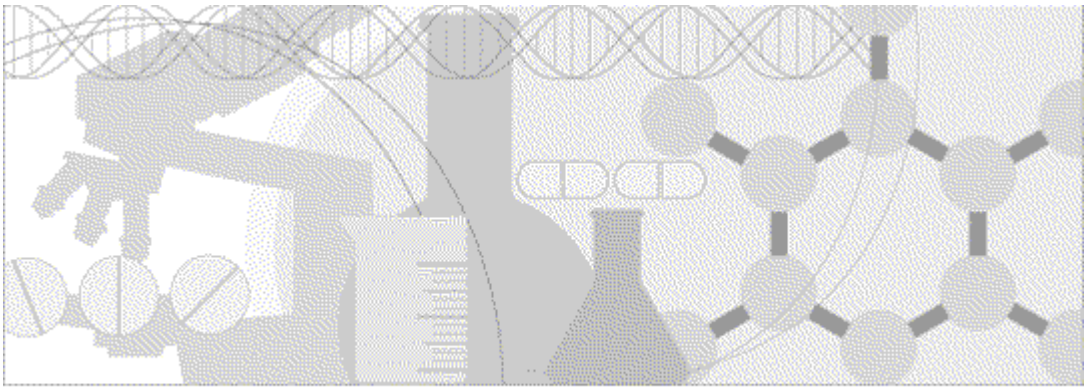
Secure Configuration Guide

InForm™ ITM 4.6 SP3a



ORACLE

Part Number: RN-INF46-002-03a

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 InForm application including details about the general principles of application security, and how to install, configure, and use the InForm application securely.

Audience

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

Related information

Documentation

All documentation is available from the Phase Forward Download Center and the Oracle Software Delivery Cloud.

InForm documentation	
Document	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. **Note:** The most current list of known issues is available on the Phase Forward Extranet. To sign in to the Extranet, go to www.phaseforward.com and click **Customer Login**. Enter your email address and password, and navigate to the **Known Issues** section. Select a product, and then enter your search criteria.
Secure Configuration Guide	The *Secure Configuration Guide* provides an overview of the security features provided with the InForm application including details about the general principles of application security, and how to install, configure, and use the InForm application securely.
Installation and Configuration Guide	The *Installation and Configuration Guide* describes how to install the software and configure the environment for the InForm application and Cognos 8 Business Intelligence application. This document is also available from the Documentation CD.
Setting Up a Trial with InForm Architect and MedML Guide	The *Setting Up a Trial with InForm Architect and MedML Guide* describes how to design and implement trials in the InForm application using the InForm Architect application. This document is also available from the Documentation CD.
Step by Step for CRCs and CRAs Guide	The *Step by Step for CRCs and CRAs Guide* describes how to use the InForm application to: • Screen and enroll patients. • Enter, update, and monitor clinical data. • Enter and respond to queries. • Run trial management reports and clinical data listings. This document is also available from the Documentation CD.

InForm documentation	
Document	Description
Reporting and Analysis Guide	The *Reporting and Analysis Guide* provides an overview of the Reporting and Analysis module. It includes a brief overview of the Reporting and Analysis interface, illustrates how to access the Ad Hoc Reporting feature, and describes the study management and clinical data packages available for Reporting and Analysis. It also provides detailed descriptions of each standard report that is included with your installation. This document is also available from the Documentation CD.
Utilities Guide	The *Utilities Guide* provides information about and step-by-step instructions for using the following utilities: • PFConsole utility • MedML Installer utility • InForm Data Import utility • InForm Data Export utility • InForm Performance Monitor utility • InForm Report Folder Maintenance utility This guide also provides reference information for the MedML elements and scripting objects that are used to import and export data to and from the InForm application, as well as sample data import XML. This document is also available from the Documentation CD.
Reporting Database Schema Guide	The *Reporting Database Schema Guide* describes the Reporting and Analysis database schema. This document is also available from the Documentation CD.
Portal Administration Guide	The *Portal Administration Guide* provides step-by-step instructions for setting up the InForm Portal software, and configuring and managing the InForm Portal application. This document is also available from the Documentation CD.
Online Help	The online Help describes how to use and administer the InForm application. This document is available only from the user interface.
InForm Architect online Help	The InForm Architect online Help describes how to design and implement trials in the InForm application using the InForm Architect application. This document is available only from the user interface.

InForm documentation	
Document	**Description**
MedML Installer utility online Help	The MedML Installer utility online Help provides information about, and step-by-step instructions for using, the MedML Installer utility, which is used to load XML that defines study components into the InForm database. This guide also provides reference information for the MedML elements and scripting objects that are used to import and export data to and from the InForm application, as well as sample data import XML. This document is also available from the user interface.
InForm Data Export utility online Help	The InForm Data Export utility online Help provides information about and step-by-step instructions for using the InForm Data Export utility, which is used to export data from the InForm application to the following output formats: • Customer-defined database (CDD). • Name value pairs. This document is also available from the user interface.
InForm Data Import utility online Help	The InForm Data Import utility online Help provides information about and step-by-step instructions for using the InForm Data Import utility, which is used to import data into the InForm application. This document is also available from the user interface.

If you need assistance

If you are an Oracle customer with a maintenance agreement, you can contact the Global Support Center for assistance with product issues.

Your maintenance agreement indicates the type of support you are eligible to receive and describes how to contact Oracle. Additionally, the Oracle website lists the toll-free support number for your product, location, and support level:

http://www.oracle.com/support

In the event that our toll-free telephone service is interrupted, please use either of the following methods to contact the Global Support Center:

- Email

  saasclinicalsupport_ww@oracle.com

- Telephone

In the US:	1-800-633-0925
Outside the US:	+44 207 13 12 801

Oracle also provides assistance with User Management, Site Assessment, and Provisioning. Please refer to your Master Services Agreement and individual Statement of Work to determine if you are eligible to use these services.

CHAPTER 1

Security overview

In this chapter

Application security overview

To ensure security in the InForm 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 8 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 *Configure strong user passwords* (on page 8).

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. For more information, see *Passwords for new users* (on page 10).

Encourage users to choose password-reset questions and answers that are easy for them to remember, but difficult for someone else to guess. For more information, see *Security questions* (on page 10).

Lock computers to protect data

Encourage users to lock computers that are left unattended. For more information, see *Login security* (on page 10).

Provide only the necessary rights to perform an operation

Assign users to user types, assign rights to rights groups, and assign users to rights groups and groups so that they can perform only the tasks necessary for their jobs.

For more information, see:

- *Users assigned to user types* (on page 12).
- *Rights assigned to rights groups* (on page 12).
- *Users assigned to rights groups* (on page 12).
- *Users assigned to groups* (on page 12).

Protect sensitive data

Set up forms to collect only the minimum amount of Protected Health Information needed for the trial. Tell users not to send sensitive information, such as Protected Health Information or passwords, over email. Provide access to Protected Health Information only to users who need it for their jobs. For more information, see *Restricted viewing of Protected Health Information* (on page 14).

CHAPTER 2

Secure installation and configuration

In this chapter

Installation overview

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

Secure Socket Layer (SSL)

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

Configure strong database passwords

When you install the InForm application, the following database administrator users are created.

- **InForm Admin**—PFDADMIN.
- **Streams Admin**—strmadmin.
- **Reporting Admin**—rptinstall.
- **PFCapAdmin**—PFCapAdmin.
- **Content Store**—Unique name set by the customer.

When you install the Cognos software for the Reporting and Analysis module, the Cognos System Admin user is created.

Ensure all your database passwords are strong passwords.

Close all unused ports

System ports and protocols in use must comply with the Global IT Firewall Security Standards. Keep only the minimum number of ports open. Close all ports not in use.

The InForm application always uses the following port:

- **Port 1521**—Default connection to the Oracle database.

The InForm application may use the following ports:

- **Port 80**—For the client connection (HTTP).
- **Port 443**—For the client connection (HTTPS).

Note: The InForm application does not require both Port 80 and Port 443. You can configure the InForm application to use only HTTP or only HTTPS.

Disable all unused services

Disable all unused services.

The InForm application uses the following services:

- InForm Service
- IBM Cognos 8
- COM+ System Application
- Distributed Transaction Coordinator
- DNS Client
- IIS Admin Service
- Oracle MTS Recovery Service
- World Wide Web Publishing Service

Post installation configuration

Restrict access to InForm server machines

Allow only administrator and system accounts access to the InForm 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 *Password configuration for user security* (on page 10).

Configure rights and rights groups

Assign users to user types, assign rights to rights groups, and assign users to rights groups and groups, so that users can perform only the tasks necessary for their jobs.

For more information, see:

- *Users assigned to user types* (on page 12).
- *Rights assigned to rights groups* (on page 12).
- *Users assigned to rights groups* (on page 12).
- *Users assigned to groups* (on page 12).

CHAPTER 3

Security features

In this chapter

User security features

Password configuration for user security

An administrator can define the following formatting, entry, and reuse requirements for passwords directly in the InForm application on the System Configuration page. For the recommended settings see, *General security principles* (on page 3).

- Minimum length of the password. Recommended setting is 8 characters.
- Whether the password must include a number. Recommended setting is Yes.
- Whether the password must include an upper-case letter. Recommended setting is Yes.
- Whether the password must include a nonalphanumeric character. Recommended setting is Yes.
- Whether the password can be reused. Recommended setting is No.
- Number of login attempts allowed. Recommended setting is 3.
- Whether password recovery is enabled. Recommended setting is Yes.
- Email address for password recovery notifications. Recommended setting is Yes.
- Number of days before the password expires. Recommended setting is 90 days.

Passwords for new users

When you create new users, the users should change their passwords the next time they log in. At the initial log in, each user can set up a question, answer, and provide an email address. A temporary password is sent to the email address provided.

Login security

Users must enter their user names and passwords to log in. The application does not allow duplicate user names.

If either a user name or password is incorrect, an error message appears, but does not tell the user the value that is incorrect. Therefore, if someone else is using the account to attempt to log in, the message does not confirm either a user name or password.

Security questions

If a user exceeds the number of allowed login attempts, resulting in a locked user account, the user can answer security a question to reset the password and unlock the account. Password questions and answers are available in the application to control access to some studies.

- At the initial login, each user can specify a security question and answer used when the user forgets the password.
- The user sets the password and provides the answer to the security question.
- To reset a password in the application, the user must provide the correct answer.

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 and continue working on a form without losing data.

This security feature is controlled by the following settings on the System Configuration page:

- **Re-authentication inactivity period**—Number of minutes of inactivity that can pass before the InForm application requires a user to log in again.
- **Re-identification period**—Number of minutes that a session can be active before the InForm application requires a user to log in again.

Select values for these settings that work with your trial protocol.

Automatically inactivated user accounts

Studies are configured to allow a defined number of attempts to log in correctly. When a user exceeds the number of allowed login attempts, which is defined on the System Configuration page, the user account is inactivated and the user cannot log in.

Only a user with the appropriate rights can activate an automatically inactivated account. Relevant rights include:

- Activate Site User.
- Deactivate Site User.
- Activate Sponsor User.
- Deactivate Sponsor User.

Restricted access to the application

You can restrict access to the application in the following ways.

- Terminate a user.

  Typically, you terminate users who leave the organization. Terminated users cannot log in. All users, including terminated users, remain in the trial for audit purposes. Terminated users can be reinstated and then activated.

- Inactivate a user.

  Typically, a user is automatically inactivated when the user fails to log in after the number of attempts set on the System Configuration page. After the user account is inactivated only an administrator can manually reactivate the user. The user must be reactivated before the user can work in the application.

Application security features

Users assigned to user types

You can assign users to user types.

The following user types are available:

- **Site User (default)**—User who performs site functions. Queries in the Candidate state are not visible to Site users. This user is not allowed to see certain information, for example Candidate queries.
- **Sponsor User**—User who performs sponsor functions such as monitoring and data management. Queries in the Candidate state are visible to sponsor users.

Note: These options do not appear for system users.

Rights assigned to rights groups

A right is the permission to perform a specific activity. A rights group is a collection of rights.

Rights grant access to different parts of the application. Entire parts of the application are hidden when users do not have the rights to work in those areas.

When a new user is created in the InForm application, an administrator with the right to modify user information assigns the user to a rights group, providing the user permissions to perform specific trial activities.

For example, a user can be assigned to a rights group with the appropriate rights to screen and enroll patients. The individual Enroll Patients right is static, but the group of rights assigned to the rights group are configurable.

A user can be a member of only one rights group.

Users assigned to rights groups

After you review the rights that are assigned to rights groups and make any necessary changes, you can assign users to rights groups. A user assigned to a rights group has the rights that are granted to that rights group. Changes to a rights group are immediately applied to all users assigned to the rights group.

Users assigned to groups

Groups allow you to associate users who have similar roles in a trial and allow them access to specific areas of InForm functionality. Groups provide an advanced level of authorization. In order to perform certain activities, a user must both have rights to perform the activities and be in a group for which the activities are authorized.

The InForm application allows you to define and maintain different types of groups. Users can sign forms, enter queries, and access the Reporting and Analysis module if they are assigned to the

corresponding groups and have the appropriate rights.

Users assigned to sites

Users can view patient and visit information only for the sites to which they are assigned. Users must also be assigned to rights groups that grant them access to this information.

Display overrides

Display overrides allow you to refine user access to individual data items on forms. For a particular rights group, you can specify whether the group of items that make up an item group is Hidden, Editable, or Read-Only. This designation overrides the rights conveyed by membership in the rights group and also overrides the display properties of the items in the group. This additional level of security allows you to give users with the same set of rights different access to specific items.

To create item definition display overrides, use the Central Designer application.

Data security features

Restricted viewing of Protected Health Information

You can use user types, rights, groups, and display overrides to restrict the users that can view Protected Health Information, which appears in patient profiles.

Access to confidential patient information is also restricted. Therefore, your trial is set up so that only specific users, such as clinical research coordinators, can enter patient data.

Audit trails for data security

Audit trails record updates to the following information:

- Patient information
- Data on forms
- Queries
- Signatures

Audit trails are comprehensive records that include the person who made the change, the date and time of the change, the change itself, as well as additional details. You cannot modify data in an audit trail.

Freezing and locking data

You can freeze or unfreeze data on the patient, visit, form, and item levels. Freezing prevents changes in data—either temporarily during a trial, or permanently at the end of a trial.

- Freezing a patient freezes all visits, forms, and items for that patient.
- Freezing a visit freezes all forms and items within the visit.

After a patient, visit, form, or item is frozen, you cannot update the data, but you can issue manual queries for items. If a repeating form is frozen, no new instances of the repeating form can be added to a visit.

Note: If an update is made to a frozen item when someone responds to a manual query, the item maintains its frozen status to prevent additional updates to the item aside from query generation.

To prevent any further modification to data, you can also lock a patient, visit, form, or item.