Oracle® Health Sciences InForm CRF Submit

Secure Configuration Guide

Release 6.3

F30577-01

Oracle Health Sciences InForm CRF Submit Secure Configuration Guide, Release 6.3

F30577-01

Contents

3 Security features

Preface

This preface contains the following sections:

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.

Related resources

All documentation and other supporting materials are available on the Oracle Help Center.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through Support Cloud.

Contact our Oracle Customer Support Services team by logging requests in one of the following locations:

- English interface of Oracle Health Sciences Customer Support Portal (https://hsgbu.custhelp.com/)
- Japanese interface of Oracle Health Sciences Customer Support Portal (https://hsgbu-jp.custhelp.com/)

You can also call our 24x7 help desk. For information, visit http://www.oracle.com/us/support/contact/health-sciences-cloud-support/index.html or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Additional copyright information

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.

1

Security overview

In this chapter

Application security overview

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

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

General security principles

In this section

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.
- Does not contain a common word, name, or any part of the user name.

For more information, see Configure strong user passwords.

Change passwords periodically

It is good practice to change both system account passwords and user passwords periodically. Follow your organization's operating procedures for the frequency of making changes.

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.

Require secure session practices

Sponsor and site users must observe the following rules:

- Run Oracle InForm in a single browser session.
- Run Oracle InForm in a single browser window.
- Log out of Oracle InForm before closing the Oracle InForm browser window.

Lock computers to protect data

Encourage users to lock computers that are left unattended.

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.
- Rights assigned to rights groups.

2
Secure installation and configuration

In this chapter

Installation overview

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

For more information, see:

Transport Layer Security (TLS)

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

Oracle recommends that you use TLS version 1.2 or higher, as versions 1.1 and below have been found to be vulnerable.

Transparent Data Encryption (TDE)

Oracle InForm CRF Submit provides protection for database data through Transparent Data Encryption (TDE). Oracle Data Guard SQL Apply can be used to provide data protection for a primary database with Transparent Data Encryption (TDE) enabled.

Use SSL to communicate with Oracle InForm CRF Submit servers

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

About entering passwords

The Oracle InForm software and installation scripts do not contain default or hard-coded passwords. You must supply passwords for predefined users, such as the Windows OS user and Oracle database users.

Installation scripts prompt for passwords on the command line or allow a file containing the passwords to be passed in as parameters.

> **Note:**
>
> If you use password parameter files, delete the files after installation.

Configure strong database passwords

During the Oracle InForm CRF Submit installation, you are prompted for two database usernames and passwords, one for the Oracle InForm 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.

During the installation, users are prompted for the server manager, business API, connector, storage, doc gen, and source data API ports. Default values are recommended but they are configurable. These ports must also be open.

Oracle InForm CRF Submit defaults to the following ports, but can be configured to use non-standard ports.

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

Oracle InForm does not require both Port 80 and Port 443. However, you must configure Oracle InForm to use either HTTP or HTTPS.

Disable all unused services

Disable all unused services.

Oracle InForm CRF Submit 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

In this section

Restrict access to Oracle InForm CRF Submit server machines

Allow only the necessary user accounts access to the Oracle InForm 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 eight characters requires users to create more secure and complex passwords than a minimum required password length of six characters.

Configure roles and rights

Using the Admin function within Oracle InForm 6.2, you can set up one or more specific rights groups in Oracle InForm for use with Oracle InForm CRF Submit. Rights groups control what data will and will not appear on the PDF output. Items hidden from sites will not be added to the PDF if a site user rights group is selected.

When you log into an earlier version of Oracle InForm and have administrative rights, you can add Oracle InForm rights groups to Oracle InForm CRF Submit, edit the rights associated with a rights group, and delete a rights group from Oracle InForm CRF Submit. Rights groups, themselves, are set up in Oracle InForm.

In addition, limit membership in the Windows Users Group. For more information, see General security principles.

Download PDF and CSV output onto a secure machine

When you download archives and history reports, you can specify the location to which to write the download. Make sure that this is a secure location.

3
Security features

In this chapter

User security features

In this section

Passwords for new users

When you create a new user, you supply a user name and password. Users must change their passwords the first time they log in.

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

Select values for these settings that work with your study 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 study 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.

To restrict access to the Oracle InForm CRF Submit Admin tool

This must be done by removing or disabling the user in the domain of the Server Manager server.

Application security features

In this section

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, such as data entry.
- **Sponsor user**—User who performs study functions, such as reviewing and verifying clinical data.

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 Oracle InForm, an administrator with the right to modify user information assigns the user to a rights group, providing the user permissions to perform specific study activities.

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

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

For more information, see *User Guide for Sponsors*.

Users assigned to sites

Users can view subject 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.

Data security features

In this section

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 subject profiles.

During the study design, access to confidential subject information can also be restricted. Therefore, study designers set up the study so that only specific users, such as clinical research coordinators, can enter subject data.

Audit trails for data security

Audit trails record updates to the following information:

- Resource strings (used in messages and emails)
- Group rights
- Security keys
- Server changes
- System configuration settings
- Sponsor settings
- Trial settings

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.

For more information, see *User Guide for Sponsors*.