Secure Configuration Guide

Oracle® Health Sciences InForm 6.0.1.2

Part Number: E96087-01

Contents

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 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* (on page 11).

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* (on page 16).

Lock computers to protect data

Encourage users to lock computers that are left unattended. For more information, see *Login security* (on page 16).

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 18).
- *Rights assigned to rights groups* (on page 18).
- *Users assigned to rights groups* (on page 19).
- *Users assigned to groups* (on page 19).

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*.

Transport Layer Security (TLS)

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

Secure cookies

If HTTPS is enabled for communication between the InForm and Cognos 10 Business Intelligence applications, for additional security, Oracle recommends that you secure Cognos cookies.

For more information, see the Cognos documentation.

Install only the InForm features needed

To enhance security, the InForm installer allows you to select the features to install.

- Minimal—Default option. This option installs:
  - InForm core software
  - Required utilities
  - Documentation

  If you plan to use the Reporting and Analysis module, do not select the Minimal option. It does not install the reporting utilities.
- Complete—Recommended option. This option installs:
  - InForm core software
  - Required utilities
  - Sample study
  - InForm Portal
  - All InForm utilities
  - Documentation

  For the Complete option, all the utilities are installed. You cannot select specific utilities to install.

- Custom—Installs the InForm core software and required utilities and the following options, if they are selected:
  - Documentation
  - Sample study
  - InForm Portal
  - InForm utilities

    For Custom installations, all the utilities are selected by default to be installed. You can choose whether to install each of the following utilities:
    - InForm Data Import
    - InForm Data Export
    - InForm Performance Monitor
    - InForm Reporting

      If you plan to use the Reporting and Analysis module, the InForm Reporting utility must be selected.

Note: If you are using the Reporting and Analysis module, you must install the Cognos software, and run the Reporting installers and the reporting utilities that are installed by the InForm application.

About entering passwords

The 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. For more information, see the *Installation Guide*.

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

Configure strong administrator passwords

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

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

When you configure the Oracle Directory Server for the Reporting and Analysis module, you create the Cognos System Admin user.

Ensure that all passwords for these users are strong passwords.

Close all unused ports

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

The InForm application 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).
- **Port 389**—For connection to the Oracle Directory Server for reporting.
- **Port 9300**—For connection to the Cognos server for reporting.

Note: The InForm application does not require both Port 80 and Port 443. However, you must configure the InForm application to use either HTTP or HTTPS.

Disable all unused services

Disable all unused services. The InForm application uses the following services:

- InForm Service.
- IBM Cognos 10 Business Intelligence.
- COM+ System Application.
- Distributed Transaction Coordinator.
- DNS Client.
- IIS Admin Service.
- Oracle MTS Recovery Service.
- World Wide Web Publishing Service.

Terminate unneeded user accounts

The InForm application creates a number of user accounts for studies.

Certain user accounts that were created in InForm releases prior to release 6.0 are not required by the InForm 6.0 application and can be terminated.

- When studies are migrated to an InForm 6.0 release, these accounts are terminated automatically.

  It is possible, though unlikely, that a study design has a dependency on an account that is not required by the InForm application. Before terminating these accounts for active studies, ensure that no dependency exists. If necessary, change the study to remove the dependency before terminating the account.

- The InForm 6.0 releases do not create non-critical accounts by default.
- Some user accounts are required by the InForm application and cannot be terminated. Do not terminate or deactivate these user accounts.

The following table summarizes how user accounts are handled in an InForm 6.0 release.

Account name	After migration	In InForm 6.0.x
UM	Terminated	Not created
UA	Terminated	Not created
InfAdmin	Terminated	Not created
InFusionAdmin	Terminated	Not created
InFormUser	Terminated	Not created
Pfreportuser	Terminated	Not created
Sysadmin	Terminated	Not created
system	Terminated	Terminated
Pfreportinguser	Not terminated	Not terminated
autoquery	Terminated	Terminated
pfarchuser	Terminated	Not created
ctcoding	Terminated	Terminated
ctvalidation	Terminated	Terminated
IVRS	Terminated	Not created

Add a nosniff header

Configure IIS to add a nosniff header to HTTP responses from InForm by running the following command from the administrator command prompt on the InForm application server:

```
"appcmd.exe set config /section:httpProtocol /+customHeaders.["name='X-
Content-Type-Options',value='nosniff'"] /commit:apphost"
```

Update the VISITBARSCRIPT.JS resource file

Contact Oracle Global Support for a script that updates the VISITBARSCRIPT.JS resource file to change the Datatype from STYLE to SCRIPT.

Some newer versions of the Microsoft Internet Explorer, Google Chrome, or Mozilla Firefox browsers, which perform MIME-type validation, can cause InForm to return the VISITBARSCRIPT.JS resource file as a style sheet (css/text) instead of as javascript. As a result, when a form is changed, clicking the Submit button does not detect the changes (a popup saying this appears), and you may not be able to successfully submit the form changes. The script fixes this issue so that you can successfully submit form changes.

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 eight characters requires users to create more secure and complex passwords than a minimum required password length of six characters.

For more information, see *Password configuration for user security* (on page 16).

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 18).
- *Rights assigned to rights groups* (on page 18).
- *Users assigned to rights groups* (on page 19).
- *Users assigned to groups* (on page 19).

Configure the pfreportinguser account

The InForm application includes a user named pfreportinguser, which is used to perform certain functions for the Reporting and Analysis module, including running pfrinit and the model updater service. If the password for this user expires, clinical data in the Reporting and Analysis module is not updated and becomes out of date.

To ensure that the data in the Reporting and Analysis module remains current, a user with administrative rights must do the following:

1 Reset the password for the pfreportinguser account before it expires.

> **Note:** The amount of time before a password expires is configured in the Password Expiration Period field on the System Configuration page in the InForm Admin user interface. The recommended setting is 90 days.

2 Run the following pfadmin command to propagate the password change to the Reporting and Analysis database:

```
PFADMIN SETSERVER PFREPORTINGUSERPW <studyname>
```

You supply the new password in a parameter file or in response to a command line prompt.

For more information, see the *Installation Guide*.

Change the pfuser password as required

Change the pfuser password as required by your operating procedures. To change the password:

1 *Run pfadmin* (on page 12).

2 *Update IIS with the new pfuser password* (on page 13).

3 *Update COM+ applications with the new password* (on page 13).

Run pfadmin

The following pfadmin command resets the pfuser account password in the InForm registry and the Windows account:

```
PFADMIN CONFIG SERVICE /PFUSER
```

You supply the new password in a parameter file or in response to a command line prompt.

> **Note:** You must use the same password when you update IIS. For more information, see ***Update IIS with the new pfuser password*** (on page 13).

Update IIS with the new pfuser password

When you change the pfuser password, you must manually update the value in IIS.

1 Select **Start** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.

2 Expand the tree until you see the children of Default Web Site.

3 Select a study listed under Default Web Site.

4 Double-click **Authentication** in the center panel, select **Anonymous Authentication**, and then click **Edit** in the Actions panel on the right.

5 Copy the user name in the **Specific user** field, and then click **Set**.

The Set Credentials dialog box appears.

6 Paste the user name you copied into the User name field, and enter the new password in the password fields.

> **Note:** The new password should be the same as the password that was entered when pfadmin config service/pfuser was run. For more information, see ***Run pfadmin*** (on page 12).

7 Expand the study tree of the study that you selected in step 3.

8 For each child node listed under the study, repeat steps 4 to 6 to update the password.

9 Repeat steps 3 to 8 for:

- Each study listed under Default Web Site.
- The Schema virtual directory listed under Default Web Site.
- The System virtual directory listed under Default Web Site.

Update COM+ applications with the new password

When you change the pfuser password, you must manually update the value in all the COM+ applications for the study.

1 Select **Start > Administrative Tools > Component Services**.

2 Expand **Component Services > Computers > My Computer**.

3 Select **COM+ Applications**.

4 In the middle panel, right-click any COM+ application, and then select **View > Details**.

The middle panel changes to a detailed display.

5 Right-click **InFormDisp**, and select **Properties**.

6 Select the **Identity** tab.

7 Enter the new password in the password fields.

8 Click **Apply**, and then click **OK**.

9 Repeat steps 5 to 8 for each COM+ application that has a listed account of PfUSR_<machine name>.

Change the PFCapAdmin password as required

Change the PFCapAdmin password as required by your operating procedures. You change the password by updating the MotioCAP_informcap.properties file. For more information, see the *Installation Guide*.

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) and the *User Guide*.

- 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 consecutive failed login attempts allowed. Recommended setting is 3.
- Whether password recovery is enabled. Recommended setting is Yes.
- Number of days before the password expires. Recommended setting is 90 days.

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.

Login security

InForm requires users to authenticate by logging in with a unique user name and password. You can use the following authentication methods:

- **Local**—User information stored in the InForm application is used for authentication.
- **Single Sign-On (SSO)**—For studies hosted by Oracle, user information stored in Oracle® Health Sciences Identity and Access Management Services (IAMS) is used for authentication.

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 which value 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.

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 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.

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, 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 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 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 the *User Guide*.

Users assigned to rights groups

The following pre-defined rights groups are provided with the InForm software. The rights groups contain the default set of rights that are normally associated with that rights group, but they do not contain any users.

- AutoQuery RG
- PFReportUser
- User Manager
- User Activator
- InForm Server Group
- PFArchUser
- SysAdmin
- Admin
- Principal Investigator
- CRC
- CRA
- CDM
- Project Manager

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 study and to 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 have rights to perform the activities and also 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. For more information, see the *User Guide*.

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.

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.

For more information, see the *User Guide*.

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

Changed Cognos user groups

The rights for the following Cognos user groups have been changed to limit the ability of users to create user-defined HTML and user-defined SQL:

- Directory Administrators group:
  - Can view Groups and Roles, but cannot view the Capabilities.

    The ability to make any changes to Cognos Capabilities and Cognos Groups and Roles have been removed from this group.
  - Can accept only InForm Support user types.

    Sponsor or Site users can no longer be added to this group.
- Server Administrators group:
  - Can accept only InForm Support user types.

    Sponsor or Site users can no longer be added to this group.
- Authors group:
  - In Report Studio—Authors can create, edit, or run reports that use clinical or operational model packages.

    Authors cannot create, edit, or run reports that contain custom HTML and/or custom SQL.
  - In Cognos Connection—Authors can run reports that use clinical or operational model packages.

    Authors cannot run reports that contain custom HTML and/or custom SQL.

For more information, see the *Installation Guide*.

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 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:

- Subject 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.

For more information, see the *User Guide*.

Freezing and locking data

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

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

After a subject, 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 subject, visit, form, or item.

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 Help Center (https://docs.oracle.com/cd/E86240_01/index.htm)—The most current documentation set.

Documentation accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website (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 or Support Cloud. For information, visit or visit *http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info* if you are hearing impaired.