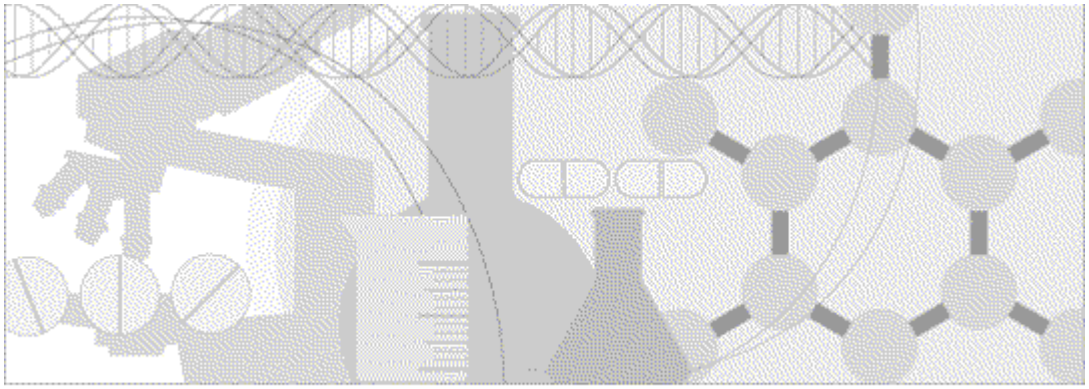
Secure Configuration Guide

Oracle® Health Sciences Central Designer Release 2.1.2



ORACLE

Part Number: E72238-01

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

Audience

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

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 Central Designer release. Therefore, the version numbers for the documents in a release may differ.

Item	Description
Release Notes	The *Release Notes* document provides detailed information about the requirements, enhancements, and fixed issues in the current release.
Known Issues	The *Known Issues* document provides detailed information about the known issues in this release, along with workarounds, if available.
Installation Guide	The *Installation Guide* provides system requirements and instructions for installing and upgrading the Oracle® Health Sciences Central Designer software and the Oracle® Health Sciences Central Designer Administrator software.
Administrator Guide	The *Administrator Guide* describes how to use the Oracle® Health Sciences Central Designer Administrator software to set up users, permissions, system configuration parameters, and catalog defaults.
User Guide	The *User Guide* introduces the study design environment in the Oracle® Health Sciences Central Designer application and describes how to work as a study design team in that environment, including how to: • Work collaboratively. • Maximize study design efficiency by reusing study objects. • Manage collections of study objects.
InForm Design Guide	The *InForm Design Guide* describes how to design a study for deployment to the InForm application.
Rules Reference Guide	The *Rules Reference Guide* is a reference to the tools that are available for creating rule expressions, including: • Study object properties. • Functions. • Constants. • Data mappings. • Methods, operators, and literals.

Item	Description
Secure Configuration Guide	The *Secure Configuration Guide* provides an overview of the security features provided with the Oracle® Health Sciences Central Designer application, including details about the general principles of application security, and how to install, configure, and use the Central Designer application securely.
Third Party Licenses and Notices	The *Third Party Licenses and Notices* document includes licenses and notices for third party technology that may be included with the Central Designer software.
Secure Development Guide	The *Secure Development Guide* provides an overview of common security risks for developers using Application Programming Interfaces (APIs) with the Oracle® Health Sciences Central Designer application, and information on how to address those risks.

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.

If you need assistance

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.

Finding Central Designer information and patches on My Oracle Support

The latest information about the Central Designer application is on the Oracle Support self-service website, My Oracle Support. Before you install and use the Central Designer application, check My Oracle Support for the latest information, including *Release Notes* and *Known Issues*, alerts, white papers, bulletins, and patches.

Creating a My Oracle Support account

You must register at My Oracle Support to obtain a user name and password before you can enter the site.

1 Open a browser to https://support.oracle.com.

2 Click the **Register** link.

3 Follow the instructions on the registration page.

Finding information and articles

1 Sign in to My Oracle Support at https://support.oracle.com.

2 If you know the ID number of the article you need, enter the number in the text box at the top right of any page, and then click the magnifying glass icon or press **Enter**.

3 To search the knowledge base, click the **Knowledge** tab, and then use the options on the page to search by:

- Product name or family.
- Keywords or exact terms.

Finding patches

You can search for patches by patch ID or number, product, or family.

1 Sign in to My Oracle Support at https://support.oracle.com.

2 Click the **Patches & Updates** tab.

3 Enter your search criteria and click **Search**.

4 Click the patch ID number.

The system displays details about the patch. You can view the Read Me file before downloading the patch.

5 Click **Download**, and then follow the instructions on the screen to download, save, and install the patch files.

Finding Oracle documentation

The Oracle website contains links to Oracle user and reference documentation. You can view or download a single document or an entire product library.

Finding Oracle Health Sciences documentation

For Oracle Health Sciences applications, go to the Oracle Health Sciences Documentation page at http://www.oracle.com/technetwork/documentation/hsgbu-clinical-407519.html.

Note: Always check the Oracle Health Sciences Documentation page to ensure you have the most up-to-date documentation.

Finding other Oracle documentation

1 Do one of the following:

- Go to http://www.oracle.com/technology/documentation/index.html.
- Go to http://www.oracle.com, point to the **Support** tab, and then click **Product Documentation**.

2 Scroll to the product you need, and click the link.

Finding prerequisite software for Oracle Health Sciences applications

Prerequisite software for Oracle Health Sciences applications is available from the following locations:

- Download the latest major or minor release from the Oracle Software Delivery Cloud (https://edelivery.oracle.com/).

  For information on the credentials that are required for authorized downloads, click **FAQ** on the main page of the Oracle Software Delivery Cloud portal.

- Download subsequent patch sets and patches from My Oracle Support (https://support.oracle.com).

  To find patch sets or patches, select the **Patches & Updates** tab.

If a previous version of prerequisite software is no longer available on the Oracle Software Delivery Cloud, log a software media request Service Request (SR). Previous versions of prerequisite software are archived and can usually be downloaded. After you open an SR, you can check its status:

- US customers: Call 1-800-223-1711.
- Outside the US: Check www.oracle.com/us/support/contact/index.html for your local Oracle Support phone number.

For more information on logging a media request SR, go to My Oracle Support for Document 1071023.1: Requesting Physical Shipment or Download URL for Software Media (https://support.oracle.com/epmos/faces/DocumentDisplay?id=1071023.1).

CHAPTER 1

Security overview

In this chapter

Application security overview

To ensure security in the Central Designer 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

In the Central Designer Administrator application, an administrator should require that each user password meets the following requirements, which you set in the **System Config > Settings > Security** section of the Central Designer Administrator application:

- Expires every 90 days. Configure this option in the **Passwords expire every** field.
- Has not been used recently. Configure the number of previously-used passwords that cannot be reused in the **Enforce password history** field.
- Contains a minimum of 8 characters. Configure this option in the **Minimum password length** field.
- Contains at least two of the following. Configure this option by setting the **Password complexity** setting to High.
  - One letter and one number.
  - One non-alphanumeric character.
  - One upper-case and one lower-case letter, character, and at least either one number or special character.

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).

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 roles, and assign rights to roles so that users can perform only the tasks necessary for their jobs.

For more information, see:

- *Rights assigned to roles* (on page 13).
- *Users assigned to roles* (on page 13).

CHAPTER 2

Secure installation and configuration

In this chapter

Installation overview

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

Transport Layer Security (TLS)

To encrypt the transmission of data between the application server and the client computers, you must enable Transport Layer Security (TLS) and obtain an X.509 certificate using your company certificate store or a third party.

For improved security, Oracle recommends that you disable SSL on the Central Coding application server and enable TLS 1.1 or above.

Signing authorizations and deployment packages

Signing web service authorizations and deployment packages is required. You must install the certificates used for signing on all application servers before you install the Central Designer application server. During the Central Designer application server installation, you are prompted to select a certificate for signing web service authorizations, and a certificate for signing deployment packages and InForm web service authorizations.

For more information, see the *Installation Guide*.

Use digital certificates issued by Certificate Authorities

A Certificate Authority (CA) assures users that the server information has been verified by a trusted source.

Oracle recommends that you use digital certificates that are issued by a Certificate Authority, and that do the following:

- Verify the server and domain.
- Use 256-bit encryption.
- Include a $1 million per year warranty.

Configure strong database passwords

When you install the Central Designer application, a system database administrator user is created. Only a system database administrator can perform the installation. Ensure all your database passwords are strong passwords.

Close all unused ports

Keep only the minimum number of ports open. You should close all ports not in use.

The Central Designer application uses the following ports:

- **80**—Used when the client applications are separated from the application servers and database server by a firewall, and do not use an SSL connection (HTTP).
- **443**—Used when the client applications are separated from the application servers and database server by a firewall, and use an SSL connection (HTTPS).
- **1521**—Used by the Oracle Listener service.
- **53000**—Used for communication between application servers behind a firewall.

Disable all unused services

The Central Designer application installs the job scheduler service on each application server. Make sure the job scheduler service is running, and disable unknown, unused services.

Post-installation configuration

Restrict access to Central Designer server machines

Allow only administrator and system accounts access to the Central Designer application server and database server machines.

Limit the number of users with access to the server machines. 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 roles

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

For more information, see:

- *Rights assigned to roles* (on page 13).
- *Users assigned to roles* (on page 13).

Configure IIS to prevent clickjacking

To secure the web server and prevent clickjacking on the http://<*server name*>/CentralDesignerInstall page, from which you install the Central Designer and Central Designer Administrator applications, configure the HTTP response header in IIS.

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 in the Central Designer Administrator software. For the recommended settings, see *General security principles* (on page 3) and the *Administrator Guide*.

- Number of days before the password expires. Maximum recommended setting is 90 days.
- Number of recently used passwords that are remembered in the system and cannot be reused. Minimum recommended setting is four passwords.
- Minimum length of the password. Minimum recommended setting is eight characters.
- Number of login attempts allowed. Maximum recommended setting is three.
- Password complexity. Recommended setting is High.
- Amount of time that a user is locked out after exceeding the allowed number of login attempts. Recommended setting for the system and user accounts is 30 minutes.
- Length of time a user can be inactive before session timeout. Recommended setting is 20 minutes.
- Amount of time before a user must reauthenticate during a session. Recommended setting is four hours.

Passwords for new users

When you create new users, the users should change their passwords the next time they log in.

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.

No data loss after a session transaction

The Central Designer application is 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 in the application without losing data.

This security feature is controlled by the following settings in the Central Designer Administrator application:

- **Inactivity timeout**—Number of minutes of inactivity that can pass before the Central Designer application requires a user to log in again.
- **User must re-authenticate every**—Number of minutes that a session can be active before the Central Designer application requires a user to log in again.

Select values for these settings that work with your studies.

Automatically deactivated user accounts

The Central Designer application is 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 in the Central Designer Administrator application, 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 users.
- Terminate and deactivate users.

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 to the application. All users, including terminated users, remain in the study for audit purposes. A terminated user can never be activated or deactivated. If you terminate a user account, you can never use the account again.

- Deactivate a user.

  Typically, a user is automatically deactivated when the user fails to log in after the number of attempts set in the Central Designer Administrator software. After the user account is deactivated only an administrator can manually reactivate the user. The user must be reactivated before the user can work in the application.

Security events logs

The Central Designer application is configured to log the following security events:

- Successful logins.
- Failed logins.
- Password changes.
- Unauthorized access attempts.
- Unexpected failed validations of SAML tokens (indicating attempted bypass of validation).
- Changes to password management policies.

The following information is logged for every security event:

- Date and time.
- IP address.
- User name.
- Computer name.
- Event message, where applicable.

The data is captured in the PM_AUDIT_EVENT table. Because this table might grow rapidly over time, make sure to periodically export it, and then either truncate the table, or delete older rows.

Application security features

Rights assigned to roles

A right is the permission to perform a specific activity. A role can have a library, study, or application scope. Each scope has a set of rights that you can grant to the role.

Rights grant access to different parts of the Central Designer and Central Designer Administrator applications. 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 Central Designer application, an administrator with the right to modify user information assigns the user to a role in the library, study, or application scope, providing the user permissions to perform specific activities.

For example, a user can be assigned to the Study Collaboration role, which contains the right to create and assign tasks. The individual Create and assign tasks right is static, but the group of rights assigned to the Study Collaboration role are configurable.

For more information, see the *Administrator Guide*.

Users assigned to roles

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

In addition, for each library and study role, a corresponding team exists. When you assign a user to a role, the user is also assigned to the team for that role. To assign a user to a team associated with a role, you rust first assign the user to the role.

A user can be assigned to a role that has one of the following scopes:

- **Library**—A user assigned to a library role is granted the rights associated with the role only in libraries where that user is also a member of the library team for the role.
- **Study**—A user assigned to a study role is granted the rights associated with the role only in studies where the user is also a member of the study team for the role.
- **Application**—A user assigned to an application role is granted all of the rights that are associated with the role, without restrictions.

You can also grant users the rights to perform administrative tasks such as configuring users, roles, rights, and system configuration settings. Administration users can also have unlimited rights in the Central Designer application. Ensure that you limit the users who have administration rights. For a description of administration rights, see the *Administrator Guide*.

Default user

The Central Designer application installs the system user by default. During the installation, you configure a password for this user. In addition, you can configure the lockout time for the system user separately from all other users. By default, this user is assigned the superuser and DesignerAdministrator roles.

Oracle recommends that you create administrator accounts for individual users, and delete the system user after the initial application configuration.

Data security features

Protecting study objects

You can protect a library or a study to prevent users from making changes to study objects that you do not want to be modified.

When you protect a study or library, changes cannot be made to study objects or to the structure of the study or library.

When a study object is protected, its icon changes to reflect its protected state.

For more information, see the *Administrator Guide*.

Audit trails for data security

Audit trails are comprehensive records that include information about each change that occurs in the Central Designer application.

The audit trail for the Central Designer application records each change, and for each change:

- Person who made the change.
- Date and time of the change.

You cannot modify data in an audit trail. For more information, see the *User Guide*.