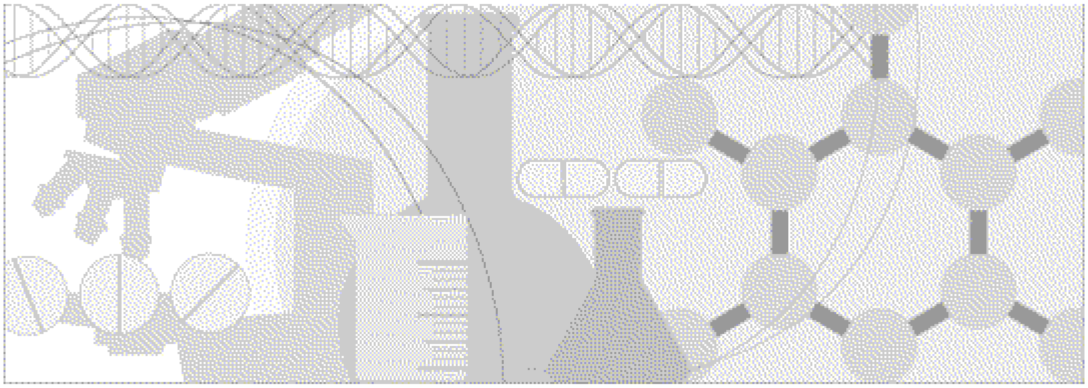
Secure Configuration Guide

Oracle® Health Sciences Central Coding
Release 3.1



Part Number: E69158-01

Contents

CHAPTER 1

Security overview

In this chapter

Application security overview

To ensure security in the Central Coding 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.
- Expires after 90 days.
- Does not contain a common word, name, or any part of the user name.

For information about specific password configuration settings available in Central Coding, see ***Password configuration for user security*** (on page 10).

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 11).

Provide only the necessary rights to perform an operation

Configure rights, assign roles to users, and assign users to work teams so that they 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).
- ***Users assigned to work teams*** (on page 13).

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 ***Restricted viewing of sensitive data*** (on page 14).

CHAPTER 2

Secure installation and configuration

In this chapter

Installation overview

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

Secure with HTTPS

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

Enable TLS 1.2 and higher on the Central Coding application server

Oracle recommends that you configure the following security settings on the Central Coding application server:

- Enable TLS 1.2 and higher.
- Disable SSL 2.0, SSL 3.0, TLS 1.0, and TLS 1.1.

For more information, see the *Installation Guide*.

Configure strong database passwords

During the Central Coding installation, you are prompted to create a single initial user and to create a password for the user. This user logs into the Central Coding application and creates all additional users. Ensure all your database passwords are strong passwords.

Close all unused ports

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

The Central Coding application always uses the following ports:

- **Port 1521**—Default connection to the Oracle database.
- **One port between 14000-14100**—For connection to the Job Scheduler. When multiple instances of the Central Coding application are installed on the same server, the port number is incremented for each additional instance.

The Central Coding application may use the following ports:

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

> **Note: The Central Coding application does not require both Port 80 and Port 443. You can configure the Central Coding application to use only HTTP or only HTTPS. For more information, see the *Installation Guide*.**

Disable all unused services

Disable all unused services.

The Central Coding application uses the following services:

- Central Coding Job Scheduler Service.
- 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.

Install a signing certificate

The Central Coding software uses X.509 digital certificates for securing communications with:

- The Job Scheduler service—You select the certificate in the installation wizard and you can replace it after installation using a utility installed with Central Coding.
- InForm Adapter web services—You select the certificate using a utility installed with Central Coding

A single certificate can be used for securing communications with both the Job Scheduler and the InForm Adapter web services. Use a digital certificate issued by a recognized Certificate Authority (CA).

For more information, see the *Installation Guide*.

Post-installation configuration

Restrict access to Central Coding server machines

Allow only the necessary user accounts access to the Central Coding 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 more information, see ***Password configuration for user security*** (on page 10).

Configure roles and rights

Configure rights and assign roles to users so that they can perform only the tasks necessary for their jobs. For more information, see ***Rights assigned to roles*** (on page 13) and ***Users assigned to roles*** (on page 13).

CHAPTER 3

Security features

In this chapter

User security features

Password configuration for user security

In environments with native authentication, an administrator can define the following formatting, entry, and reuse requirements for passwords directly in the Central Coding application on the System Configuration page.

- **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.

Passwords for new users

For security, in environments with native authentication three types of users can be defined in the Central Coding application. In all cases, the user profile is stored in the Central Coding database along with the user ID. The user types differ in where the system stores the passwords and how the system authenticates the user. The user type is set on the User details page in the Central Coding user interface.

- **Native user**—Password maintained by the Central Coding application.

  When the user logs in, the authentication module hashes the password entered by the user and compares it to the hashed password stored in the database. The user is granted access to the application only if the hashes match.

- **Windows user**—Does not have a password stored in the database.

  When the user logs in, the authentication module uses the username and password entered on the Login page and uses a Windows API to authenticate the user.

  In this mode, the Central Coding application has no knowledge of what the password is, and it is up to Windows to determine if the user is granted access. This user type requires Central Coding users to be created as part of a Windows domain. The format of the user ID supports only the user ID, such as **joe** if you want to log in to the current domain, or **EAST\joe** if you want to authenticate the user **joe** in the domain **EAST**.

- **Certificate user**—The system checks a digital certificate for a valid user name and password.

Login security

Users must enter their user names and passwords to log in. The application does not allow duplicate user names. There are two authentication methods, depending on the type of environment:

- **Environments with native authentication**—User information stored in the Central Coding application is used for authentication.
- **Oracle SSO environments**—User information stored in Oracle® Health Sciences Identity and Access Management Services (IAMS) is used for authentication.

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 Coding 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 without losing data.

In environments with native authentication, this security feature is controlled by the following settings on the System Configuration page:

- **Authentication inactivity timeout**—Period of inactivity after which a user session times out. Default is 20 minutes.
- **Authentication expiration**—Length of time after which a user session times out. Default is 4 hours (240 minutes).
- **Authentication token duration**—Length of time the user login is valid. Default is 10 hours.
- **Authentication token renew duration**—Length of time a previously created security token can be renewed without requiring a user to re-enter the user name and password. Default is one week.
- **Authentication token clock slush**—Number of minutes the server clocks for the Central Coding and InForm Adapter application servers can be out of sync. The default is 5 minutes (meaning that a token will be accepted if the server clock is within 5 minutes of the server that issued the token).

Automatically locked user accounts

The Central Coding 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 on the System Configuration page in environments with native authentication, the user account is locked out for a specified time interval and the user cannot log in. When the time interval elapses, the user can log in again.

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

- **Super user lockout timeout**—Length of consecutive time before an automatically locked super user account is unlocked.
- **Non-Super user lockout timeout**—Length of consecutive time before an automatically locked

non-super user account is unlocked.

Restricted access to the application

Access to the application can be restricted in the following ways.

- You can terminate a user.

  Typically, you terminate users who leave the organization. Terminated users cannot log in and cannot be reactivated. All users, including terminated users, remain in the study for audit purposes.

- You can deactivate a user.

  Typically, you manually deactivate users to keep them from accessing the application without removing them from the system. Deactivated accounts can be reactivated.

Application security features

Rights assigned to roles

The application comes with a predefined set of roles, which are configurable, and rights, which are not configurable.

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.

The predefined roles with selected rights represent typical job responsibilities. You can change the rights that are assigned to each role to suit the needs of your organization.

For example, a user assigned to the coder role has the appropriate rights to code requests. The individual Code Request right is static, but the group of rights assigned to the coder role is configurable.

For more information, see the *User 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.

Users assigned to work teams

Work teams provide a high level of control over the Central Coding request-processing workflow. Users are assigned to work teams. Rules are used to determine which work team or work teams are assigned to a coding request.

The criteria used to organize work teams may be defined by a system administrator to meet the business needs of an organization. Coding requests are assigned to work teams rather than to individual users. Work teams act as a filter for the list of coding requests that are presented to individual users. Users see only those requests that are assigned to the work team or work teams to which they belong.

Data security features

Restricted viewing of sensitive data

You can use roles, rights, and work teams to restrict the data users can view.

Audit trails for data security

Audit trails record updates to the following items:

- Users, roles, rights, and work teams.
- Coding request information.
- Codes, terms, dictionary version, and the reason for change.
- Coding request statuses.
- Approvals.
- Dictionaries.
- Synonym lists associated with the dictionary and changes from impact analysis.
- Synonym lists.
- Stopword lists.
- Algorithms.
- User authentication (available through database queries).

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*.

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 Central Coding 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

Document	Description	Part number	Last updated
Release Notes	This document provides information about system requirements and descriptions of new features, enhancements, and bug fixes for the current release.	E69155-01	3.1
Known Issues	This document provides information about known issues for the current release, along with workarounds, if available.	E69154-01	3.1
Secure Configuration Guide	This document provides an overview of the security features of the application, along with details about how to install, configure, and use the Central Coding application securely.	E69158-01	3.1
Installation Guide	This document provides an architectural overview of the Central Coding application, a description of system requirements, and step-by-step instructions for installing, uninstalling, managing and upgrading the Central Coding software.	E69159-01	3.1
User Guide	This document provides an overview of the Central Coding application, descriptions of all system functions, and step-by-step instructions for using and configuring the Central Coding application.	E69156-01	3.1
Quick Start for Coders and Approvers	This document provides a brief overview of the main tasks that coders and approvers perform in the Central Coding application, including step-by-step instructions for coding and approving requests.	E69161-01	3.1
Third Party Licenses and Notices	This document provides details about licenses and notices for third party technology that may be included in or distributed with the Central Coding application.	E69160-01	3.1

Note: If your environment is integrated with the InForm application, in addition to the items in the Central Coding documentation set, you must refer to the InForm Adapter *Installation Guide* for information about installing the InForm Adapter software.