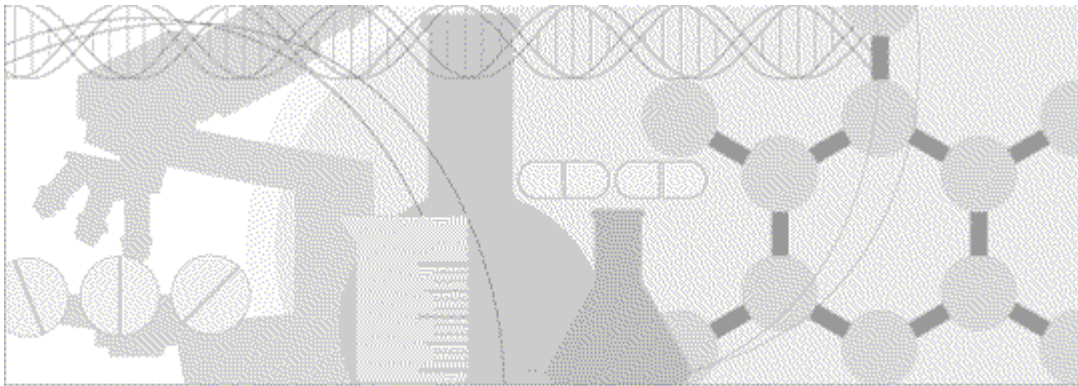


# Secure Configuration Guide

Oracle<sup>®</sup> Health Sciences Central Coding  
Release 3.0.4



ORACLE<sup>®</sup>

Part Number: E58691-01

Copyright © 2011 - 2014, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

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.

# Contents

<b>About this guide</b>	<b>v</b>
Overview of this guide.....	vi
Audience .....	vi
Documentation .....	vii
Documentation accessibility.....	viii
If you need assistance.....	ix
Finding Central Coding information and patches on My Oracle Support.....	ix
Finding Oracle documentation .....	x
Finding prerequisite software for Oracle Health Sciences applications .....	x
<b>Chapter 1 Security overview</b>	<b>1</b>
Application security overview.....	2
General security principles .....	3
<b>Chapter 2 Secure installation and configuration</b>	<b>5</b>
Installation overview .....	6
Secure with HTTPS .....	6
Disable SSLv2 and SSLv3 on the Central Coding application server.....	6
Configure strong database passwords.....	6
Close all unused ports.....	6
Disable all unused services.....	7
Install a signing certificate.....	7
Post-installation configuration .....	8
Restrict access to Central Coding server machines .....	8
Configure strong user passwords .....	8
Configure roles and rights.....	8
<b>Chapter 3 Security features</b>	<b>9</b>
User security features .....	10
Password configuration for user security.....	10
Passwords for new users .....	10
Login security.....	11
No data loss after a session transaction.....	11
Automatically locked user accounts .....	11
Restricted access to the application.....	12
Application security features.....	13
Rights assigned to roles .....	13
Users assigned to roles .....	13
Users assigned to work teams .....	13
Data security features.....	14
Restricted viewing of sensitive data .....	14
Audit trails for data security .....	14



# About this guide

## In this preface

Overview of this guide.....	vi
Documentation .....	vii
If you need assistance.....	ix

## Overview of this guide

The *Secure Configuration Guide* provides an overview of the security features provided with the Oracle® Health Sciences Central Coding application, including details about the general principles of application security, and how to install, configure, and use the Central Coding application securely.

## Audience

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

# Documentation

The product documentation is available from the following locations:

- **Oracle Software Delivery Cloud** (<https://edelivery.oracle.com>)—The complete documentation set.
- **My Oracle Support** (<https://support.oracle.com>)—*Release Notes* and *Known Issues*.
- **Oracle Technology Network** (<http://www.oracle.com/technetwork/documentation>)—The most current documentation set, excluding the *Release Notes* and *Known Issues*.

All documents may not be updated for every Central Coding release. Therefore, the version numbers for the documents in a release may differ.

Title	Description
<i>Release Notes</i>	The <i>Release Notes</i> document presents information about new features, enhancements, and updates for the current release.
<i>Known Issues</i>	The <i>Known Issues</i> document presents information about known issues for the current release.
<i>Secure Configuration Guide</i>	The <i>Secure Configuration Guide</i> provides an overview of the security features provided with the Oracle® Health Sciences Central Coding application, including details about the general principles of application security, and how to install, configure, and use the Central Coding application securely.
<i>Installation Guide</i>	The <i>Installation Guide</i> provides the following: <ul style="list-style-type: none"> <li>• Architectural overview of the Central Coding application</li> <li>• Step-by-step instructions for installing, upgrading, and uninstalling the Central Coding software</li> <li>• Descriptions of system functions</li> <li>• Step-by-step instructions for managing the Central Coding application at the server level, including loading coding dictionaries, adding studies and adapters using the command line, and producing performance metrics.</li> </ul>
<i>User Guide</i>	The <i>User Guide</i> provides an architectural overview of the Central Coding application, descriptions of all system functions, and step-by-step instructions for using the Central Coding application and managing the coding dictionaries.
<i>Quick Start for Coders and Approvers</i>	The <i>Quick Start for Coders and Approvers</i> provides a brief overview of the tasks that coders and approvers perform in the Central Coding user interface, including step-by-step instructions for coding and approving requests, and working with queries.
Page-level Help	The page-level Help describes the function(s) and fields for each page in the user interface.

**Note:** If you are integrating 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.

## 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

Oracle customers have access to support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info>, or if you are hearing impaired, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs>.

## Finding Central Coding information and patches on My Oracle Support

The latest information about the Central Coding application is on the Oracle Support self-service website, My Oracle Support. Before you install and use the Central Coding 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 **FAQs** 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](http://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 .....	2
General security principles .....	3

## 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 more information, 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 .....	6
Post-installation configuration.....	8

## 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.

### Disable SSLv2 and SSLv3 on the Central Coding application server

Oracle recommends that for improved security you disable SSLv2 and SSLv3 on the Central Coding application server and enable TLS1.0 and above. For more information, see the Microsoft website (<http://social.technet.microsoft.com>).

### 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

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 Central Coding application always uses the following port:

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

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 the following communications:

- Central Coding securely communicates with the Job Scheduler service. The installation wizard includes the ability to select a certificate for Job Scheduler.
- Central Coding securely invokes InForm Adapter web services. A utility is provided to select a certificate that will be used to secure InForm Adapter web services.

A single certificate can be used for securing both Job Scheduler and InForm Adapter web services.

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 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 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 .....	10
Application security features.....	13
Data security features .....	14

# User security features

## Password configuration for user security

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

- **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, 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.

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.

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

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 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.

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*.