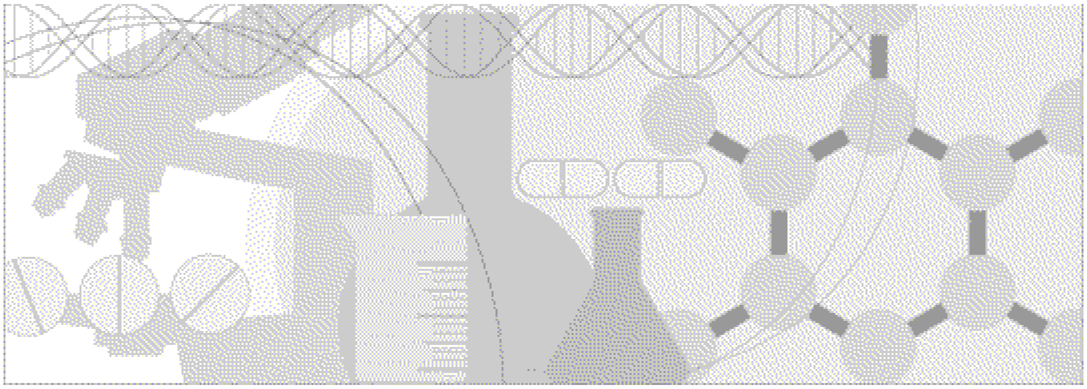
Secure Configuration Guide

Central Coding™ 3.0 SP1



Part Number: RN-CCD30-003-010

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software -- Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

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

About this guide

In this preface

Overview of this guide

The *Secure Configuration Guide* provides an overview of the security features provided with the 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.

Related information

Documentation

The Central Coding 3.0 SP1 documentation includes the following items. All documentation is available from the Phase Forward Download Center and the Oracle Software Delivery Cloud.

Title	Description
Release Notes	The *Release Notes* document presents information about new features, enhancements, and updates for the current release.
Known Issues	The *Known Issues* document presents information about known issues for the current release. **Note:** The most current list of known issues is available on the Phase Forward Extranet. To sign in to the Extranet, go to www.phaseforward.com and click **Customer Login**. Enter your email address and password, and navigate to the **Known Issues** section. Select a product, and then enter your search criteria.
Secure Configuration Guide	The *Secure Configuration Guide* provides an overview of the security features provided with the Central Coding application including details about the general principles of application security, and how to install, configure, and use the Central Coding application securely.
Installation Guide	The *Installation Guide* provides an architectural overview of the Central Coding application, a description of the system requirements, and step-by-step instructions for installing, uninstalling, and upgrading the Central Coding software. This document is also available from the Documentation CD.
User Guide	The *User Guide* 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. This document is also available from the Documentation CD and the Central Coding user interface.
Software Administration Guide	The *Software Administration Guide* provides an architectural overview of the Central Coding application, descriptions of system functions, and 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. This document is also available from the Documentation CD.

Title	Description
Quick Start for Coders and Approvers	The *Quick Start for Coders and Approvers* 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. This document is also available from the Documentation CD.
Page-level Help	The page-level Help describes the function(s) and fields for each page in the user interface. This document is also available from the Central Coding 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 and configuring X.509 digital certificates.

If you need assistance

If you are an Oracle customer with a maintenance agreement, you can contact the Global Support Center for assistance with product issues.

Your maintenance agreement indicates the type of support you are eligible to receive and describes how to contact Oracle. Additionally, the Oracle website lists the toll-free support number for your product, location, and support level:

http://www.oracle.com/support

In the event that our toll-free telephone service is interrupted, please use either of the following methods to contact the Global Support Center:

- Email

  saasclinicalsupport_ww@oracle.com

- Telephone

In the US:	1-800-633-0925
Outside the US:	+44 207 13 12 801

Oracle also provides assistance with User Management, Site Assessment, and Provisioning. Please refer to your Master Services Agreement and individual Statement of Work to determine if you are eligible to use these services.

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 8 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

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 Socket Layer (SSL)

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

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.

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

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 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*.