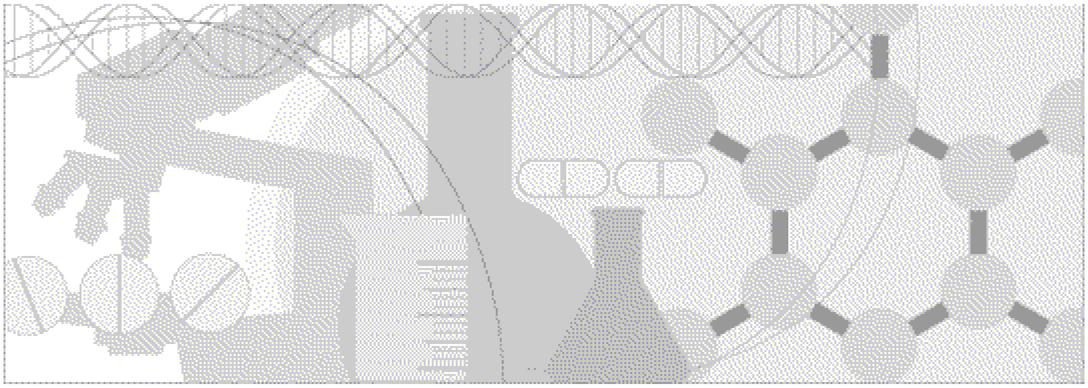
Secure Configuration Guide

Clintrial Integration Solution
Release 4.6.2



Part Number: E69249-02

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.

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

CHAPTER 1

Security overview

In this chapter

Application security overview

To ensure security in the CIS 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 ***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.

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

For more information, see ***Application security features*** (on page 12).

CHAPTER 2

Secure installation and configuration

In this chapter

Installation overview

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

Configure strong database passwords

During the CIS installation, you are prompted for two database usernames and passwords, one for the CIS database, the other for the CIS administration database user. Ensure that these database passwords are strong passwords.

Use Transport Layer Security (TLS)

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

For improved security, Oracle recommends that you configure the following security settings on the CIS application servers:

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

Install a signing certificate issued by a Certificate Authority

The CIS software uses a X.509 digital certificate to secure communications between CIS and InForm Adapter web services.

You select the certificate during installation or during the post-installation configuration. For more information, see the *Installation Guide*.

Use a digital certificate issued by a recognized Certificate Authority (CA) that:

- Assures users the server information has been verified by a trusted source.
- Verifies the existence of the organization and the ownership of the domain.
- Provides a monetary warranty when issued.

Disable all unused services

Disable all unused services.

The CIS application uses the following services:

- IIS Admin Service.
- Oracle MTS Recovery Service.
- Oracle TNS Listener.
- World Wide Web Publishing Service.
- PhaseForward CIS Sync Job Scheduler Service.
- PhaseForward CIS Sync Service.

Close all unused ports

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

The CIS application uses the following TCP ports:

- **Port 1521**—Default connection to the Oracle database.
- **Port 1139**—Used by the Phase Forward CIS Sync Job Scheduler.
- **Port 9000**—Used by the Phase Forward CIS Sync Service.

The CIS application may use the following ports:

- **Port 80**—Default HTTP port.
- **Port 443**—Default HTTPS port.

Post-installation configuration

Restrict access to CIS server machines

Allow only the necessary user accounts access to the CIS server machine. Disable or delete any unnecessary users.

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 ***Application security features*** (on page 12).

Secure the predefined CIS user accounts

CIS includes the following predefined user accounts:

- CAAdmin
- CISAdmin
- CISPower
- CISUser
- Service

To secure your CIS environment, Oracle recommends that you change the passwords for these accounts. 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 and entry requirements for passwords directly in the CIS application on the Security tab of the Configuration page.

- Minimum length of the password. Recommended setting is 8 characters.
- Number of consecutive failed login attempts allowed. Recommended setting is 3.
- Number of days before the password expires. Recommended setting is 30 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

CIS requires users to authenticate by logging in with a unique user name and password. 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 re-authentication

The CIS 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 Security tab of the Configuration page:

- **Inactivity timeout**—Period of inactivity after which a user session times out. Default setting is 20 minutes.
- **Authentication expiration**—Period of time after which a user session times out. Default setting is 4 hours.

Automatically locked user accounts

The CIS 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 Configuration page, the user account is locked out until a CIS administrator unlocks the user account. After the account is unlocked, the user can log in again.

For more information, see ***Password configuration for user security*** (on page 10).

Restricted access to the application

You can restrict user access to the application in the following ways:

- Terminate a user.

  Typically, you terminate users who leave the organization. Terminated users cannot log in. 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 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

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.

CIS includes predefined roles for the Synchronization pages and the Administration pages. 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.

When a new user is created, an administrator with the right to modify user roles assigns the user to one or more roles, providing the user permissions to perform specific activities.

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.

Data security features

Audit trails for data security

Auditing of transactions that occur in an integrated study occurs in both the Clintrial software and the InForm software.

The CIS application creates an audit trail with information about synchronization transactions.

For more information, see the *Administrator 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 CIS 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.

CIS 4.6.2 documentation

Item	Description	Part number	Last updated
Release Notes	The *Release Notes* document presents information about new features, enhancements, and updates for the current release.	E71106-01	4.6.2
Known Issues	The *Known Issues* document presents information about known issues for the current release.	E71107-01	4.6.2
Installation Guide	The *Installation Guide* provides procedures for installing, configuring, and upgrading the CIS Administration software. It also includes product interoperability considerations.	E71108-02	4.6.2
Secure Configuration Guide	The *Secure Configuration Guide* provides an overview of the security features provided with the Oracle® Health Sciences CIS application, including details about the general principles of application security, and how to install, configure, and use the CIS application securely.	E69249-02	4.6.2
Administrator Guide	The *Administrator Guide* explains how to use the CIS administration tool (CIS Administration) to manage adapters, load-balanced machines, CIS protocols, and synchronization connections. It includes troubleshooting, data transfer and storage information, and key database tables.	DC-CIS46-001-000	4.6 SP0
Designer Guide	The *Designer Guide* presents Integrated study design considerations.	DC-CIS46-002-000	4.6 SP0

Item	Description	Part number	Last updated
Online Help	The online Help includes field definitions, instructions for performing the tasks on each page of the CIS Administration user interface, and concepts and procedures for performing synchronization and general administrative tasks with the CIS Administration application.	DC-CIS46-003-000	4.6 SP0
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 CIS software.	E59144-01	4.6.1.4