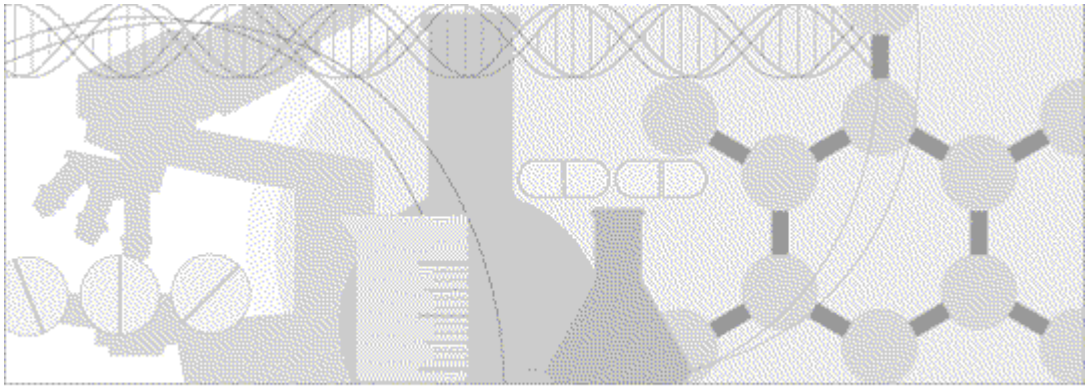
Secure Configuration Guide

Oracle® Health Sciences IRT Cloud Service Release 5.5.7



ORACLE

Part Number: E69423-01

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

Audience

This guide is for users who install and configure the IRT application, and developers who develop and test custom study-specific code based on the IRT core.

Documentation

The product documentation is available from the following locations:

- My Oracle Support (https://support.oracle.com)—*Release Notes* and *Known Issues*. These are posted for Oracle employees only.
- 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 IRT release. Therefore, the version numbers for the documents in a release may differ.

Title	Description	Last updated
Release Notes	The *Release Notes* document lists the system requirements for the IRT Designer software, and provides information about new features, enhancements, and updates for the current release.	5.5.7
Known Issues	The *Known Issues* document provides information about known issues for the current release, along with workarounds, if available.	5.5.7
Secure Configuration Guide	The *Secure Configuration Guide* provides an overview of the security features provided with the Oracle® Health Sciences IRT application, including details about the general principles of application security, and how to install, configure, and use the IRT application securely.	5.5.7
Installation Instructions	The *Installation Instructions* provide an overview of the components of the IRT application, a description of a typical IRT environment, and step-by-step instructions for installing the IRT software and deploying study packages.	5.5.7
User Guide	The *User Guide* provides online access to all tasks you can perform with the IRT application, as well as supporting concepts and reference information. You can access the *User Guide* from the Help button in the IRT application.	5.5.7
Administration Guide	The *Administration Guide* provides concepts and step-by-step instructions you use to perform tasks such setting up roles and permissions, configuring corrections to subject information, setting up notifications, adding custom menus to the user interface, managing integrations, and using features for testing and support. The *Administration Guide* is included in the online help in its entirety.	5.5.7
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 IRT software.	5.5.7

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 IRT information and patches on My Oracle Support

The latest information about the IRT application is on the Oracle Support self-service website, My Oracle Support. Before you install and use the IRT 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.

CHAPTER 1

Security overview

In this chapter

Application security overview

To ensure security in the IRT application, carefully configure the following system components:

- Global Web Services (GWS)
- Web Container
- Client Support Tool/MT Application (CST/MT)
- IRT Core

Carefully configure the following third-party components:

- Web browsers
- Firewalls
- Load balancers
- Virtual Private Networks (VPNs)

General security principles

Use the latest versions of software and documentation

Before beginning the installation, check the Oracle Software Delivery Cloud (https://edelivery.oracle.com) or the Download Center (https://extranet.phaseforward.com) for the latest patchsets and patches, as well as the accompanying *Release Notes* and *Known Issues* documents, and the latest versions of the documentation.

Use the latest recommended versions of the IRT software, Windows server, .Net Framework, and SQL Server.

Keep passwords private and secure

Tell users never to share passwords, write down passwords, or store passwords in files on their computers.

All users should change their passwords when they log in for the first time.

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 permissions to perform an operation

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

For more information, see:

- *Permissions assigned to roles* (on page 12).
- *Users assigned to roles* (on page 12).

Monitor system activity

Ensure system security with good security protocols, proper system configuration, and system monitoring. Audit and review audit records. Each component within a system has some degree of monitoring capability. Follow audit advice in this document and regularly monitor audit records. For more information, see *Audit trails for data security* (on page 13).

Protect sensitive data

Collect only the minimum amount of sensitive information needed for the study.

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 access to sensitive data* (on page 13).

CHAPTER 2

Secure installation and configuration

In this chapter

Installation overview

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

Restrict network access to critical services

Set up a firewall between the internet and an isolated server and between the isolated server and the intranet. This configuration creates a demilitarized zone (DMZ), which blocks any illegal traffic and contains intrusions.

Keep both the IRT application middle-tier and the IRT database behind a firewall. In addition, place a firewall between the middle-tier and the database. The firewalls provide assurance that access to these systems is restricted to a known network route, which can be monitored and restricted, if necessary. As an alternative, a firewall router can substitute for multiple, independent firewalls.

Transport Layer Security (TLS)

Configure your environment so that the IRT application servers are hosted behind a firewall with an appliance such as an F5 load balancer for handling TLS and converting to HTTP.

The IRT application allows for TLS setup within the data center by forcing encryption on the SQL server.

Configure strong database passwords

Ensure all your database passwords are strong passwords.

Close all unused ports and open necessary 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 IRT application may use the following ports:

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

  Note: The IRT application does not require both Port 80 and Port 443. You can configure the IRT application to use only HTTP or only HTTPS.

- **Port 1244**—For Global Web Services (GWS).
- **Port 1433**—For access to the SQL server.

Disable all unused services

Disable all unused services. Install only the database engine feature on the SQL server.

The IRT application uses the following services:

- ASP.NET State Service (web server only).
- Net.Tcp Listener Adapter (web server only).
- Net.Tcp Port Sharing Service (web server only).
- Windows Time Service
- World Wide Web Publishing Service (web server only).

Post-installation configuration

Verify cookie settings

By default, the IRT Web Container installs the web.config file with the following cookie settings:

```
httpOnlyCookies="true"
requireSSL="true"
```

Do not change the httpOnlyCookies setting.

If you are using a dedicated TLS accelerator device, such as an F5 load balancer, and creating an HTTP connection from it to the IRT web server, change the requireSSL setting to "false".

Keep WSDL generation and GET/POST settings disabled

By default, IRT Global Web Services ships with a web.config file with WSDL generation and GET/POST disabled. These settings should not be enabled in a production environment. For more information, see the *Installation Instructions*.

Restrict access to the IRT server machines

Limit the number of users with access to the server machine. Disable or delete any unnecessary users.

Authorize Global Web Services

Any servers with applications that call Global Web Services (GWS) methods need to use the same encryption and validation keys as the server that is hosting GWS.

Copy the GlobalServices_AuthTicket_EncryptionKey and GlobalServices_AuthTicket_ValidationKey keys from the C:\ClarixIRTConfig\ServerSettings.config file and reference those keys in any other .config files (for example, web.config).

Set up forms authentication for R4 studies

By default, phone passwords are not written to the forms authentication ticket. For installations supporting legacy R4 studies, the following ASP.NET Forms Authentication setting should be turned on for backward compatibility.

```
supportLegacyTrials="true"
```

Protect sensitive information in configuration files

To protect sensitive information in configuration files (for example, passwords and encryption keys), use the .NET Protected Configuration. For more information, see your .NET documentation.

CHAPTER 3

Security features

In this chapter

User security features

Login security

IRT allows two types of authorization (phone and web) for a single user account.

Each password should meet the following guidelines:

- Does not contain the 6 digit numeric user ID.
- Does not contain a word from the dictionary table.
- Does not contain a common word, name, or any part of the user name.

You can control password requirements with the following configuration keys:

- **minPasswordLength**—Minimum password length. Passwords should contain a minimum of 8 characters.
- **maxPasswordLength**—Maximum password length.
- **minUpperCase**—Minimum upper case characters required. Passwords should contain at least one upper case character.
- **minLowerCase**—Minimum lower case characters required.
- **minNumeralAndSpecialCharacters**—Minimum numeric characters or special characters required. Passwords should contain at least one number or special character.
- **excludePhonePwds**—Excluded phone passwords. Phone passwords must be complex and at least 5 digits long.
- **pwdHistory**—Number of previous passwords to keep track of per user. A password should not be one of the last 5 passwords of the user.
- **passwordExpiration**—Password expiration. Passwords should expire after 60 days.
- **maxFailedLoginAttempt**—Maximum failed authentication attempts allowed.
- **minWaitAfterPasswordChange**—Minimum length of time before users are allowed to change their passwords again.
- **minWaitAfterFailedLogin**—Minimum wait time after each failed login attempt.
- **passwordResetTokenExpiresAfter**—Password or new user creation token expiration.
- **maxPasswordResetPerHour**—Maximum password resets allowed per hour per user.
- **failedLoginWindowTime**—Failed login time window.

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, the user account is locked and the user cannot log in.

A user with the appropriate permissions can unlock a user account.

Accounts are automatically locked after 3 invalid attempts within 10 minutes.

Restricted access to the application

By default, an authenticated user has no access to studies. To gain access to studies and specific features within studies, users must be granted access to the study and to a role within the study.

This security feature is controlled by the following settings in the CST/MT application:

- Add Users to Protocol
- Batch Add Users to Protocol

These settings allow specified users to view the studies in their list when they log in to the IRT application.

Application security features

Permissions assigned to roles

A right is the permission to perform a specific activity. A role is a collection of permissions.

Permissions grant access to different parts of the application. Entire parts of the application are hidden if users do not have the permissions to work in those areas.

The Manage Permissions administrative page in each IRT study maps the list of roles in the study to the available permissions in that study.

Users assigned to roles

The list of available roles can differ for each IRT study. You can modify the list of available roles in each study with the options on the Manage Roles page.

You can use the Upload Users batch process to assign users to roles. When a user accesses a study for the first time, the user must provide a User Authentication Code to activate their account.

You can manually assign users to roles by using the CST/MT application to access the Manage Users function and edit the protocol settings.

Data security features

Restricted access to sensitive data

You can use rights and permissions to restrict the users who can view sensitive data.

Access to confidential subject information is restricted. Therefore, your study is set up so that only specific users, such as clinical research coordinators, can enter subject data.

Audit trails for data security

An audit trail is available from the Audit History View and the Audit Site Report. 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.

CHAPTER 4

Security considerations for developers

In this chapter

Follow secure coding standards

Ensure that coding follows Oracle Global Product Security (GPS) standards.

Avoid direct SQL

Use LLBLGen collections and LINQ to LLBLGen rather than SQLConnection, SQLCommand, and SQLDataReader. The LLBLGen data access provider parameterizes all SQL sent to the database appropriately, which prevents SQL injection attacks.

Configure unique permission IDs

Each AppBlock, report, and page should have a unique permission ID. Do not share a general permission ID across features.

Use permission infrastructure

Use the infrastructure provided for checking whether the given user has access to a permission, site, depot, shipment, notification, and so on. These are provided as LINQ extension methods on the underlying collections.

For example:

```
Sites.DataSource = _linq.Site.ForUser(CurrentSession.UserID);
```

Verify URL and form parameters

The base permissions infrastructure automatically checks whether the current user can access a given page. However, you must verify that the user has access to the given record(s) being edited.

For example:

```
/DrugOrderShipInfo.aspx?SDR_enterDrugOrderFld=010004
```

The permissions system redirects any user without permission to enter shipment information. However, the code still verifies that drug order 010004 is in the list of shipments available to this user.

For example:

```
_linq.Shipment.ForUser(CurrentSession.UserID)
```