Oracle® Health Sciences ClearTrial Cloud Service

Secure Configuration Guide

Release 5.3

E60054-01

February 2015

This guide describes essential security management options for the Oracle Health Sciences ClearTrial Cloud Service application for the 5.3 release.

1 Introduction

This security guide provides guidelines and recommendations for securely installing, configuring, and managing the ClearTrial software and its system components.

1.1 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.

This guide presents the following security guidelines and recommendations:

- "General Security Principles" on page 1-1.
- "Secure Installation and Configuration" on page 1-3.
- "Application Security Features" on page 1-4.

2 General Security Principles

This section provides general recommendations for securing the application.

For Web enablement, you must protect resources from unauthorized access via the Internet. In addition, access to highly confidential data or strategic resources should be available to only a few trusted users or system administrators.

2.1 Configure Strong Passwords on the Database

Although the importance of passwords is well known, the following basic rule of security management is worth repeating:

Ensure all your passwords are strong passwords.

You can strengthen passwords by creating and using password policies for your organization.

> **Note:** For system accounts, avoid applying password policies that include a password lifetime. Key components of the application may stop working upon automatic password expiration.

You should modify the following passwords to use your policy-compliant strings:

- Passwords for the database default accounts, such as SYS and SYSTEM.
- Passwords for the database application-specific schema account, *cleartrial_530*.
- Password for the database listener. If you do not configure the database listener to require an authorization password, you unnecessarily expose the underlying database service names to unauthorized individuals.

For guidelines on securing passwords and for additional ways to protect passwords, refer to the *Oracle Database Security Guide* specific to the database release you are using.

2.2 Change Passwords Periodically

It is good practice to change both system account passwords and user passwords periodically. Follow your organization's operating procedures for the frequency of making changes.

2.3 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.

Encourage users to choose password-reset questions and answers that are easy for them to remember, but difficult for someone else to guess.

2.4 Keep Software Up to Date

Keep all software versions current by installing the latest patches for all components, including all critical security updates.

2.5 Implement the Principle of Least Privilege

In implementing the principle of least privilege, you grant users the fewest number of permissions needed to perform their jobs. You should also review user permissions regularly to determine their relevance to users' current job responsibilities.

2.6 Monitor System Activity

One of the main requirements of system security is monitoring. Auditing and reviewing audit records address this requirement. Each component within a system has some degree of monitoring capability. Oracle recommends that you establish a policy to check and monitor activities in your system regularly. Refer to the database and application server documentation for audit functionality.

2.7 Restrict Network Access to Critical Services

Oracle recommends that you install a firewall between the WebLogic application servers and the Internet. 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 substitutes for multiple, independent firewalls.

See your firewall documentation or ask your system administrator for assistance.

There should not be any access from the Internet to the application's Database server. The Database server should only respond to connections from the WebLogic application servers.

3 Secure Installation and Configuration

This section provides information for securely installing and configuring the ClearTrial application including, but not limited to, configuring firewall settings, installing signed certificates when using HTTPS, and closing unused ports.

3.1 Install Critical Patch Updates (CPUs) and Critical Patch Set

To ensure that your installation includes up-to-date security fixes, install the latest Oracle CPUs and critical patch set.

3.2 Use SSL (HTTPS) Between the Internet and Application Servers

Information sent over the network and across the Internet in clear text may be intercepted. Secure Sockets Layer (SSL) and its successor, Transport Layer Security (TLS), are features that provide encryption of network traffic between the browser and the Oracle Clinical web server.

Configure your environment so that the ClearTrial WebLogic application servers are hosted behind a firewall with an appliance such as an F5 load balancer for handling HTTPS.

The load balancer should be the SSL termination point as the WebLogic application servers respond only to HTTP.

3.3 Close All Open Ports Not in Use

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

3.4 Secure the Environment

To ensure security in the ClearTrial application, carefully configure all components, including the following third-party components:

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

For more information, see the documentation for the application you are configuring.

4 Application Security Features

ClearTrial is a multi-tenant application that provides application security features at a customer or tenant level. These are available to configure when a customer or tenant is provisioned by Tier 1 support:

- Forgot password—Allow or not allow users to reset password via the **Forgot Your Password** link.
- Lock IP to session—Record the user's IP address in the session and prevent requests from any other IP for that session. This prevents session hijacking.
- Login Attempts—Establish the maximum number of unsuccessful login attempts allowed for a user before the account is locked.

In addition to these tenant-level features, the customer's delegated administrator can also use:

- **User Access Control**—Assign users to predefined roles and assign further permissions within those roles. By doing so, the customer's administrator can restrict the access of users to only the features that are appropriate for their job responsibilities.

  For more information about primary roles and additional capabilities, see the *Oracle Health Sciences ClearTrial Cloud Service System Administrator User Guide*.

4.1 Authentication Methods

The ClearTrial software requires users to authenticate by logging in with a tenant identifier, user name, and password.

4.2 User Access Control

To access the ClearTrial application, every user must have a user account. Delegated system administrators are created for customers to manage the user accounts for their organizations.

4.2.1 Provide Only the Necessary Rights to Perform an Operation

Assign database roles or custom roles so that users can perform only the tasks necessary for their jobs.

5 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 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.

Oracle Health Sciences ClearTrial Cloud Service Secure Configuration Guide, Release 5.3
E60054-01