Oracle® Clinical, Oracle® Clinical Remote Data Capture, and Oracle® Thesaurus Management System

Security Configuration Guide

Release 5.1

E53566-02

March 2015

This guide describes essential security management options for the following applications:

- Oracle Clinical Release 5.1
- Oracle Clinical Remote Data Capture Onsite (RDC Onsite) Release 5.1
- Oracle Thesaurus Management System (TMS) Release 5.1

1 Introduction

This security guide provides guidelines and recommendations for installing, configuring, and monitoring Oracle Clinical, RDC Onsite, and TMS to make them more secure in customer environments. This is a practical guide for technical users, installers, and system administrators who implement and maintain the Oracle Clinical, RDC and TMS systems. This document discusses guidelines for hardening of the OC, RDC and TMS security applications, and other system hardening configuration recommendations.

This document cannot address every security scenario that might be applicable to a particular implementation and environment; however, it provides basic recommendations for securing Oracle Clinical, RDC Onsite, and TMS. Oracle recommends that you fully test the security setup in a non-production environment to ensure proper functionality and integrity before you install the software.

This security guide will help you ensure that Oracle Clinical and the various components involved in the setup are properly secured. Oracle recommends that you secure each Oracle Clinical, RDC Onsite, and TMS environment in alignment with your company's enterprise security policies.

This guide is not intended to replace the Oracle Clinical technical documentation (Install Guide and Administration Guides) delivered with the product. It provides references to relevant information in Install and Administration technical documentation guides. Readers of this guide should have a good understanding of the Oracle Clinical (OC), Remote Data Capture (RDC) and Thesaurus Management System (TMS). Implementing Oracle Clinical security requires an in-depth understanding of many disciplines, including WebLogic Server administration, Oracle Database security administration, and network security administration.

This guide presents the following security guidelines and recommendations:

- "General Security Principles" on page 1-2
- "Secure Installation and Configuration" on page 1-3
- "Application Security Features" on page 1-6

ORACLE

In addition, see the following documents for security configuration instructions:

- *Oracle Fusion Middleware Understanding Security for Oracle WebLogic Server*
- *Oracle Fusion Middleware Securing Oracle WebLogic Server*
- *Oracle Fusion Middleware Information Roadmap for Oracle WebLogic Server*
- *Oracle Application Server Web Services Security Guide*

2 General Security Principles

This section provides general security recommendations for securing any application.

The most critical resource to protect is the Oracle Clinical database, which contains information that is both sensitive and critical to the performance of your business. Oracle recommends that you protect most of your computing resources from unauthorized access, manipulation, or destruction from both internal and external parties.

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 Restrict Network Access to Critical Services

Oracle recommends that you install a firewall between the database and application servers. In addition, if you are using Web Tier, consider placing a firewall between the Oracle HTTP Server (OHS) and the WebLogic Server. 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.

If the Oracle Clinical client computer has a personal firewall, you must either disable it or configure it for RDC to function correctly.

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

2.2 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.

2.3 Set Up a Change Management Process

Oracle recommends that you establish a policy to set up a change management process to keep track of all the changes in your software systems. All changes to software should be approved and audited.

2.4 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.

2.5 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.

2.6 Use Profiles

In the Oracle database, a profile is a named set of resource limits and password parameters that restrict database usage and instance resources for a user. By default, every Oracle Clinical, RDC Onsite, and TMS user is assigned the DEFAULT profile. You can change its limitations on resources or password use or assign a separate profile to each user or user role. Each user can have only one profile. For more information, see the *Oracle Clinical Administrator's Guide*, the *Oracle Database Security Guide*, and Section 3.9, "Limit the Number of Sessions per User."

2.7 Lock Computers to Protect Data

Encourage users to lock computers that are left unattended.

2.8 Close All Open Ports Not in Use

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

2.9 Secure the Environment

To ensure security in the Oracle Clinical, RDC Onsite, and TMS applications, 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.

2.10 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.

3 Secure Installation and Configuration

This section provides information for securely installing and configuring the Oracle Clinical, RDC Onsite, and TMS applications, 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.

For more information, see the *Oracle Clinical Installation Guide*.

3.2 Use SSL (HTTPS) Between Browser and Web Server

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.

For more information, see the *Oracle Clinical Installation Guide*.

3.3 Signed Certificates for HTTPS

To support HTTPS for Oracle Clinical, you need to request a signed certificate from a Certificate Authority (CA) vendor such as Thawte or Verisign, and then import the signed certificate into the Oracle Wallet for the Oracle Application Server.

For more information, see the *Oracle Clinical Installation Guide*.

3.4 Disable Unused Services

The Oracle Clinical, RDC Onsite, and TMS applications do not use the following services or information for any functionality:

- **Simple Mail Transfer Protocol (SMTP).** This protocol is an Internet standard for e-mail transmission across Internet Protocol (IP) networks.
- **Identification Protocol (identd).** This protocol is generally used to identify the owner of a TCP connection on UNIX.
- **Simple Network Management Protocol (SNMP).** This protocol is one method for managing and reporting information about different systems.

Therefore, restricting these services or information will not affect those Oracle applications. If you are not using these services for other applications, Oracle recommends that you disable these services to minimize your security exposure.

If you need SMTP, identd, or SNMP for other applications, be sure to upgrade to the latest version of the protocol to provide the most up-to-date security for your system.

In addition, Oracle recommends that you remove unused Oracle Clinical User accounts if you are upgrading from earlier releases.

3.5 Replace Verbose Errors with Custom Messages

Web applications issue HTTP error messages, such as Error Code 500 (Internal Server Error) and Error Code 404 (Not Found), for servlet exceptions that occur at run time (for example, when a servlet is processing the form data). Some internal error messages are verbose and provide sensitive system information.

To tighten the security on your production systems, Oracle recommends that you replace the verbose error messages with brief customized messages.

You can create an HTML error page containing a custom message, and then use the XML error-page element and subelements in the web.xml file to specify the HTML

error page to use for the servlet exceptions. You can create a different error message for each error number or use the same generic message for more than one error.

Oracle recommends that you edit the web.xml file for the:

- RDC Onsite application
- OPA Administration utility
- TMS application

3.6 Secure the WebLogic Server

For information on securing the WebLogic Server, see:

- *Oracle Fusion Middleware Securing Oracle WebLogic Server*
- *Oracle Fusion Middleware Securing a Production Environment for Oracle WebLogic Server*
- "Security" in *Oracle Fusion Middleware Information Roadmap for Oracle WebLogic Server*

3.7 Provide Security for Session-Tracking Cookies

You can use the XML session-tracking element to provide security for the RDC Onsite and TMS Lite Browser session-tracking cookies.

In the orion-web.xml file, you can configure the following flags (attributes) for the session-tracking element:

- **set-secure —** Requests that your Internet browser only honor the HTTPS protocol to access Web sites. If you set the secure flag to **true,** users must enter https:// to access Web sites. Entering http:// will not work.
- **HttpOnly —** Requests that your Internet browser honor only the HTTP and HTTPS protocols to access Web sites. Other protocols, such as FTP, will not work.

> **Note:** If you configure the secure and HttpOnly flags for session-tracking cookies, you must make the changes on all servers in a load-balanced environment.

Once you complete the above changes, access to the application using HTTP will not work. Users will be forced to use HTTPS only.

3.8 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.

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 accounts, such as RXC, OPA, and RXC_PD. You can run the Set Password (set_pwd) utility to set stronger passwords for the default Oracle Clinical schemas. For details on using the utility, refer to the *Oracle Clinical Administrator's Guide*.
- 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.

3.9 Limit the Number of Sessions per User

To prevent any one user from potentially tying up all resources, limit the number of sessions any user can open concurrently.

To do this, do one of the following:

- Create a new profile, following instructions in the *Oracle Clinical Administrator's Guide* section "Creating a New Profile," and set SESSIONS_PER_USER to whatever number you choose. RDC Onsite users routinely use three sessions at once, so set the value to at least three. Assign the new profile to users, following instructions in the *Oracle Clinical Administrator's Guide*.
- Edit the DEFAULT profile that is assigned to all users by default. The DEFAULT profile initially defines unlimited resources, including for SESSIONS_PER_USER. You can change those limits with the ALTER PROFILE statement. See the *Oracle Database SQL Language Reference*.

3.10 Hide Oracle Forms Version Numbers

By default, the current version of Oracle Forms is displayed when someone accesses a forms servlet URL. This is because the form parameter in formsweb.cfg calls test.fmx, which displays the version number so that you can check the version you are running.

To change this behavior:

1. Create a new file based on test.fmx that does not display the version number.
2. In formsweb.cfg, default section, set form=*your_new_file*.

3.11 Secure the Reports Server

See My Oracle Support note *Secure the Showjobs Web Command in a Non Secured Reports Server in Oracle Reports 11g*, ID 1242614.1.

4 Application Security Features

This section includes:

- "Oracle Clinical Security" on page 1-7
- "RDC Onsite Security" on page 1-8
- "TMS Security" on page 1-10

4.1 Oracle Clinical Security

This section provides information for securing the Oracle Clinical application, users, and data.

4.1.1 Restrict Access to the Application

Use the following security features to ensure that users can access only the parts of the application that they need to do their jobs.

- **Assign study privileges:** To restrict user access to Oracle Clinical study and site data, you can define and maintain users' study privileges. You must explicitly give users access to study data, either by granting them Superuser status, which allows access to all studies, or explicitly granting access to specific studies or groups of studies (programs and projects). For more information, see the *Oracle Clinical Administrator's Guide*.
- **Configure menu-based security options:** Oracle Clinical includes a set of predefined database roles that allow access to a predefined set of Oracle Clinical menu items, including second- and third-level menu items. You can enforce security by assigning users only the database roles they need to do their work, preventing them from seeing other parts of the system and taking actions they are not authorized to take. For more information, see the *Oracle Clinical Administrator's Guide*.

4.1.2 Restrict Access to View Files

The logs and output files generated by PSUB batch jobs are stored in database tables. When you wish to view a file, this data is fetched and displayed securely on the browser. You need to set up file viewing in Oracle Clinical so that users can:

- View report outputs and log files
- View some log files from Parameterized Submission (PSUB) batch jobs
- View HTML previews of DCI Forms Layout definitions

For more information, see the *Oracle Clinical Administrator's Guide*.

4.1.3 Grant the Right to Run Jobs

Users who need to submit PSUB jobs must have the OCPSUB account as a proxy database account for PSUB jobs.

The password for the OCPSUB database account is stored in Oracle Wallet.

For more information, see the *Oracle Clinical Administrator's Guide*.

4.1.4 Secure SAS Setup

Oracle Clinical supports extracting Oracle and SAS views of clinical patient data. SAS is optional and must be purchased separately.

To grant a user access to the data extracts:

- Add the opapps system account to the oclsascr user group to give the user access to the RXC_SAS_VIEW and SAS_OUTPUT_ROOT directory structures. This account executes the SAS jobs. Individual users should not be provided with operating system accounts at all.
- Decide on and configure the method to authenticate the SAS connection to the database. For more information, see the *Oracle Clinical Installation Guide*.

For more information, see the *Oracle Clinical Administrator's Guide*.

4.1.5 Restricted Viewing of Personal/Protected Health Information (PHI)

Assign privileges to access specific studies and database roles restricting access to specific menu items. Access to menus determines whether you have browse, update, or no access to patient data. It also determines which types of jobs and reports you are able to run.

4.2 Secure the Reports Server

See My Oracle Support note *Secure the Showjobs Web Command in a Non Secured Reports Server in Oracle Reports 11g*, ID 1242614.1.

4.3 RDC Onsite Security

This section provides information for securing the RDC Onsite application, users, and data.

4.3.1 Restrict Access to the Application

Use the following security features to ensure that users can access only the parts of the application that they need to do their jobs.

- **Assign study and site privileges:** To restrict user access to RDC Onsite study and site data, you can define and maintain users' study and site privileges. You must explicitly give users access to study data, either by granting them Superuser status, which allows access to all studies, or explicitly granting access to specific studies or groups of studies (programs and projects). Within each study, you can restrict access to patients assigned to specific sites. For more information, see the *Oracle Clinical Remote Data Capture Onsite Administrator's Guide*.
- **Restrict access to types of CRFs (Data Collection Instruments):** RDC Onsite includes a predefined set of user roles. By default, these roles have UNRESTRICTED access to all DCIs. You can change the default access for any role to RESTRICTED, and then further define which DCIs within the user's study/site access can be accessed by that user's role. For more information, see the *Oracle Clinical Administrator's Guide*.
- **Grant Oracle Clinical users access to RDC Onsite:** A user who has access to a study in Oracle Clinical does not automatically have access to that study in RDC Onsite unless you use the Study Security form in the RDC Administration application to assign specific privileges to the user. For more information, see the *Oracle Clinical Remote Data Capture Onsite Administrator's Guide*.

4.3.2 Grant Functional Privileges at the Study and Site Level

You can control users' ability to do the following by study and site:

- Update CRF data or just CRF discrepancies.
- Verify CRFs.
- Approve CRFs.
- Update Source Data Verification Plans for sites.
- Update CRF status for custom review types.
- Browse CRFs.

- Browse CRF verification or custom review status.

For more information, see the *Oracle Clinical Remote Data Capture Onsite Administrator's Guide*.

4.3.3 Manage Security with Data Entry Configuration Settings

In RDC Onsite, data entry configuration settings allow you to do the following:

- Resolve discrepancies at the time the discrepancy is raised.
- Perform privileged update of locked CRFs.

See the *Oracle Clinical Remote Data Capture Onsite Administrator's Guide* for more information.

4.3.4 Check External Links that May Expose Account Data

In RDC Onsite, you can add customized links to the Home page, the Patient Summary Report page, and the CRF Help icon. Any information that can be made available through a URL can be made accessible to RDC Onsite users.

In addition, your customized links support passing session parameters, such as login user ID and user role, to a URL. By passing these session parameters, you can create target Web pages that switch the content according to the user login ID, user role, study, and site. You can create links that access Web sites relevant to your clinical trial or that relate to your use of the RDC Onsite application.

However, be aware that in some situations, like links that access external Web sites, passing account data and session information may pose a security risk. In these cases, you can define the link to pass no session parameters to the URL.

For details on configuring links, refer to the *Oracle Clinical Remote Data Capture Onsite Administrator's Guide*.

4.3.5 Enforce Password Security

Each password should meet or exceed the minimum requirements for the application. For example, a password may need to:

- Contain a minimum of eight characters.
- Contain at least one upper case character, and one alphanumeric character.

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

Oracle enables a database administrator to enforce various rules about passwords at the database level, including setting a password lifetime, after which users must set a new password; disallowing reuse of previous passwords; locking an account after a user attempts to log on a specified number of times; and creating complexity rules for passwords through a PL/SQL function. For more information, see the *Oracle Clinical Administrator's Guide*.

4.3.6 Restrict Actions Against Locked CRFs

If you lock a CRF, by default, RDC Onsite restricts access to the locked CRF. Even if you chang the restriction access, users can work with a locked CRF only if they have the proper privileges.

For more information, see the *Oracle Clinical Remote Data Capture Onsite Administrator's Guide*.

4.3.7 Profiles

In RDC Onsite, a profile is a named set of resource limits and password parameters that restrict database usage and instance resources for a user. By default, every RDC user is assigned the DEFAULT profile, which has no limitations on resources or password use. You can assign a separate profile to each user or user role by which passwords are validated. Each user can have only one profile, and creating a new one supersedes any earlier one.

For more information, see the *Oracle Clinical Administrator's Guide*.

4.3.8 Restricted Viewing of Personal/Protected Health Information (PHI)

You use the roles and privileges in RDC Onsite to restrict the users who can view and enter PHI. With study and site privileges, you restrict access to data for patients assigned to a particular site. Further, you define the type of access a user has to that patient data: browse, update, verify, or approve.

4.4 TMS Security

This section provides information for securing the TMS application, users, and data.

4.4.1 Use Data Access Groups to Restrict Access to the Application

In TMS, database roles dictate which windows in the user interface a user can access. For users assigned to one or more Data Access Groups (DAGs), their assignments dictate the data they see in TMS windows and in the HTML Browser, and whether or not they can operate on TMS data in specific dictionaries and/or domains. You define DAGs in the Maintain DAGs window and then assign users to the group either in the User Assignments tab of the Maintain DAGs window or as you create user accounts. For more information, see the *Oracle Thesaurus Management System User's Guide*.

4.4.2 Enforce Password Security

Each password should meet or exceed the minimum requirements for the application. For example, a password may need to:

- Contain a minimum of eight characters.
- Contain at least one upper case character, and one alphanumeric character.

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

Oracle enables a database administrator to enforce various rules about passwords at the database level, including setting a password lifetime, after which users must set a new password; disallowing reuse of previous passwords; locking an account after a user attempts to log on a specified number of times; and creating complexity rules for passwords through a PL/SQL function. For more information, see the *Oracle Clinical Administrator's Guide*.

4.4.3 Database Roles and Menu-Based Security

TMS includes predefined roles that you can assign to users. A predefined role determines the functions and menu options that are available to a user.

You can enforce security by assigning users only the database roles they need to do their work, preventing them from seeing other parts of the system and taking actions they are not authorized to take.

You can also create custom database roles, which may be required if the database roles that are supplied as part of the installation do not fit or cannot be modified to fit your business model.

For more information, see the *Oracle Thesaurus Mangement System User's Guide*.

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 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.

Oracle Clinical, Oracle Clinical Remote Data Capture, and Oracle Thesaurus Management System Security Configuration Guide, Release 5.1
E53566-02