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

Security Configuration Guide

Release 4.6.2

E24464-01

July 2011

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

- Oracle Clinical 4.6.2
- Oracle Clinical Remote Data Capture Onsite 4.6.2 (RDC Onsite)
- Oracle Clinical Remote Data Capture Classic 4.6.2 (RDC Classic)
- Oracle Thesaurus Management System 4.6.2 (TMS)

1 Introduction

This guide presents the following security guidelines and recommendations:

- Configuring Strong Passwords on the Database
- Closing All Open Ports Not in Use
- Disabling the Telnet Service
- Disabling Other Unused Services
- Replacing Verbose Errors with Custom Messages
- Deleting or Disabling Demos
- Hiding Sensitive Information on the Apache Server
- Checking External Links that May Expose Account Data
- Providing Security for Session-Tracking Cookies
- Disabling Cross-site Tracing
- Change Record
- Documentation Accessibility

2 Configuring 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. 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.

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.

3 Closing All Open Ports Not in Use

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

4 Disabling the Telnet Service

The Oracle Clinical, RDC Onsite, and TMS applications do not use the Telnet service. Telnet listens on port 23 by default.

If the Telnet service is available on the Oracle Clinical host machine, Oracle recommends that you disable Telnet in favor of Secure Shell (ssh). Telnet, which sends clear-text passwords and user names through logins, is a security risk to your servers. Disabling Telnet tightens and protects your system security.

5 Disabling Other Unused Services

In addition to not using Telnet, 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.

6 Replacing 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

6.1 Creating the HTML Error Page

You need to design and create the customized HTML error pages that you specify in the web.xml file. For example, for error 500, you can create a 500error.html page with the following lines of code:

```
<HTML>
  <HEAD>
    <TITLE> HTML Error Page </TITLE>
  </HEAD>
  <BODY>
  <P>An internal server error occurred. Contact the administrator.</P>
  </BODY>
</HTML>
```

After you create your customized HTML error page, place the page in the appropriate directories as follows:

- **For the RDC Onsite application:** *ORACLE_AS10gR3_HOME*\j2ee\rdc\applications\olsardc\rdconsite
- **For the OPA Administration utility:** *ORACLE_AS10gR3_HOME*\j2ee\opa\applications\opaadmin\opaadmin
- **For the TMS application:** *ORACLE_AS10gR3_HOME*\j2ee\opa\applications\tms\tmsuix

6.2 Editing the web.xml File

After you can create an HTML error page containing your customized message, you must edit the web.xml file to specify the error numbers and the HTML error page to display for that error. 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 modify the web.xml file for each instance of RDC Onsite, OPA Administration, and TMS in your installation.

To edit the web.xml file and specify your customized error pages:

1. Log in to Oracle Enterprise Manager 10g Application Server Control.
2. Stop the appropriate instance:
   - **For RDC Onsite:** Stop the rdc OC4J instance.
   - **For OPA Administration:** Stop the OPA OC4J instance.
   - **For TMS:** Stop the OPA OC4J instance.
3. Log in to the application server computer.
4. Navigate to the appropriate WEB-INF directory depending on which web.xml file you are modifying:
   - **For RDC Onsite:**

     ORACLE_AS10gR3_HOME\j2ee\rdc\applications\olsardc\rdconsite\WEB-INF
   - **For OPA Administration:**

     ORACLE_AS10gR3_HOME\j2ee\opa\applications\opaadmin\opaadmin\WEB-INF
   - **For TMS:**

     ORACLE_AS10gR3_HOME\j2ee\opa\applications\tms\tmsuix\WEB-INF
5. Open the **web.xml** file with a text editor.
6. Add the following lines to the file:

   ```
   <error-page>
       <error-code>number</error-code>
       <location>/file-name.html</location>
   </error-page>
   ```

   Where *number* is the HTTP error code and *file-name* is the name of the HTML page you created for the error. For example:

   ```
   <error-page>
       <error-code>500</error-code>
       <location>/500error.html</location>
   </error-page>
   ```

   > **Note:** If you installed the Oracle Thesaurus Management System patch TMS_4.6.1.6, the patch automatically adds the <error-page> entry to the TMS web.xml file. You need to edit the lines and replace the default information with the error number and the corresponding custom HTML error page that you created.

7. Save your changes.
8. Restart the appropriate instance.

7 Deleting or Disabling Demos

Oracle Application Server ships with several demos, which are available on the Demonstrations tab on the Welcome page. Demos are available for configured components only. You should not make these demos available in a production environment because some demos contain system default information that others can use to gain unauthorized access to your system.

The sample Oracle Clinical demos execute the following scripts and display the client's environment settings:

- echo.exe
- echo2.exe

To secure the Oracle application server, Oracle recommends that you:

1. Apply the latest available CPU patch for the application server.
2. Delete the following executable files:

   ORACLE_HOME\Apache\Apache\fcgi-bin\echo.exe

   ORACLE_HOME\Apache\Apache\fcgi-bin\echo2.exe

   Alternatively, you can disable the demos by moving the echo.exe and echo2.exe files from the *ORACLE_HOME*\Apache\Apache\fcgi-bin directory to another protected directory.
3. Navigate to the htdocs directory.
4. Move all the files in the htdocs directory to another protected directory so no one can access.

8 Hiding Sensitive Information on the Apache Server

By default, many Apache installations expose the following sensitive information:

- The Apache version currently running
- The operating system and version currently running
- The names of the Apache modules installed on the server

Attackers can use this information to their advantage when performing an attack. In addition, it sends the message that you did not modify the default values or behavior.

To hide sensitive information on the Apache server, you need to add or edit the following lines in the httpd.conf file:

```
ServerSignature Off
ServerTokens Prod
ExtendedStatus Off
```

9 Checking 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*.

10 Providing Security for Session-Tracking Cookies

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

10.1 Configuring the Secure and HttpOnly Flags

To configure the secure and HttpOnly flags for session-tracking cookies:

1. Navigate to the appropriate directory on Oracle Application Server 10*g* Release 3 depending on whether you are configuring the session-tracking cookie for the RDC Onsite application or the TMS application.

   - **For RDC Onsite:**

     ORACLE_AS10gR3_HOME\j2ee\rdc\application-deployments\olsardc\rdconsite

   - **For TMS:**

     ORACLE_AS10gR3_HOME\j2ee\opa\application-deployments\tms\tmsUix

   > **Note:** Make sure you navigate to the correct directory. On Oracle Application Server 10*g* Release 3, the orion-web.xml file is also located in the following directory:
   >
   > *ORACLE_AS10gR3_HOME*\j2ee\rdc\applications\rdconsite\rdconsite\WEB-INF
   >
   > However, modifying this version of the orion-web.xml file does not enable the secure and HttpOnly flags.

2. Back up the **orion-web.xml** file.
3. Open the original **orion-web.xml** file with a text editor.
4. Add the **session-tracking** element to the file. For example:

```
<session-tracking set-secure="true"
cookie-domain="domain-name;HttpOnly" />
```

where:

domain_name is the domain name of the server to which the user connects (that is, the URL domain that users specify in their browser). For example:

sys63.mycompany.com

Note that the server may not be the actual server you are working on, but may be the proxy server or the load balancer that you connect to in order to access this server. Note also that you must make these changes on all servers in a load-balanced environment.

5. Save your changes.
6. Restart the appropriate instance.
   - **For RDC Onsite:** Restart the rdc OC4J instance.
   - **For TMS:** Restart the OPA OC4J instance.

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

10.2 Confirming the Secure and HttpOnly Flags Are Configured Properly

You can confirm that the secure and HttpOnly flags are configured properly and verify the system behavior by inspecting the Set-Cookie headers that are passed from the Oracle Application Server 10*g* Release 3 to the client.

To confirm that you configured the secure and HttpOnly flags properly:

1. Open a standard *HTTP Traffic Tracking* utility. Many HTTP Traffic Tracking utilities are available for download from the World Wide Web. You can download and install the utility if you do not have one available on your system.
2. Use your *HTTP Traffic Tracking* utility to start the RDC Onsite application.

   On the RDC Onsite Login page, verify that the utility reports that the secure and HttpOnly flags are enabled. For example:

   ```
   Set-Cookie:
   JSESSIONID=ab2418b1fbb64b646d4cc23877268f8938200949de1019683f2b3f4a1a2f603c.e3
   8Oa3aQaxiOai0LbhaRbx0Tb30Pe0; domain=sys63.mycompany.com; path=/olsa/oc;
   secure; HttpOnly
   ```

11 Disabling Cross-site Tracing

To disable cross-site tracing:

1. Navigate to the following directory on Oracle Application Server 10*g* Release 2:

   ORACLE_AS10gR2_HOME\Apache\Apache\conf
2. Open the **httpd.conf** file with a text editor.
3. Add the following lines to the file:

   ```
   LoadModule rewrite_module modules/ApacheModuleRewrite.dll
   AddModule mod_rewrite.c
   ```

4. Add the following lines if not already present in the file:

```
RewriteEngine On
RewriteCond %{REQUEST_METHOD} ^TRACE
RewriteRule .* - [F]
RewriteCond %{REQUEST_METHOD} ^TRACK
RewriteRule .* - [F]
RewriteCond %{REQUEST_METHOD} ^PUT
RewriteRule .* - [F]
RewriteCond %{REQUEST_METHOD} ^DELETE
RewriteRule .* - [F]
RewriteCond %{REQUEST_METHOD} ^CONNECT
RewriteRule .* - [F]
RewriteCond %{REQUEST_METHOD} ^PATCH
RewriteRule .* - [F]
RewriteCond %{REQUEST_METHOD} ^PROPFIND
RewriteRule .* - [F]
RewriteCond %{REQUEST_METHOD} ^PROPPATCH
RewriteRule .* - [F]
RewriteCond %{REQUEST_METHOD} ^MKCOL
RewriteRule .* - [F]
RewriteCond %{REQUEST_METHOD} ^COPY
RewriteRule .* - [F]
RewriteCond %{REQUEST_METHOD} ^MOVE
RewriteRule .* - [F]
RewriteCond %{REQUEST_METHOD} ^LOCK
RewriteRule .* - [F]
RewriteCond %{REQUEST_METHOD} ^UNLOCK
RewriteRule .* - [F]
```

5. Save your changes.
6. Restart the HTTP server for your changes to take effect.

Note: These settings apply only to Oracle Application Server 10*g* Release 2. They do not affect Oracle Application Server 10*g* Release 3.

12 Change Record

April 2011: Original publication of this document

July 2011: Add part number and release on www.oracle.com; changed title and introduction to reflect applicability to RDC Classic as well as RDC Onsite; no content changes.

13 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 Clinical, Oracle Clinical Remote Data Capture, and Oracle Thesaurus Management System Security Configuration Guide, Release 4.6.2
E24464-01