Oracle® Health Sciences Clinical Development Analytics

Security Guide

Release 3.1.1

E63314-01

May 2015

This document provides the security guidelines that must be followed to use the Oracle Health Sciences Clinical Development Analytics (OHSCDA) application. It includes the following sections:

1 General Security Principles

The following principles are fundamental to using any application securely.

1.1 Keeping Software Up To Date

One of the principles of good security practice is to keep all software versions and patches up to date.

1.2 Keeping Up To Date on Latest Security Information Critical Patch Updates

Oracle continually improves its software and documentation. Critical Patch Updates are the primary means of releasing security fixes for Oracle products to customers with valid support contracts. They are released on the Tuesday closest to the 17th day of January, April, July and October. We highly recommend customers apply these patches as soon as they are released.

1.3 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 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® WebLogic Portal Security Guide* specific to the database release you are using.

ORACLE®

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 RXI.

- The password for the database listener. Oracle recommends that you do not configure a password for the database listener as that will enable remote administration. For more information, refer to *Oracle® Database Net Services Reference 11g Release 2 (11.2)*.

1.4 Following the Principle of Least Privilege

The principle of least privilege states that users should be given the least amount of privilege to perform their jobs. Overly ambitious granting of responsibilities, roles, grants — especially early on in an organization's life cycle when people are few and work needs to be done quickly — often leaves a system wide open for abuse. User privileges should be reviewed periodically to determine relevance to current job responsibilities.

1.5 Managing Default User Accounts

Lock and expire default user accounts.

1.6 Closing All Open Ports Not in Use

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

1.7 Disabling the Telnet Service

Oracle Health Sciences Clinical Development Analytics Standard Configuration does not use the Telnet service.

Telnet listens on port 23 by default.

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

1.8 Disabling Other Unused Services

In addition to not using Telnet, the Oracle Health Sciences Clinical Development Analytics Standard Configuration does 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 a method for managing and reporting information about different systems.

Restricting these services or information does not affect the use of Oracle Health Sciences Clinical Development Analytics Standard Configuration. 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.

1.9 Designing for Multiple Layers of Protection

When designing a secure deployment, design multiple layers of protection. If a hacker should gain access to one layer, such as the application server, that should not automatically give them easy access to other layers, such as the database server.

Providing multiple layers of protection may include:

- Enable only those ports required for communication between different tiers, for example, only allowing communication to the database tier on the port used for SQL*NET communications (1521 by default).

- Place firewalls between servers so that only expected traffic can move between servers.

1.10 Enabling SSL

Due to the complexity in setting up SSL, it is not enabled by default during installation. Communications between the browser and the application servers should be restricted to SSL. See the Oracle WebLogic Server 11g guidelines for instructions on enabling SSL.

You must start the Oracle WebLogic Server with a parameter to exclude SSL 2.0 and/or SSL 3.0 to in order to mitigate the SSL V3.0 "Poodle" Vulnerability, CVE-2014-3566. For more information, see *How to Change SSL Protocols (to Disable SSL 3.0) in Oracle Fusion Middleware Products* (Doc ID 1936300.1) on My Oracle Support (https://support.oracle.com)

2 Protected Health Information

OHSCDA contains the following subject data that are used for both out of the box reports and/or available for use in ad hoc queries:

- Date of Birth

- Initials

- Subject ID (concatenation of initials and date of birth)

- Screening # (concatenation of initials and date of birth)

If you have concerns over these data, you have several options available. You can configure the source systems to not use initials and data of birth in Subject ID and Screening # measures. Additionally, you can remove the Data of Birth and Initials measures from the presentation in OHSCDA as these are not used in any out of the box reports.

2.1 Removing PHI Measures

You can configure the OHSCDA repository to remove measures that contain PHI data. Refer to OBIEE documentation for full instructions on configuring the RPD.

1. Open the RPD in the OBIEE Administration tool.

2. Delete the following measures from the Subject folder in the presentation layer:

- Date of Birth

- Initials

- Subject ID (concatenation of initials and date of birth)

- Screening # (concatenation of initials and date of birth)

3. Deploy the updated RPD on the OBIEE server.

2.2 Exporting Data

OHSCDA out of the box utilizes native OBIEE export functionality. You can export any report into PDF, Excel, Powerpoint, web archive (.mht), csv, tab delimited, or xml.

If you have concerns over exporting data, you have several options available. You can modify the dashboard properties and remove the export link at the bottom of reports. You can also enable the OBIEE's Usage Tracking option. This option tracks which queries were run by which users and when.

3 Security Guidelines for Oracle Business Intelligence Enterprise Edition

While installing and configuring the OBIEE Server, you should follow guidelines in the document *Oracle® Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition 11g Release 1 (11.1.1)Part Number E10543-02.*

3.1 Checking External Links that May Expose Account Data

It is possible to add customized links to web applications that are deployed in a web server. Through this mechanism, any information that can be made available through a URL can be made accessible to OHSCDA users. In addition, your customized links may support passing session parameters, such as the log-in user ID, and currently selected Product, Program, Study and Site to a URL. By passing these session parameters, you can access Web pages specific to you current selections on these attributes. However, you should be aware that in links that access external Web sites, passing account data and session information may pose a security risk.

3.2 Managing Usage Tracking

For information, see *Oracle® Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition.*

4 Setting up Transparent Data Encryption Tablespace

To set up the transparent data encryption tablespace, perform the following configuration steps:

1. Create a wallet by executing the following syntax at the command line.

```
mkstore -wrl <wallet_location> -create
```

> **Note:** `<wallet_location>` is the directory where you want to create and store the wallet.

The command will prompt for the wallet password twice. Enter the same password and note down the password as it will used later.

2. Update the sqlnet.ora file.

    a. Navigate to $ORACLE_HOME\NETWORK\ADMIN.

    b. Update the sqlnet.ora file for ENCRYPTION_WALLET_LOCATION.

    For example,

    ```
    ENCRYPTION_WALLET_LOCATION=
        (SOURCE=(METHOD=FILE)(METHOD_DATA=
            (DIRECTORY=<wallet location>)))
    ```

3. Create a wallet key and open the wallet in the database.

    ```
    ALTER SYSTEM SET ENCRYPTION KEY IDENTIFIED BY "<password>";
    ```

    > **Note:** You must enter the same password used in step 1.

4. Create an encrypted tablespace. Run the following command:

    ```
    CREATE TABLESPACE <tablespace name>
    DATAFILE '<data file location>' SIZE 500M
    AUTOEXTEND ON NEXT 1m
    ENCRYPTION USING 'AES256'
    DEFAULT STORAGE (ENCRYPT);
    ```

5. Create a schema and grant access to the encrypted tablespace.

    To create user or schema, run the following command:

    ```
    Create user <username> identified by <user_password>;
    ```
    To grant user access, execute the following command:

    ```
    Grant connect, resource to <username>;
    ```
    To grant tablespace quota, execute the following command.

    ```
    ALTER USER <username> QUOTA UNLIMITED ON <tablespace name>;
    ```

5 Configuring SSO for OHSCDA OBIEE Using Oracle Access Manager 11g

This section describes the steps to configure SSO in Oracle Access Manager (OAM) 11g.

5.1 Prerequisites

The following are the prerequisites:

- OAM 11g installation must be configured to work with the desired LDAP.

    (For example, OUD), as the identity data-store.

- User profiles must exist in the LDAP server as well as in the Argus Safety with the same credentials.

- Oracle Web Tier 11.1.1.3 (or higher) must be installed on the same server where the OBIEE server is installed and configured with the WebLogic Server hosting OBIEE.

- Oracle Webgate 11g must be installed on the same server where the OBIEE server is installed.

5.2 Installing SSO on OAM 11g

To install SSO on OAM 11g, perform the following steps:

1. Navigate to the OAM 11g OAM Console URL (http://oam_server:port/oamconsole) and log in with the OAM Admin credentials.

2. Select the **System Configuration** tab.

3. Select the **Access Manager Settings** submenu in the left navigation window of the browser.

4. Double-click **SSO Agents** and select the **OAM Agents** option to open the **OAM Agents** sub window.

5. Click **Create 11g Webgate** and enter the following details:

   - Specify the name for the OHSCDA Policy.

   - In the **Security** field, select the **Open** option.

   - Enter the host identifier. For example, <obiee_server>.

     > **Note:** The <obiee_server> refers to the server where the OBIEE 11g is installed along with Oracle Web Tier and Oracle Webgate.

   - Select the **Auto Create Policies** option.

6. Click **Apply** to save and register the 11g Webgate and policies with OAM.

7. On the subsequent page, update the details for the OHSCDA policy created in step 5.

   - **Cache Pragma Header**: Private

   - **Cache Control Header**: Private

8. Click **Apply**.

9. Navigate to the **Policy Configuration** tab.

10. Expand and double-click **Shared Components > Resource Type > Host Identifiers > <obiee_server>** (for example, server.domain.com) to open the **Host Identifiers** window and add the following details:

    - <obiee_server>
    - <obiee_server> <port>
    - <obiee_server_ip>
    - <obiee_server_ip> <port>

      > **Note:** <obiee_server> refers to the server where the OBIEE 11g is installed along with Oracle Web Tier and Oracle Webgate. The port refers to the Oracle Web Tier Port.

11. Expand and double-click **Application Domains > <OHSCDA Policy> > Authentication Policies > Protected Resource Policy**.

12. Ensure that the Authentication Scheme is set as **LDAPScheme**.

13. Ensure that the following resources are present:

- /
- /…/*

14. Add the following response variables:

- **Name**: OAM_REMOTE_USER
- **Type**: Header
- **Value**: $user.attr.uid [based on the LDAP schema setup]

15. Click **Apply** and save the changes.

16. Expand and double-click **Application Domains > <OHSCDA Policy> > Authorization Policies > Protected Resource Policy**

17. Ensure that the following resources are present:

- /
- /…/*

18. Add the following response variables:

- **Name**: OAM_REMOTE_USER
- **Type**: Header
- **Value**: $user.attr.uid [based on the LDAP schema setup]

19. Click **Apply** to save the changes.

20. Navigate to the OHSCDA Web Tier Machine [<obiee_server>], where the OHSCDA OBIEE server is installed.

21. Run the installer for Webgate (OFM Webgate 11g for OAM 11g) to complete the installation.

22. Configure the 11g Webgate using the following steps to communicate with the OAM 11g server:

> **Note:** For more information, see *Oracle® Fusion Middleware Installation Guide for Oracle Identity Management*
>
> *11g Release 1 (11.1.1).*

a. Move to the following directory under your Oracle Home for Webgate:

On UNIX Operating Systems:

```
<Webgate_Home>/webgate/ohs/tools/deployWebGate
```

On Windows Operating Systems:

```
<Webgate_Home>\webgate\ohs\tools\deployWebGate
```

b. On the command line, run the following command to copy the required bits of agent from the **Webgate_Home** directory to the Webgate Instance location:

On UNIX Operating Systems:

```
./deployWebgateInstance.sh -w <Webgate_Instance_Directory> -oh
<Webgate_Oracle_Home>
```

On Windows Operating Systems:

```
deployWebgateInstance.bat -w <Webgate_Instance_Directory> -oh
<Webgate_Oracle_Home>
```

where, `<Webgate_Oracle_Home>` is the directory where you have installed
Oracle HTTP Server Webgate and created as the Oracle Home for Webgate, as
shown in the following example:

```
MW_HOME>/Oracle_OAMWebGate1
```

The `<Webgate_Instance_Directory>` is the location of Webgate instance home,
which is the same as the instance home of Oracle HTTP Server, as shown in
the following example:

```
<MW_HOME>/Oracle_WT1/instances/instance2/config/OHS/ohs1
```

c. Run the following command to ensure that the **LD_LIBRARY_PATH** variable
contains <Oracle_Home_for_Oracle_HTTP_Server>/lib:

On UNIX (depending on the shell):

```
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:<Oracle_Home_for_Oracle_
HTTP_Server>/lib
```

On Windows:

Set the `<Webgate_Installation_Directory>\webgate\ohs\lib` location and
the `<Oracle_Home_for_Oracle_HTTP_Server>\bin` location in the PATH
environment variable.

Add a semicolon (;) followed by this path at the end of the entry for the PATH
environment variable.

d. From your current working directory, move up one directory level:

On UNIX Operating Systems, move to:

```
<Webgate_Home>/webgate/ohs/tools/setup/InstallTools
```

On Windows Operating Systems, move to:

```
<Webgate_Home>\webgate\ohs\tools\EditHttpConf
```

e. On the command line, run the following command to copy the **apache_
webgate.template** from the **Webgate_Home** directory to the Webgate instance
location (renamed to webgate.conf) and update the **httpd.conf** file to add one
line to include the name of **webgate.conf**:

On UNIX operating systems:

```
./EditHttpConf -w <Webgate_Instance_Directory> -oh <Webgate_Oracle_
Home> -o <output_file>
```

On Windows operating systems:

```
EditHttpConf.exe -w <Webgate_Instance_Directory> -oh <Webgate_
Oracle_Home> -o <output_file>
```

where, `<Webgate_Oracle_Home>` is the directory where Oracle HTTP Server Webgate is installed for Oracle Access Manager and created as the Oracle Home for Webgate, as shown in the following example:

`<MW_HOME>/Oracle_OAMWebGate1`

The `<Webgate_Instance_Directory>` is the location of Webgate instance home, which is the same as the instance home of Oracle HTTP Server, as shown in the following example:

`<MW_HOME>/Oracle_WT1/instances/instance2/config/OHS/ohs1`

The `<output_file>` is the name of the temporary output file used by the tool, as shown in the following example:

`Edithttpconf.log`

f. Copy Generated Files (Artifacts) to the Webgate Instance Location from the OAM 11g server.

The 11g Webgate Agent (<OHSCDA Policy>), which was created in the OAM 11g OAM Console, would have also created the following artifacts on the OAM 11g server:

- cwallet.sso

- ObAccessClient.xml

This is based on the Security Mode that you have configured, which in this case is **Open**.

On the OAM 11g server, these files are present at the following location:

`<OAM_FMW_HOME>/user_projects/domains/<OAM_domain>/output/<OHSCDA Policy>`

23. Copy these files to the <obiee_server> in the following directory:

`<Webgate_Instance_Directory>/webgate/config` directory

For example, `<MW_HOME>/Oracle_ WT1/instances/instance2/config/OHS/ohs1/webgate/config`.

24. Restart the Oracle HTTP Server instance.

To stop the Oracle HTTP Server instance, run the following commands on the command line:

`<MW_HOME>/Oracle_WT1/instances/instance2/bin/opmnctl stopall`

To restart the Oracle HTTP Server instance, run the following commands on the command line:

`<MW_HOME>/Oracle_WT1/instances/instance2/bin/opmnctl startall`

25. Configure the HTTP Server as a reverse proxy for the WebLogic Server. To execute this, modify the **mod_wl_ohs.conf** file present at the following location:

`OracleWebTierHome\instances\instance2\config\OHS\ohs1`

The following is a template to configure **mod_weblogic**:

LoadModule weblogic_module "${ORACLE_HOME}/ohs/modules/mod_wl_ ohs.so"

This empty block is needed to save mod_wl related configuration from EM to this file when changes are made at the base virtual host level:

```
<IfModule weblogic_module>
# WebLogicHost <WEBLOGIC_HOST>
# WebLogicPort <WEBLOGIC_PORT>
# Debug ON
# WLLogFile /tmp/weblogic.log
# MatchExpression *.jsp

<Location /console>
SetHandler weblogic-handler
WebLogicHost <WebLogic host name>
WeblogicPort <WebLogic port number
WLProxySSL ON
WLProxySSLPassThrough ON
</Location>

<Location /em>
SetHandler weblogic-handler
WebLogicHost <WebLogic host name>
WeblogicPort <WebLogic port number
WLProxySSL ON
WLProxySSLPassThrough ON
</Location>

<Location /analytics>
SetHandler weblogic-handler
WebLogicHost <WebLogic host name>
WeblogicPort <OBIEE Analytics Port>
WLProxySSL ON
WLProxySSLPassThrough ON
</Location>

<Location /analyticsRes>
SetHandler weblogic-handler
WebLogicHost <WebLogic host name>
WeblogicPort <OBIEE Analytics Port>
WLProxySSL ON
WLProxySSLPassThrough ON
</Location>

<Location /xmlpserver>
SetHandler weblogic-handler
WebLogicHost <WebLogic host name>
WeblogicPort <OBIEE Analytics Port>
WLProxySSL ON
WLProxySSLPassThrough ON
</Location>

</IfModule>
# <Location /weblogic>
# SetHandler weblogic-handler
# PathTrim /weblogic
# ErrorPage http:/WEBLOGIC_HOME:WEBLOGIC_PORT/
# </Location>
```

26. Restart the Web Tier Instance in WebLogic EM or as described in step 23.

27. Configure a new authenticator for Oracle WebLogic Server on the OBIEE server using the following steps:

    a. Login to the WebLogic Server Administrator Console and navigate to **Security Realms > myrealm**.

b. Click the **Providers** tab.

c. Click **Lock & Edit** on the right corner of the webpage, highlighted as Change Center.

d. Click **New** to create a new authentication provider and add the following details:

Name: A name of your choice <Name>

Type: OracleInternetDirectoryAuthenticator

e. After saving the details, click the new authenticator that you have created, and enter the following details:

In the sub tab, change the Control Flag as **SUFFICIENT**

f. Click **Save**.

g. Click the **Provider Specific** tab and enter the following settings required using values for your environment:

- **Host**: Your LDAP host.

- **Port**: Your LDAP host listening port.

- **Principal**: LDAP administrative user.

For example, cn=Directory Manager

- **Credential**: LDAP administrative user password.

- **User Base DN**: Same search base as in Oracle Access Manager.

For example, dc=us, dc=oracle, dc=com

- **All Users Filter**:

For example, (&(uid=*) (objectclass=person))

- **User Name Attribute**: Set as the default attribute for username in the directory server.

For example, uid

- **Group Base DN**: The group search base.

For example: dc=us, dc=oracle, dc=com

- **All Groups Filter**:

For example, (&(cn=*)(|(objectclass=groupofUniqueNames)(objectclass=groupOfURLs)))

- **Group From Name Filter**:

For example, (|(&(cn=%g)(objectclass=groupofUniqueNames))(&(cn=%g)(objectclass=groupOfURLs)))

- **Static Group Name Attribute**:

For example, cn

- **Static Group Object Class**:

For example, groupofuniquenames

- **Static Member DN Attribute**:

For example, uniquemember

- **Static Group DNs from Member DN Filter**:

For example, (&(uniquemember=%M)(objectclass=groupofuniquenames))

- **Dynamic Group Name Attribute**:

For example, cn

- **Dynamic Group Object Class**:

For example, groupOfURLs

- **User Dynamic Group DN Attribute**:

For example, uniquemember

- Leave the other defaults as is.

- **GUID Attribute**: The GUID attribute defined in the OUD LDAP Server

For example, uid

   h.   Click **Save**.

28. Configure a new Identity Asserter for WebLogic Server using the following steps:

   a.   In the Oracle WebLogic Server Administration Console, select **Security Realms** from the left pane and click the realm which you want to configure.

For example, myrealm.

   b.   Select **Providers**.

   c.   Click **New** and enter the following values in the fields:

Name: <Name>OAMIdentityAsserter or a name of your choice

Type: OAMIdentityAsserter

   d.   Click **OK**.

   e.   Click on the newly created asserter and set the Control Flag to **REQUIRED**.

   f.   Ensure that the Active Types that you have selected is **OAM_REMOTE_ USER**.

   g.   Click **Save**.

   h.   Navigate to the **Provider Specific** tab and enter the following details:

- **Transport Security**: open

- **Application Domain**: <Name>, as set in the OAM 11g Console

- **Access Gate Name**: <Name>, as specified in the OAM 11g Console

- **Primary Access Server**: <Name>:<Port>, OAM 11g server with port

   i.   Click **Save**.

   j.   In the **Providers** tab, perform the following steps to reorder providers:

i. Click **Reorder**.

ii. On the **Reorder Authentication Providers** page, select a provider name and use the arrows to order the following providers:

- <Name>OAMIdentityAsserter

- OCDAAuthenticator

- DefaultAuthenticator

- DefaultIdentityAsserter

iii. Click **OK** to save your changes.

k. In the **Providers** tab, click **Default Authenticator** and change the Control Flag to **Sufficient**.

l. In the Change Center, click **Activate Changes**.

m. Restart Oracle WebLogic Server

29. Delete the **BISystemUser** present in the default embedded LDAP (using Security Realms in the **Administration Console** Link of the WebLogic Server) and add the same or another user in the newly added OID.

You must add this user to the BI Application Roles using the following steps:

a. Navigate to **Administration Console > Security Realms > myrealm > Users and Groups > Users** and select the **BISystemUser** check box (from Provider: Default Authenticator).

b. Click **Delete**.

c. Navigate to **Security Realms > myrealm > Roles and Policies > Realm Roles**.

d. In the tree structure, expand **Global Roles** node and select the **Roles** link.

e. In the subsequent screen, click the **Admin Role** link.

f. Click **Add Conditions**.

g. In the next screen, select the Predicate List as **User** and click **Next**.

h. In the **User Argument Name**, enter **BISystemUser** and click **ADD**.

i. Click **Finish**.

j. In the **Role Conditions** screen, ensure that the set operator is set to **Or**.

k. Save the configuration.

l. Navigate to the Enterprise Manager of OBIEE or the Fusion Middleware Control page and navigate in the tree structure to the **Business Intelligence > coreapplication** node.

m. In the Business Intelligence drop-down menu, select **Security > Application > Roles**.

n. In the Roles displayed, select **BISystem**, and in the next screen remove the old **BISystemUser** (from the Default Provider), and add the newly created **BISystemUser** user in OUD.

o. Add the trusted user's credentials to the oracle.bi.system credential map.

p. Using Fusion Middleware Control target navigation pane, navigate to **farm > WebLogic Domain**, and select **bifoundation_domain**.

i. Using the WebLogic Domain menu, select **Security** > **Credentials.**

ii. Open the oracle.bi.system credential map, and select **system.user**.

iii. Click **Edit**.

iv. In the **Edit Key** dialog box, enter **BISystemUser** (or a name of your choice) in the **User Name** field.

v. In the **Password** field, enter the trusted user's password that is contained in Oracle Internet Directory.

vi. Click **OK**.

q. Restart the Managed Servers.

30. Enable the SSO authentication in the Weblogic Server for OBIEE using the following steps:

   a. Login to Fusion Middleware Control (EM) of the WebLogic Server.

   b. Navigate to the **Business Intelligence Overview** page.

   c. Navigate to the **Security** page.

   d. Click **Lock and Edit Configuration**.

   e. Select **Enable SSO,** this makes the SSO provider list active.

   f. Select the configured SSO provider from the list, as **Oracle Access Manager**.

   g. In **The SSO Provider Logoff URL**, specify the following URL:

   http://<oam_server>:14100/oam/server/logout

   h. Click **Apply**.

   i. Click **Activate Changes**.

   j. Restart the Oracle Business Intelligence components using Fusion Middleware Control.

6 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.