

# Oracle® Health Sciences Clinical Development Analytics

Security Guide

Release 4.0

E89764-02

January 2023

---

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:

- [Section 1, "General Security Principles"](#)
- [Section 2, "Protected Health Information"](#)
- [Section 3, "Security Guidelines for Oracle Health Sciences Clinical Development Analytics"](#)
- [Section 4, "Security Guidelines for Oracle Analytics Server"](#)
- [Section 5, "Setting Up Transparent Data Encryption Tablespace"](#)
- [Section 6, "Configuring SSO for OHSCDA OAS Using Oracle Access Manager 12c"](#)

## 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. Oracle highly recommends customers to apply these patches as soon as they are released. Critical patch updates are available at <http://www.oracle.com/technetwork/topics/security/alerts-086861.html#CriticalPatchUpdates>.

### 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.

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 12c (12.1)*.

## 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 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 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. 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 TLS

Due to the complexity in setting up TLS 1.2, it is not enabled by default during installation. Communications between the browser and the application servers should be restricted to TLS 1.2.

Set the `weblogic.security.SSL.protocolVersion` system property to TLS V 1.2. For more information, see *Oracle Fusion Middleware Securing Oracle WebLogic Server 10.3.6*.

## 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 Oracle Analytics Server (OAS) documentation for full instructions on configuring the RPD.

1. Open the RPD in the OAS 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 OAS server.

## 2.2 Exporting Data

OHSCDA out of the box utilizes native OAS 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 OAS's Usage Tracking option. This option tracks which queries were run by which users and when.

## 3 Security Guidelines for Oracle Health Sciences Clinical Development Analytics

Oracle Health Sciences Clinical Development Analytics (OHSCDA) spans several applications: Oracle Clinical, Oracle's Siebel Clinical, and InForm are the data sources, and Informatica ETL Execution Plans and transform Oracle Clinical, Siebel Clinical, and InForm data structures into the star schemas in an Oracle database. Oracle Analytics Server (OAS), which reads from the star schemas and provides the user interface where end users can view and analyze data through dashboards and reports. The execution of the ETL is controlled by the Oracle Data Warehouse Administration Console (DAC) or Oracle Data Integrator (ODI) for the respective OHSCDA technology stack release.

The Oracle WebLogic Server Administration Console is used to manage the embedded directory server used to authenticate users and groups. Oracle Fusion Middleware Control is used to create and manage the application roles and policies that control access to OAS resources.

Each of the following applications requires its own security implementation:

- **Transactional Applications:** Create and maintain access to Oracle Clinical, Siebel Clinical, and InForm using the application interfaces.
- **DAC:**
  - Access to modify DAC specifications should be limited to administrators. Other users who need to review execution plans and source specifications should be given read-only access to the DAC repository.
  - Create and maintain access to DAC using its user interface.
- **Informatica:**
  - Access to modify Informatica specifications should be limited to administrators. Other users who need to review mappings and workflows should be given read-only access to the Informatica repository.
  - Create and maintain access to Informatica using its user interface.
- **ODI:**

- Access to modify ODI specifications should be limited to administrators. Other users who need to review mappings should be given read-only access to the ODI repository.
- Create and maintain access to ODI using its user interface.
- **Oracle RDBMS:** End users of OHSCDA do not need to have accounts in the Oracle database schema that hosts the warehouse. Give access to the warehouse schema only to those who need to administer the warehouse tables.
- **OAS:**
  - **Authentication:** Use the Oracle WebLogic Server Administration Console to manage the embedded directory server that is used to authenticate users and groups.
  - **Authorization:** Use the Oracle Fusion Middleware Control to create and manage the Application roles and Application Policies that control access to OAS resources.  
Predefined OAS user groups determine the privileges allowed to users and allow access to the shipped OHSCDA dashboards and reports. You can create additional user groups as needed in OAS.

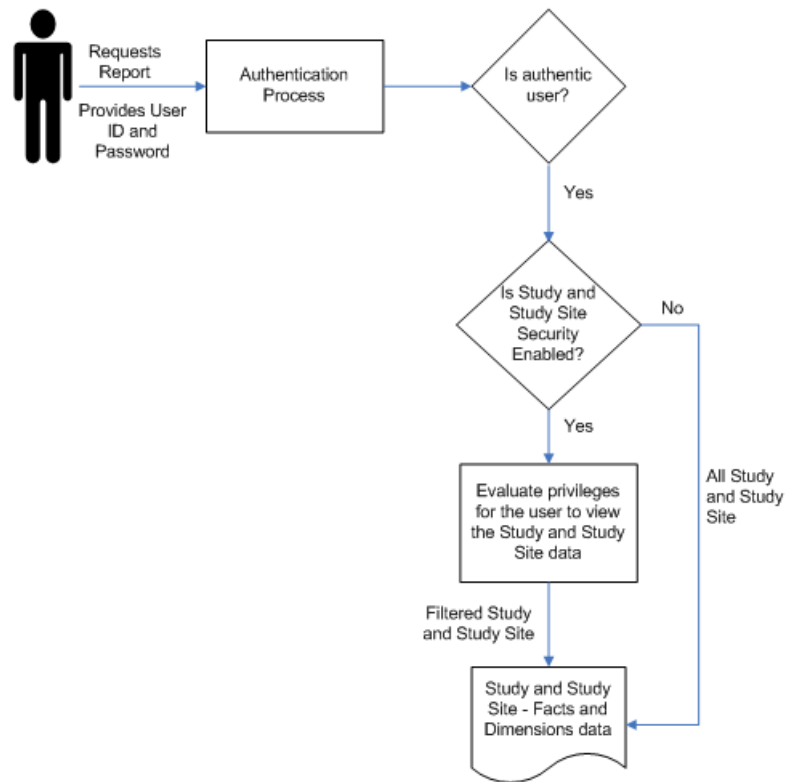
Data access controls which OAS users see what study and Study-site level data.

In OHSCDA,

- *study-level data* means planned sites, documents, and enrollment
- *study site-level data* means all other OHSCDA data

You can allow all users to see study-level data from all studies and study site-level data from all study sites, or you can require explicit access to particular studies and study sites for each user. You may need to create Oracle Clinical, Siebel Clinical, or InForm user accounts in order to explicitly control access by OHSCDA users to Study and Study-site level data. For more information, see [Section 3.2, "Setting Up Study and Study Site Data Access for Users"](#).

**Figure 1 Study and Study Site Security Implementation**



### Study and Study Site Security Implementation

\*\*\*\*\*

You must set up security for the following basic types of users:

- **OCDA End Users:** Users who can view Oracle Clinical, Siebel Clinical, and InForm data in OHSCDA through dashboards and reports. The specific dashboards and reports they can view are determined by the user groups they belong to.
- **OCDA Programmers:** Users who are authorized to create their own reports in the Analysis component of OAS or OCDA, which does not require any programming skills. You can distinguish between people who can simply create ad hoc reports and those who can save the reports they create to a dashboard so that other people can use them.
- **Informatica or ODI Programmers:** Users who can modify the functionality of OHSCDA by modifying the predefined ETL Programs that OHSCDA uses to transform transactional source data in Informatica or ODI repository for use in OHSCDA. They may also create new ETL Programs to support custom dashboards and reports in OHSCDA.
- **OCDA Schedulers:** Users who schedule OHSCDA jobs, including the data loading job and the user data access jobs. They need privileges similar to Informatica Programmers.
- **DAC Administrators:** Users who set up DAC and grant privileges to other users.
- **Informatica or ODI Administrators:** Users who set up Informatica or ODI Setups and grant privileges to other users.

## 3.1 Setting Up User Authentication

DAC handles creation and maintenance of users for ETL administration of OHSCDA. Oracle WebLogic handles reports related user authentication for OHSCDA.

### 3.1.1 Creating User Accounts in DAC

You can create user accounts in the following ways:

- Create users in DAC. For more information, refer to the *Oracle Business Intelligence Data Warehouse Administration Console Guide*.
- If you have an Oracle LDAP Directory, migrate users to Oracle Applications. For more information, see Doc ID 1508321.1 on My Oracle Support (<https://support.oracle.com>).

### 3.1.2 Setting Up User Authorization in OAS

When a user logs in, OAS verifies that they have valid credentials and populates the OAS Group session variable with a list of the user groups the user belongs to.

Authorization at the OAS level determines which parts of OHSCDA's OAS user interface, the logged in users can access. For information on how to set up user authorization, see [Section 3.1.2.1, "Using Predefined User Groups in OAS and Creating New Ones"](#).

#### 3.1.2.1 Using Predefined User Groups in OAS and Creating New Ones

All OHSCDA end users who view Oracle Clinical, Siebel Clinical, and InForm data in OAS must be associated with one or more OAS user groups. The OAS groups determine privileges allowed to users and allow access to the shipped OHSCDA dashboards and reports. To associate users with an OAS user group, assign their OAS account to an OAS user group.

OHSCDA provides a set of predefined OAS user groups. You can create additional groups, as needed.

---

---

**Note:** To perform administrative tasks in OAS, you must be a member of OAS's predefined Administrator group.

---

---

#### 3.1.2.2 Predefined OAS User Groups

OHSCDA includes predefined OAS user groups (called *groups* in OAS) to allow OHSCDA end users access to predefined dashboards. Each dashboard allows access to a predefined set of reports. For more information about predefined reports, see *Oracle Health Sciences Clinical Development Analytics User's Guide*.

The predefined user groups allow dashboard access as follows:

- **CRA dashboard:** Executive, Study Manager, Region Manager, and CRA
- **Data Manager EDC dashboard:** Data Manager, Executive, Study Manager, and Region Manager
- **Data Manager Paper dashboard:** Data Manager, Executive, Study Manager, and Region Manager
- **Executive dashboard:** Executive
- **Region Manager dashboard:** Executive and Region Manager

- **Study Manager dashboard:** Executive, Study Manager, and Region Manager
- **Study Overview dashboard:** All users
- **Study Region Overview dashboard:** All users
- **Study Site Overview dashboard:** All users
- **Index dashboard:** All users

For more information, refer to [Section 3.1.2.4, "Assigning OAS User Groups to Dashboards and Reports"](#).

---



---

**Note:** OHSCDA ships with both the Presentation catalog and Repository groups for each predefined user group.

---



---

### 3.1.2.3 Creating User Groups in WebLogic

You can create additional user groups in WebLogic, as needed. For example:

- If you create new dashboards or reports, you may need new user groups to manage access to them.
- To create new dashboards and reports, you must allow some users access to the OAS Answers component, for which they need to be in a user group with access to Answers.

For more information refer to *Oracle Fusion Middleware Securing Resources Using Roles and Policies for Oracle WebLogic Server 12c Release 1*.

---



---

**Note:** The OAS Presentation catalog and Repository user groups must all have **exactly** the same name.

---



---

### 3.1.2.4 Assigning OAS User Groups to Dashboards and Reports

To use a group to allow users access to particular dashboards or reports, you must assign the new group to one or more dashboards or reports.

Log in to OAS, click **Settings > Administration > Privileges**. For more information, see *Administering Oracle Analytics Server*.

## 3.2 Setting Up Study and Study Site Data Access for Users

You can set two variables to either allow all users access to data from all studies and study sites or you can require each user to have explicit access to particular studies and study sites. For more information, refer to [Section 3.2.1, "Setting the Systemwide Access Variables"](#).

In OHSCDA:

- **Study data** means data pertaining to the study as a whole, including planned sites, planned enrollment, and the ratio of actual to planned subjects. It is not a roll-up of all patient data from all study sites. For security purposes, all documents are considered Study data as well, regardless of whether the document pertains to a Study, a Region, or a Study-Site.
- **Study site data** means all other OHSCDA data, including information about discrepancy management, CRF verification and approval, workloads, and more.



This means that if you set the variables to require explicit access:

- If users require access to study-wide data on planned sites, enrollment, or documents, they must have explicit access to study data for that study. Having access to all study sites does not automatically allow access to study data.
- If users require access to study site data from every site in a study, they must have explicit access to each study site. You can set up this access automatically by importing user privileges from Oracle Clinical, Siebel Clinical, or InForm. For more information, refer to [Section 3.2.3, "Importing Study and Study Site Data Access Privileges"](#).

---

---

**Note:** If a user has access to multiple, but not all, sites in a study, the totals displayed in OHSCDA reports reflect the totals for the sites to which the user has access, not the totals for all sites in the study. For more information, refer to [Section 3.2.4, "Study-Site Access Example"](#).

---

---

### 3.2.1 Setting the Systemwide Access Variables

The following static repository variables determine whether explicit access to study or study site data is required for all users:

- **Enable\_Study\_Access\_Sec:** If set to **Y**, all users must have explicit access granted to study-level data for a particular study in order to see that data. If set to **N**, all users can see study-level data for all studies.
- **Enable\_Study\_Site\_Access\_Sec:** If set to **Y**, all users must have explicit access to a particular study site in order to see site-level data for that study site. If set to **N**, all users can see site-level data for all study sites.

The default value for both variables is **N**.

---

---

**Note:** If you set these variables to **Y** you must populate a set of tables with user access data. For more information, refer to [Section 3.2.3, "Importing Study and Study Site Data Access Privileges"](#).

Oracle recommends that you set both variables to the same value.

---

---

To change the value for either variable:

1. Stop the BI Server and the BI Presentation Server Services.
2. Using the OAS Administrator tool, edit the Repository:
  - a. On the **Manage** Menu, choose **Variables**.
  - b. In the **Variable Manager** dialog, choose **Repository**, then **Variables**, then **Static**.
  - c. Open the properties of the variable, either by double-clicking it or through the context menu.
  - d. Edit the value of Default Initializer for the variable: **Y** enables access control; **N** disables access control.
  - e. Exit the Static Repository Variable dialog.
  - f. Exit the Variable Manager.
  - g. Save the modified Repository.

3. Start the BI Server and BI Presentation Server Services.

### 3.2.2 Data Access Tables

OHSCDA uses three database tables to control users' access to rows of data in the star schema fact tables that pertain to particular studies and study sites. The data access tables are:

- W\_HS\_APPLICATION\_USER\_D contains a list of the user accounts that can have data access granted to particular studies and study sites. It must be populated from an external source. OHSCDA includes a sample ETL Program for this purpose. For more information, refer to [Section 3.2.3, "Importing Study and Study Site Data Access Privileges"](#).
- W\_HS\_STUDY\_ACCESS\_SEC controls which users can see study-level data on which studies.
- W\_HS\_STUDY\_SITE\_ACCESS\_SEC controls which users can see study site-level data on which study sites.

### 3.2.3 Importing Study and Study Site Data Access Privileges

The data access tables must be populated with data. OHSCDA includes a set of template ETL programs for this purpose. The programs are called *template* programs because you will need to adjust them according to your particular configuration, if you are enabling access control. If you are not enabling access control, the template programs can be used as they are. The following list enumerates the degrees to which you may want to modify the template programs:

- If you set the systemwide access variables to **N**, run the template ETL programs as is to populate the tables with a dummy user. All users have access to all study-level and study site-level data for all studies and sites.
- If you set the systemwide access variables to **Y**, modify the ETL programs as necessary to import user access information from Oracle Clinical, Siebel Clinical, and InForm. If you are able to use OHSCDA but do not currently have either Oracle Clinical, Siebel Clinical, or InForm user accounts with privileges for specific studies or sites set, you must create user accounts with the desired privileges in one of the source transactional systems.
- If you set the systemwide access variables to **Y**, modify the ETL programs as necessary to import user access information from some other source.

#### About Oracle Clinical Template Programs

The template ETL programs for Oracle Clinical are:

- SDE\_OC\_Application\_User\_D
- SDE\_OC\_Study\_Access\_Sec
- SDE\_OC\_Study\_Site\_Access\_Sec

The Oracle Clinical table OPA.OPA\_LEVEL\_PRIVS stores study and study site data access information for Oracle Clinical and Oracle Clinical Remote Data Capture (RDC) Onsite users. The Oracle Clinical or RDC administrator sets these privileges in the Maintain Access to Studies and Maintain Access to Sites windows in either Oracle Clinical or the RDC Administration application.

The template OC ETL programs will read data from this table and populate the data access tables in the OHSCDA warehouse.

OHSCDA uses this data to allow users access to study and study site data in OAS. In Oracle Clinical and RDC the concept of study and study site data access is different from OHSCDA's, and you can specify a variety of privileges on studies and study sites, which is not required in OHSCDA where all data access is view-only. The template OHSCDA ETL programs interpret the Oracle Clinical/RDC data as follows:

- If a user has been granted any privileges on a study site in OPA\_LEVEL\_PRIVS, the programs give the user study site-level access to that study site in OHSCDA.
- If a user has been given any privileges on a study in OPA\_LEVEL\_PRIVS, the programs give the user:
  - Study-level access to that study in OHSCDA
  - Study site-level access to all the study sites in that study

The template ETL programs also remove the Oracle Clinical OPS\$ prefix from each user name. You will likely need to alter this translation of Oracle Clinical user name to OHSCDA user name. For more information, refer to [Section 3.2.3.1, "Modifying the Data Access Programs"](#).

#### **About Siebel Clinical Security ETL Programs**

The security ETL programs for Siebel Clinical are:

- SDE\_SC\_Application\_User\_D
- SDE\_SC\_Study\_Access\_Sec
- SDE\_SC\_Study\_Site\_Access\_Sec
- SDE\_SC\_Party\_Parent
- SDE\_SC\_Study\_Hierarchy
- SDE\_SC\_Study\_Site\_Hierarchy

These programs read from the standard tables describing Siebel Clinical users and protocols, and the access that users have to studies. Review the programs, and adjust them to correspond to any changes you have made from the standard Siebel Clinical model.

#### **About InForm Security ETL Programs**

The security ETL programs for InForm Clinical are:

- SDE\_IF\_Study\_Access\_Secs
- SDE\_IF\_Study\_Site\_Access\_Secs

Programs read from the standard tables describing InForm users and studies, and the access that users have to studies and study sites. Review the programs, and adjust them to correspond to any changes needed as per the custom requirement.

The other security ETL programs are:

- SIL\_Application\_User\_D
- SIL\_Study\_Access\_Sec
- SIL\_Study\_Site\_Access\_Sec

#### **3.2.3.1 Modifying the Data Access Programs**

You may need to modify the data access ETL programs for the following reasons:

- **User Name Conversion Modification:** You may need to edit the SDE programs to adapt the user name conversion to your input Oracle Clinical, Siebel Clinical, or InForm user names and your output OHSCDA user names. Be careful; if the following conditions are not met, names will not match up and access control will fail.
  - The conversion performed in the all the SDE programs must be identical
  - The resultant user name must be the same as the user name used for OHSCDA purposes. SDE ETL programs that execute the ETL to populate the data access tables have a parameter for entering the E-mail portion of the standard user name format.
- **Interpretation Logic Modification:** You may prefer to interpret the Oracle Clinical, Siebel Clinical, or InForm privileges differently in OHSCDA.
- **Source Modification:** You may want to import data access information from another source.

For instructions on modifying ETL programs, see *Oracle Health Sciences Clinical Development Analytics Administrator's Guide*.

**3.2.3.2 Running the Template Data Access Control ETL Programs** You should run your versions of these programs:

- when you first set up OHSCDA
- when new users need access
- when new studies are added
- when new sites are added to studies
- when the systemwide access variable settings are modified

You must run the programs in the order in which they are listed in [Section 3.2.3, "Importing Study and Study Site Data Access Privileges"](#). For more information, see *Oracle Health Sciences Clinical Development Analytics Administrator's Guide*.

### 3.2.4 Study-Site Access Example

In Study 012345, users U2 and U3 have study-site access defined in the OHSCDA data access table W\_STUDY\_ACCESS\_STUDY\_SITE\_SEC as follows (note that user U1 is not in the table at all):

**Table 1 Study Site Access Example**

APPLICATION_ USER_WID	STUDY_WID	STUDY_SITE_WID
U2	A	A1
U2	A	A2
U3	B	B1
U3	B	B2

The distribution of discrepancies by study site, as stored in the discrepancies aggregate table in the warehouse, is:

**Table 2 Study Site Access Example**

Study	Study Site	Number Of Discrepancies
A	A1	20
A	A2	15
B	B1	30
B	B2	10
B	B3	20

**Table 3 Study Site Access Example**

Study	Study Site	Number Of Discrepancies
A	A1	20
A	A2	15
B	B1	30
B	B2	10
B	B3	20

A query on this data has been created and saved as a report:

Users U1, U2, and U3 can run the report. When user U1 runs the report, nothing can be seen. U1 has no access to any study site data.

When user U2 runs the report, U2 sees the following:

**Table 4 Study Site Access Example**

Study	Number of Discrepancies
A	35

And U2 drills down within Study A, the following can be seen:

**Table 5 Study Site Access Example**

Study	Site	Number of Discrepancies
A	A1	20
A	A2	15
Total		35

When user U3 runs the report, U3 sees the following:

**Table 6 Study Site Access Example**

Study	Number of Discrepancies
B	40

That is, U3 sees the sum of the values for the sites U3 is entitled to see, not the sum for the study. For user U3, it is as if site B3 does not exist. Drilling down shows the same effect:

**Table 7 Study Site Access Example**

Study	Site	Number of Discrepancies
B	B1	30
B	B2	10
Total		40

---

**Note:** A given document can pertain to study-site, a region, or a study. Ideally, there would be separate security controls for each level. However, in OCDA Release 4.0, we are applying the same security to all documents. As every region and study-site belongs to a study, we control documents at the study level.

---

## 4 Security Guidelines for Oracle Analytics Server

While installing and configuring the OAS Server, you should follow guidelines in the document *Managing Security for Oracle Analytics Server*.

### 4.1 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 your 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.

### 4.2 Managing Usage Tracking

For information, see *Administering Oracle Analytics Server*.

## 5 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 be 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>;
```

## 6 Configuring SSO for OHSCDA OAS Using Oracle Access Manager 12c

For information, see the section Understand SSO Authentication and Oracle Analytics Server in *Managing Security for Oracle Analytics Server*.

## 7 Change Record

- July 2019: First version of the guide.
- January 2023: Second version of the guide. Replaced the OBIEE-related content with OAS.

## 8 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 Clinical Development Analytics Security Guide, Release 4.0  
E89764-02

Copyright © 2010, 2023, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, and MySQL are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners. Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.