Oracle Business Intelligence Enterprise Edition (OBIEE)

Security Access Process

Department of Administrative Services,
Financial Business Services

Date: 07/14/2020

Version: 1.0

Authors:

DAS FBS, Aaron Wallace
DAS IT PMO, Umer Shaikh

1 Review and Approval

1.1 Reviewed by:

Name	Title/Position/Role	Review Date
Trudy Vidal	Financial Business Systems Manager	05/12/2020
Aaron Wallace	Sr. Datamart Business Analyst	05/12/2020
Kim Simmons	Cyber Security Services Analyst	05/12/2020

1.2 Approved by:

Name	Title/Position/Role	Date
Trudy Vidal	Financial Business Systems Manager	

1.3 Changes:

The following table will identify major changes to the process that require additional review and approval by DAS FBS Management. The changes must be distributed for review and comment. The major version number will increment after each major revision.

Date	Version	Person	Change Description

Contents

2 OBIEE SECURITY ACCESS OVERVIEW

2.1 DAS ORACLE BUSINESS INTELLIGENCE ENTERPRISE EDITION (OBIEE) FOR FINANCIAL DATAMART

The DAS Financial Datamart is an electronic warehouse of data extracted from the following statewide information systems:

- Accounting – Statewide Financial Management Application (SFMA)
- Payroll – Oregon State Payroll Application (OSPA)
- Budget - Oregon Budget Information Tracking System (ORBITS)
- Position – Position Information Control System (PICS)
- Personnel – Position and Personnel Data Base (PPDB)

900+ users throughout state government access, gather and organize data housed within the DAS Datamart via Oracle Hyperion Interactive Reporting Studio (IR Studio).

DAS has implemented a replacement for IR Studio with Oracle's Business Intelligence Enterprise Edition (OBIEE) web-based tool, which is hosted at the State Data Center (SDC) and maintained by EIS Data Center Services (DCS).

This product utilizes EIS DCS shared Active Directory for user authentication. Active Directory user groups are mapped to OBIEE application roles at the system level in Enterprise Manager to automate the user role assignment in OBIEE.

To manage users and groups, EIS DCS uses Active Roles Server (ARS) Web Console. Agency Help Desk personnel and dedicated Agency ARS Administrators manage their users & groups.

The OBIEE production URL is https://obi.das.oregon.gov:9503/analytics and is only accessible through state's VPN.

OREGON ACCOUNTING MANUAL 10.70.00 - SECURITY ACCESS TO CENTRAL FINANCIAL SYSTEMS

OBIEE security process is in alignment with the Statewide Policy as outlined in Oregon Account Manual 10.70.00. This policy outlines the process and assigns responsibilities for requesting security access to the state's central financial systems. The policy applies to all entities accessing the statewide financial systems.

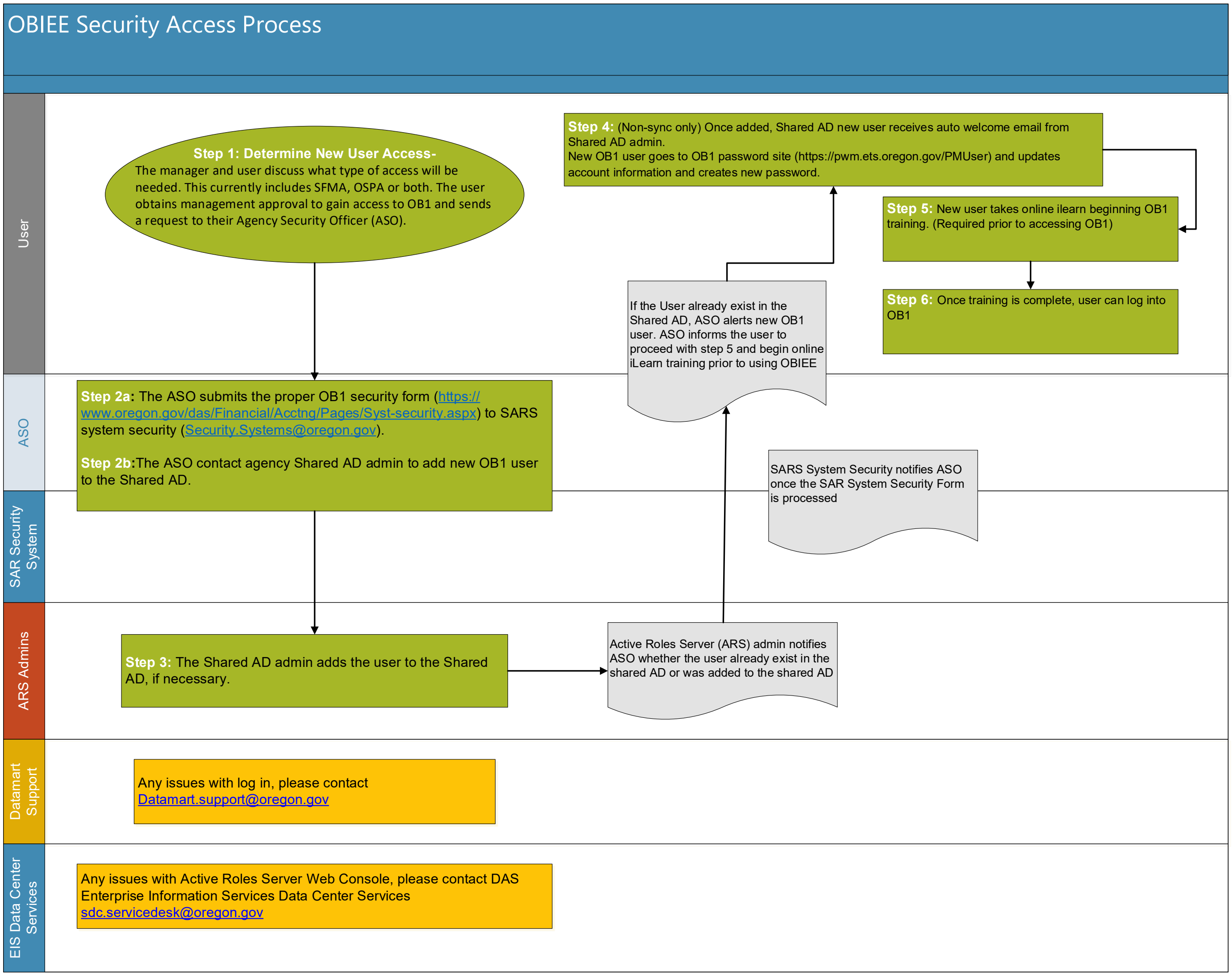
https://www.oregon.gov/das/Financial/Acctng/Documents/10.70.00.pdf

2.2 OBIEE OVERALL SECURITY ACCESS PROCESS

a) A new user needs access to OBIEE (a.k.a. 'OB1'). The manager and user discuss what type of access will be needed. This currently includes SFMA, OSPA or both. The user obtains management approval to gain access to OB1 and sends a request to their Agency Security Officer (ASO).

b) The ASO submits the proper OB1 security form (https://www.oregon.gov/das/Financial/Acctng/Pages/Syst-security.aspx) to SARS System Security (Security.Systems@oregon.gov).

c) The ASO needs to alert their agency Shared AD admin of a new OB1 user. The Shared AD admin adds the user to the Shared AD, if necessary. (Some agencies have users on the Shared AD already).
d) (Non-sync only) Once added, new user receives auto welcome email from Shared AD admin. New OB1 user goes to OB1 password site (https://pwm.ets.oregon.gov/PMUser) and updates account information and creates new password.
e) (Sync only) User is already in the Shared AD, therefore, ASO alerts new OB1 user.
f) Once SARS System Security is complete with adding user to new OB1 groups, they alert ASO.
g) ASO alerts user that OB1 access is complete.
h) New user takes online iLearn beginning OB1 training. (Required prior to accessing OB1)
i) Once training is complete, user can log into OB1. Any issues with log-in, please contact Datamart.support@oregon.gov.



OBIEE Security Access Process

Step 1: Determine New User Access-
The manager and user discuss what type of access will be needed. This currently includes SFMA, OSPA or both. The user obtains management approval to gain access to OB1 and sends a request to their Agency Security Officer (ASO).

Step 4: (Non-sync only) Once added, Shared AD new user receives auto welcome email from Shared AD admin.
New OB1 user goes to OB1 password site (https://pwm.ets.oregon.gov/PMUser) and updates account information and creates new password.

Step 5: New user takes online ilearn beginning OB1 training. (Required prior to accessing OB1)

Step 6: Once training is complete, user can log into OB1

If the User already exist in the Shared AD, ASO alerts new OB1 user. ASO informs the user to proceed with step 5 and begin online iLearn training prior to using OBIEE

Step 2a: The ASO submits the proper OB1 security form (https://www.oregon.gov/das/Financial/Acctng/Pages/Syst-security.aspx) to SARS system security (Security.Systems@oregon.gov).

Step 2b: The ASO contact agency Shared AD admin to add new OB1 user to the Shared AD.

SARS System Security notifies ASO once the SAR System Security Form is processed

Step 3: The Shared AD admin adds the user to the Shared AD, if necessary.

Active Roles Server (ARS) admin notifies ASO whether the user already exist in the shared AD or was added to the shared AD

Any issues with log in, please contact Datamart.support@oregon.gov

Any issues with Active Roles Server Web Console, please contact DAS Enterprise Information Services Data Center Services sdc.servicedesk@oregon.gov

3 OBIEE SECURITY ACCESS COMMUNICATION

a. Details of the OBIEE security process are described on the Datamart website: (https://www.oregon.gov/das/Financial/AcctgSys/Pages/datamart.aspx#security).

b. New OBIEE form and details of the OBIEE security process are described on the SARS website: (https://www.oregon.gov/das/Financial/Acctng/Pages/Syst-security.aspx)

   i. The OB1 form will include options for the user to select if they want Datamart access to the following data: SFMS, OSPS or both.

4 REVOKING OBIEE ACCESS

a. There is an automatic revoke process when it comes to the Shared AD.

   ii. Shared AD admin: No need to complete any tasks as there is an automatic revoke process.

   iii. Agency: When a user leaves, the agency will move data files from the OB1 ‘my folder’ account of the user to the ‘shared folders’ with the help of OB1 admin (ASO).

   iv. Agency ASO: Alert SARS system security to remove user from the main OB1 security group (called: DAS_OSCIO_OBIEE). This process is completed on the ARS site (https://sshelp.ets.oregon.gov/). This will ensure the user will no longer have access to OB1.

   v. SARS will include this access as part of the 6-month security review.

5 OBIEE SECURITY TRAINING

The following information and training will be available to appropriate staff:

a. Communication document on the duties of a Shared AD admin.

b. Instructions for Agency Security Officers (ASO’s) to help with the security and updating of users in OB1.

c. Instructions to help the SARS security team set up and monitor OB1 users.

d. A beginning level training, for new users of the OB1 product, setup in ilearn. This allows users access for training at any time.

6 OBIEE PASSWORD RESET

a. There are two types of users of OB1: ‘Sync’ and ‘Non-sync’.

   i. Sync: The sync users are employees already set up in the Shared AD. Sync users’ passwords are updated automatically and are the same as a users’ log-in to their work computer. When a user changes their password on their work computer, it will sync up to the OB1 application. Be aware that there may be a slight delay for the password change to sync.

ii. Non-sync: These users are employees who are manually added to the Shared AD by agency Shared AD admin. They must update their passwords every 90 days (standard password policy). A warning email will arrive 7 days prior to expiration to alert them to update their password.

1. There is a dedicated OB1 password website for OB1 non-sync users: (https://pwm.ets.oregon.gov/PMUser). This site helps to change and update OB1 passwords.
2. A non-sync user will receive an auto welcome email from the Shared AD admin after the user is added to Shared AD. The new user must immediately update their password on OB1 password site after receiving this email.

b. OB1 has a 'cancel' button viewable within the 'Results' section. A user can cancel the query at any time.