Oracle® Banking Treasury Management

Oracle Access Manager

Release 14.7.0.0.0
F71199-02
November 2022

Oracle Banking Treasury Management Oracle Access Manager, Release 14.7.0.0.0

F71199-02

Contents

Preface

This guide helps the user to understand single sign-on can be enabled for a Oracle Banking Treasury Management deployment using Oracle Fusion Middleware 12c.

The images used in the documentation are of illustration purpose and need to be used only for reference.

This preface has the following topics:

Audience

This guide is intended for anyone responsible for installing Oracle Banking Application.

Acronyms and Abbreviations

The acronyms and abbreviations are listed in this below table:

Table 1 Acronyms and Abbreviations

Abbreviations or Acronyms	Definition
DV	Derivatives
ETD	Exchange Traded Derivatives
FX	Foreign Exchange
MM	Money Market
OBTR	Oracle Banking Treasury Management
ODT	Open Development Tool
OT	Over the Counter Options
SE	Securities
SR	Securities Repo

Related Resources

For more information, see these Oracle Banking Treasury Management resources:

- *Oracle Banking Treasury Management Release Notes*

- *Oracle Banking Treasury Management Installer Index*
- *Oracle Banking Treasury Management Installer Prerequisite*

1

Pre-Requisites

The following are the pre-requisites for Oracle Access Manager (OAM) and LDAP Directory Server.

This topic has the following sub-topics:

Software Requirements

1. Oracle Access Manager – OAM (12.2.1.4.0)
   - Access Server
   - Webtier Utilities 12.2.1.4.0
   - Web Gate 12.2.1.4.0
   - Http Server
2. LDAP Directory Server
   Please make sure that the LDAP which is been used for Oracle Banking Treasury Management Single Sign on deployment is certified to work with OAM.

   List of few LDAP Directory servers supported as per OAM document (note – this is an indicative list. The conclusive list can be obtained from the Oracle Access Manager documentation):
   - Oracle Internet Directory
   - Active Directory
   - ADAM
   - ADSI
   - Data Anywhere (Oracle Virtual Directory)
   - IBM Directory Server
   - NDS
   - Sun Directory Server
3. Web Logic 12.2.1.4.0
   For the purpose of achieving single sign on for OBTR in FMW 12c, it is necessary for the weblogic instance to have an explicit Oracle HTTP server (OHS).

Background of SSO related components

The SSO related components are listed below:

- Oracle Access Manager (OAM)
- LDAP Directory Server

- WebGate/AccessGate
- Identity Asserter

This topic has the following sub-topics:

Oracle Access Manager

Oracle Access Manager (OAM) consists of the Access System, and the Identity System. The Access System secures applications by providing centralized authentication, authorization and auditing to enable single sign-on and secure access control across enterprise resources. The Identity System manages information about individuals, groups and organizations. It enables delegated administration of users, as well as selfregistration interfaces with approval workflows. These systems integrate seamlessly.

The backend repository for the Access Manager is an LDAP-based directory service that can be a combination of a multiple directory servers, which is leveraged for two main purposes:

- As the store for policy, configuration and workflow related data, which is used and managed by the Access and Identity Systems
- As the identity store, containing the user, group and organization data that is managed through the Identity System and is used by the Access System to evaluate access policies

LDAP Directory Server

To integrate Oracle Banking Treasury Management with OAM to achieve Single Sign-on feature, Oracle Banking Treasury Management's password policy management, like password syntax and password7 expiry parameters can no longer be handled by Oracle Banking Treasury Management.

Instead, the password policy management can be delegated to the Directory Server. All password policy enforcements would be on the LDAP user id's password and Not Oracle Banking Treasury Management application users' passwords.

WebGate/AccessGate

A WebGate is a Web server plug-in that is shipped out-of-the-box with Oracle Access Manager. The WebGate intercepts HTTP requests from users for Web resources and forwards it to the Access Server for authentication and authorization.

Whether you need a WebGate or an AccessGate depends on your use of the Oracle Access Manager Authentication provider. For instance, the:

- Identity Asserter for Single Sign-On: Requires a separate WebGate and configuration profile for each application to define perimeter authentication. Ensure that the Access Management Service is On.

- Authenticator or Oracle Web Services Manager: Requires a separate AccessGate and configuration profile for each application. Ensure that the Access Management Service is On.

Identity Asserter

Identity Asserter uses Oracle Access Manager Authentication services and also validates already authenticated Oracle Access Manager Users through the ObSSOCookie and creates a WebLogicauthenticated session. It also provides single sign-on between WebGates and portals. We can get more details on Identity asserter

> **Note:**
>
> This document containts the configuration of Oracle Interner Directory as LDAP server and its configuration in weblogic. This document will not discuss the configuring and setting up of OAM and LDAP directory server of other LDAP servers. This will be provided by the corresponding Software provider.

2 Configuration

This topic explains the configuration of Oracle Access Manager to enable single sign-on using Oracle Internet Directory as a LDAP server.

This topic has the following sub-topics:

Pre-Requisites

The steps provided below assume that Oracle Banking Treasury Management has already been deployed and is working (without single sign-on)

The provided below steps assume that Oracle Access Manager and the LDAP server have been installed already and the requisite setup already done with respect to connecting the two along Weblogic's Identity Asserter.

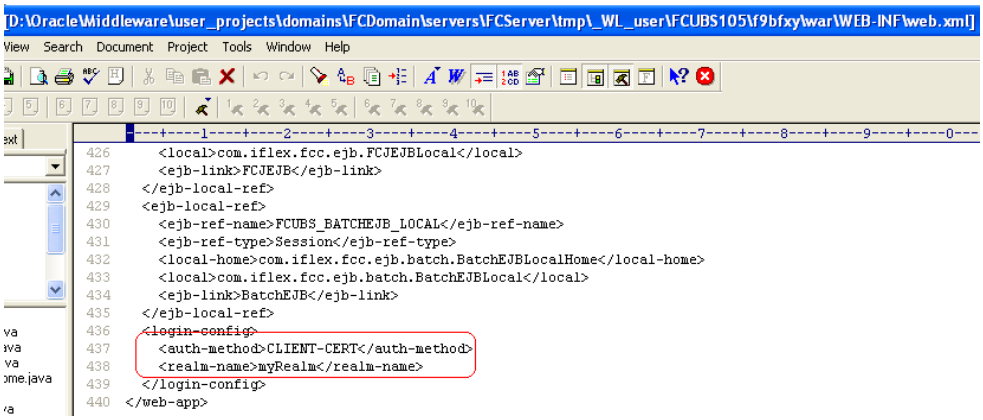
Change the web.xml file

(Optional) Enter contextual information here, including the purpose of the task.

1. Locate the web.xml file in the application (OBTR) EAR file.
2. Add the following lines under login-config.

```
<login-config>
<auth-method>CLIENT-CERT</auth-method>
<realm-name>myRealm</realm-name>
</login-config>
```

Figure 2-1 web.xml file



3. Save the file and redeploy and restart the application.

Configuring SSO in OAM Console

After installing OAM, Webtier Utilities and Webgate, extend the weblogic domain to create OAM server.

Follow the post installation scripts deployWebGate and EditHttpConf as provided in Post Installation Steps.

1. Identity Store Creation.
2. To create new User Identity Store, Login to OAM Console.
3. Navigate to **System Configuration** > **Common configuration** > **Data Sources** > **User Identity Store**.
4. Input below information in the User Identity Store.

   Choose Store Type as Oracle Internet Directory.

   Location:

   LDAP server Host name and Port Number in <HOSTNAME>:PORT format

   Bind DN:

   User name to connect the LDAP Server

   Password:

   Password to connect the LDAP Server

   User Name Attribute:

   The attribute created in LDAP, which will be the User Name for the other application (here it will be treated as the OBTR Username)

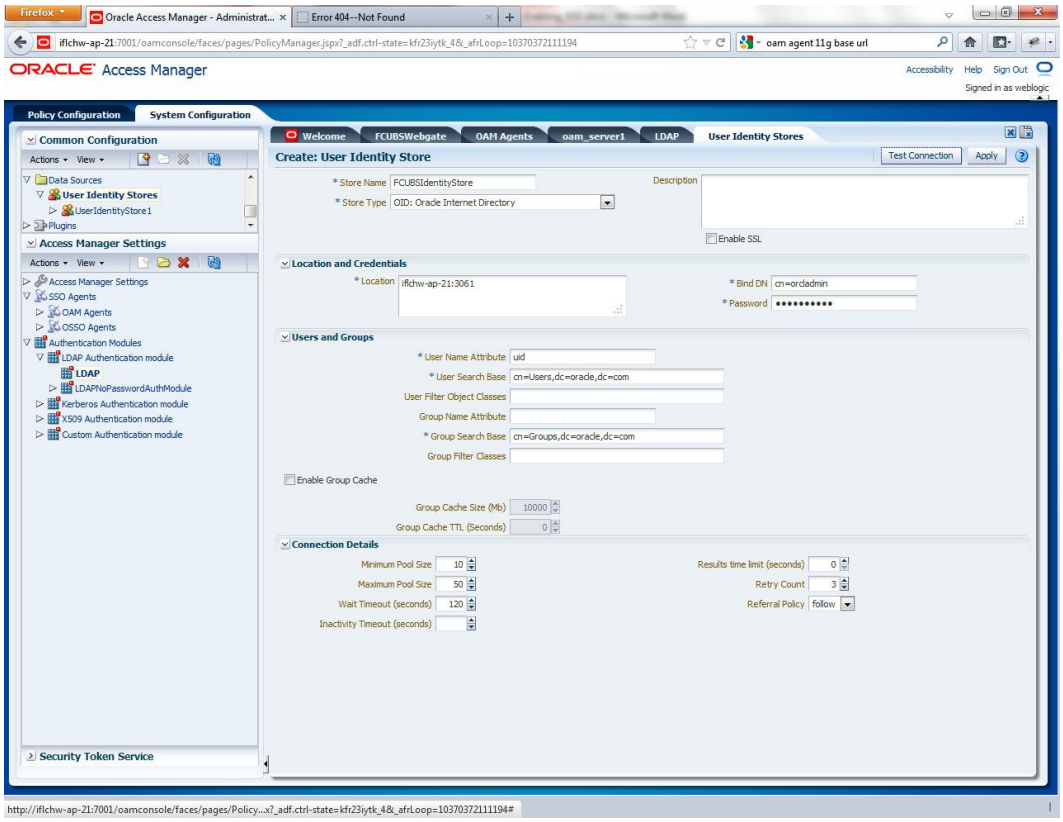
   User Search Base:

   The container of the User Name in the LDAP server.

   Group Search Base:

   The container of the Group Name in the LDAP server.

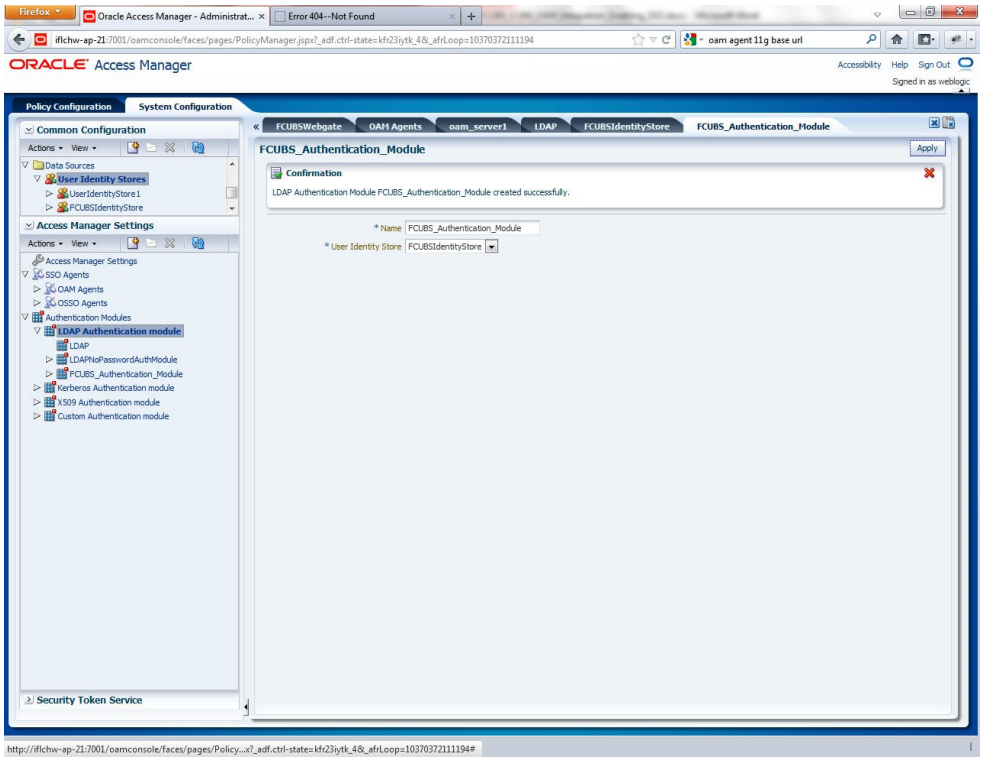
Figure 2-2 Oracle Access Manager- System Configuration



5. Click on **Apply** button after entering the above information.
6. On successful creation, click **Test connection** button to verify whether the LDAP connection is working fine.
7. To create Authentication Module, navigate to **System Configuration** > **Access Manager Settings** > **Authentication Modules** > **LDAP Authentication Module**.

   The LDAP Authentication Module screen is displayed.

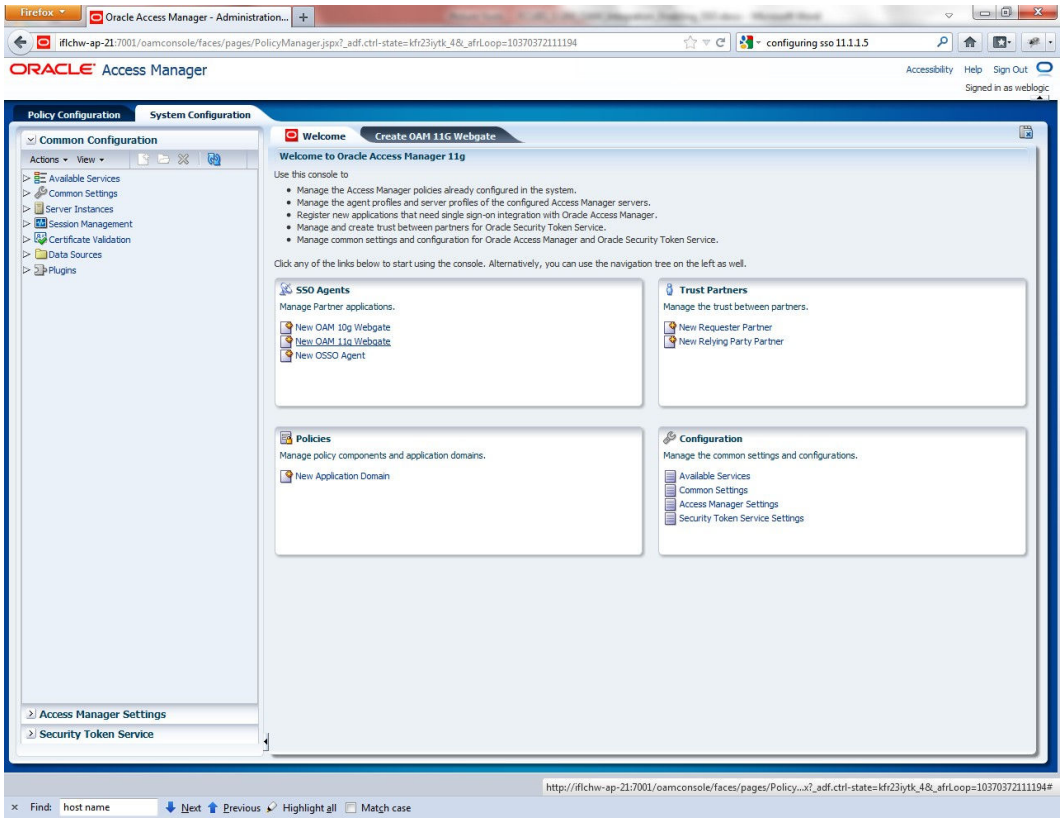
Figure 2-3 LDAP Authentication Module



8. Click the **New** button to create new Authentication Module. Input the Name of the authentication module and choose the User Identity Store we created in step 1.
9. To create OAM 12c Webgate, navigate to **System Configuration** > **Access Manager Settings** > **SSO Agents** > **OAM Agents**

   The OAM Agents page is displayed.

Figure 2-4 OAM Agents



10. Click on the **Create 12c webgate** button or Click on New OAM 12c Webgate link available in welcome page.

11. Enter any name for Webgate and Base URL (The host and port of the computer on which the Web server for the Webgate is installed) and click on apply.

    Once the OAM 12c Webgate created, add filterOAMAuthnCookie=false parameter along with default parameters in User Defined Parameters. Click ‘Apply’ button to save the changes.

12. Post OAM Webgate 12c Creation Steps

    Perform the following steps to copy the artifacts to the Webgate installation directory:

    - On the Oracle Access Manager Console host, locate the updated OAM Agent ObAccessClient.xml configuration file (and any certificate artifacts). For example: `$DOMAIN_HOME/output/$Agent_Name/ObAccessClient.xml`
    - On the OAM Agent host, copy artifacts (to the following Webgate directory path). For example: `12cWebgate_instance_dir/webgate/config/ObAccessClient.xml (for instance WebTier_Middleware_Home/Oracle_WT1/instances/instance1/config/OHS/ohs1/webgate/config/ObAccessClient.xml)`

13. To create Authentication Scheme, navigate to **Policy Configuration** > **Authentication Schemes** and click on ‘Create’ button to create new Authentication Scheme.

    Name : Any name to identify Authentication Scheme

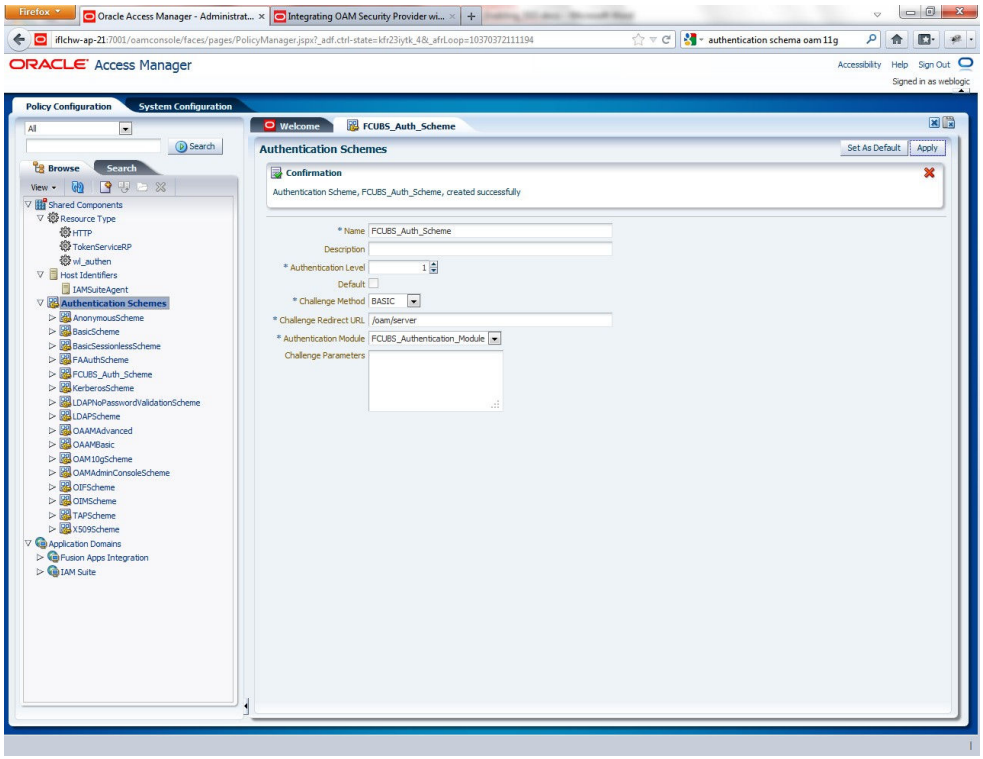
    Challenge Method : BASIC

    Challenge Redirect URL : /oam/server

Authentication Module : Choose the authentication module created in step 2.

If it is a basic authentication scheme, we need to add the 'enforce-valid-basic-auth-credentials' tag to the config.xml file located under /user_projects/domains/<MyDomain>/config/. The tag must be inserted within the <security-configuration> tag as follows: [Just before the end of security configuration tag] <enforce-valid-basic-auth-credentials>false</enforce-valid-basic-auth-credentials> </security-configuration>

Figure 2-5 Authentication Schemes



14. To create authentication policy, navigate to **Policy Configuration** > **Application Domains** > **[Webgate agent name]** > **Authentication Policies** .
15. Click new button and input the below information

    Name: Enter any name to identify the Authentication Policy (eg. OBTRWebPolicy)

    Authentication Scheme: Choose the authentication scheme created in step 5.

    Resources: Add the resources which are all need to be protected. If <WebgateName>:/…/ and <WebgateName>:/ are added in the resources then all the sources are protected.
16. Add DN in the Responses section. Enter the value as $user.attr.dn. The responses maintained in the tab will be added in the response header during the authentication.
17. To add Resources, navigate to **Policy Configuration** > **Application Domains** > **OBTRWebgate** > **Resources**.
    - Click on Create New Resource button .
    - Select the type as HTTP.

- Select the Host Identifier as OBTRWebgate
- Enter the resource URL as /FCJNeoWeb
- Select the protection level as Protected
- Click on apply button to update the resource added.

18. Select the Authentication policy and Authorisation policy as Protected Resource Policy.
19. Check whether the resources available in the authentication policies are available in Authorization Policy. During web gate creation these values are defaulted.
20. Add DN in the Responses section. Enter the value as $user.attr.dn. The responses maintained in the tab will be added in the response header during the authorization.
21. To enable the Oracle HTTP Server instances to route to applications deployed on the Oracle Weblogic Server Clusters, add the directive shown below to the mod_wl_ohs.sh file available in <Weblogic Home> /Oracle_WT1/instances/instance1/config/OHS/ohs1.

```
<Location /console>
SetHandler weblogic-handler
WebLogicHost idmhost1.mycompany.com


WeblogicPort 7001
</Location>
```

22. After configuration of webgate 12c agent launch the URL *http://<hostname>:<ohs_Port>/ohs/modules/webgate.cgi?progid=1* to verify whether the webgate configuration is fine. If the URL launches a screen as below then the webgate configuration is working fine.
23. Using OAM Test Tool (This step is not mandatory)

    There is a test tool provided in OAM software which helps us to check the response parameter values. The test tool is available in <OAM Install Dir>\ oam\server\tester. For eg. *D:\weblogic\Middleware\Oracle_IDM1\oam\server\tester*

    Use java -jar oamtest.jar to launch the OAM test tool.

Launching Oracle Banking Treasury Management

After setting up Oracle Banking Treasury Management to work on Single Sign on mode, perform the below procedure:

1. Navigate to the interim servlet URL from your browser.

   For e.g.: http://<hostname>:[port]/FCJNeoWeb

   Since the resource is protected, the WebGate challenges the user for credentials as shown below.
2. Once the user is authenticated and authorized to access the resource, the servlet gets redirected to normal Oracle Banking Treasury Management application server URL and now the new signon form will appear as below. The application will automatically redirect Oracle Banking Treasury Management home page.

   This topic has the following topics:

- SSO Parameters

SSO Parameters

To maintain the parameters required for SSO, perform the below procedure:

1. Go to **Security Maintenance** > **Sys. Administration** > **SSO Maintenance**.
2. Provide all the details like Directory Server host name, Port number, LDAP admin User id , admin Password, LDAP base and Login time out duration (in Sec).

Maintaining LDAP DN for OBTR Users

For each user id in OBTR a user has to be created in the LDAP. When creating the user in LDAP ensure that the DN used is same as the LDAP DN value that will be updated in user maintenance form.

1. Once the user is created in LDAP go to the user creation form in OBTR.

   . If the OBTR user already exists then unlock the user and update the LDAP DN value which was set when creating the user in LDAP.
2. Click on **Validate** button to check whether any other user is having the same LDAP DN value.

Launching Oracle Banking Treasury Management

After setting up Oracle Banking Treasury Management to work on Single Sign on mode, perform the below procedure:

1. Navigate to the interim servlet URL from your browser.

   For e.g.: http://<hostname>:[port]/FCJNeoWeb

   Since the resource is protected, the WebGate challenges the user for credentials as shown below.
2. Once the user is authenticated and authorized to access the resource, the servlet gets redirected to normal Oracle Banking Treasury Management application server URL and now the new signon form will appear as below. The application will automatically redirect Oracle Banking Treasury Management home page.

   This topic has the following topics:

Signoff in a SSO Situation

Oracle Banking Treasury Management does not provide for single signoff currently, i.e., when a user signs off in Oracle Banking Treasury Management, the session

established with Oracle Access Manager by the user will not be modified in any manner.

In a SSO situation the ‘Exit’ and ‘Logoff’ actions in Oracle Banking Treasury Management will function as ‘Exit’, i.e., on clicking these, the user will ‘exit’ Oracle Banking Treasury Management and will need to re-launch Oracle Banking Treasury Management using the Oracle Banking Treasury Management launch URL.