Oracle E-Business Single Sign-On (SSO) - Setup Guide

Index -

- End of Document -

Oracle E-Business Single Sign-On (SSO) - Setup Guide

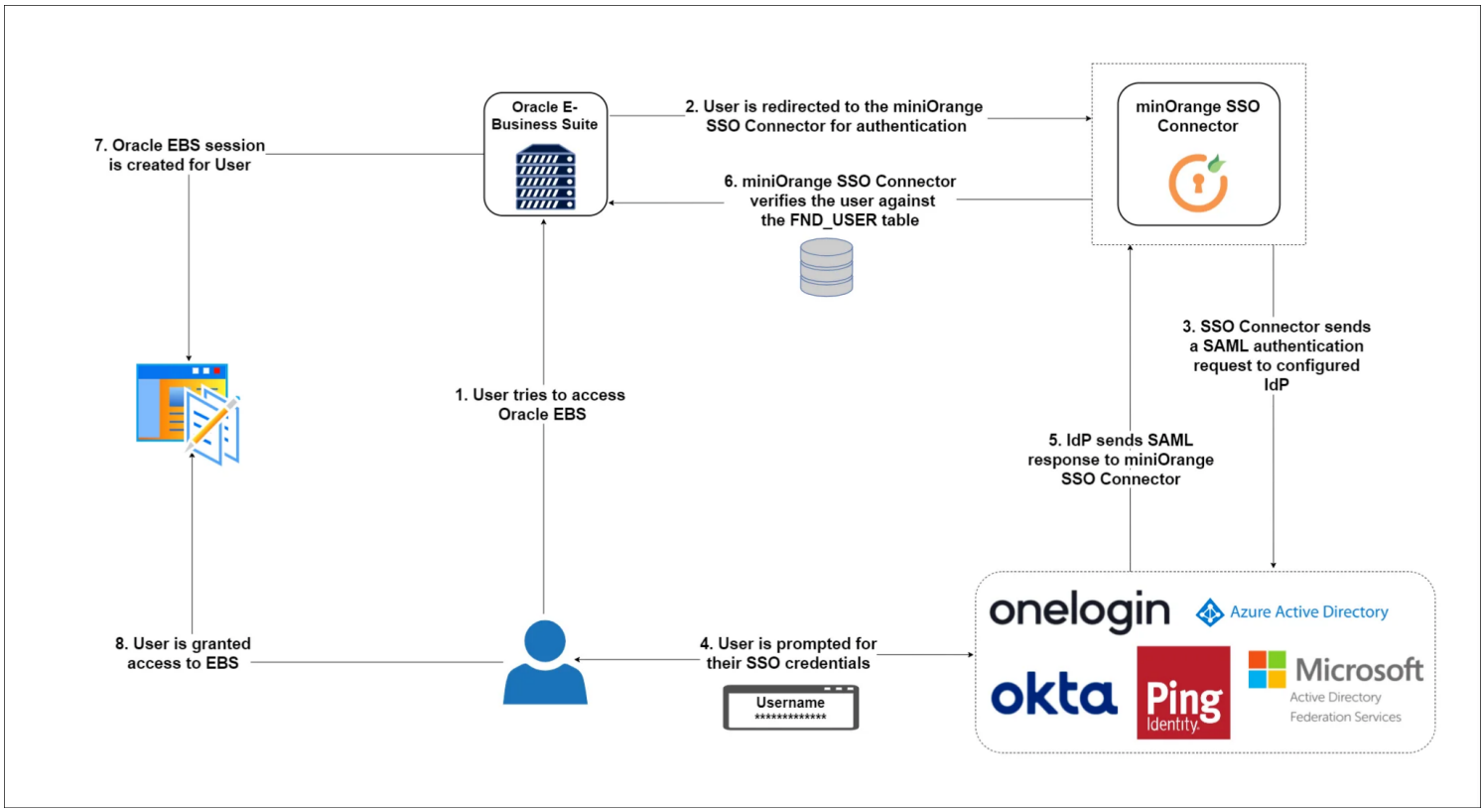
"miniOrange Oracle EBS SSO connector enables the Single Sign-On (SSO) between Oracle EBS and any IDPs without the need to purchase and install Oracle Access Manager (OAM) and Oracle Internet Directory (OID) license."

IDPs (Identity Providers) like miniOrange, ADFS, Active Directory, Azure AD, Google, Okta, Onelogin, Ping Identity, Centrify and many more are supported.

It also provides SSO support for web applications which do not provide support for federated Single Sign-On (SSO) protocols such as SAML or OAuth 2.0. SSO connector gives you the flexibility of extending your existing SAML SSO integration to Oracle EBS as well.

This is possible due to its capability to act as a broker between multiple IDPs & your configured applications. This states that you can perform seamless SSO integration for Oracle EBS with your existing authentication platform.

Authentication Flow for miniOrange Oracle EBS SSO (Single Sign-On) Solution:



General Flow -

1. The User tries to access the Oracle E-Business Suite, either directly at the AppsLogin endpoint or via a bookmarked URL.

2. Oracle EBS redirects the request to the miniOrange SSO Connector for authentication.

3. The SSO Connector sends a SAML authentication request to the configured IDP.

4. The User is Prompted to enter their SSO (IDP) credentials.

5. Configured IDP sends SAML response to miniOrange SSO Connector.

6. The Connector checks the value of the username/email attribute fetched from the IDP against the FND_USER table in the Oracle EBS Database.

7. After successful authentication, a session is created for the user in Oracle EBS.

8. User is redirected to Oracle EBS as a logged-in user.

Follow the Step-by-Step Guide given below for Oracle E-Business Single Sign-On (SSO)

1. Configure Oracle EBS with miniOrange SSO Connector

- Set aside a sub-domain for the miniOrange Oracle EBS SSO connector on the same domain as the EBS installation. For example, if the EBS installation has the URL apps.example.com:, the miniOrange Oracle EBS Single Sign-On connector could be installed on the sub-domain ebsauth.example.com.

- In your Oracle E-Business Suite installation, login as SYSADMIN and do the following:

    1. Create a new user, and assign them the role with code: UMX|APPS_SCHEMA_CONNECT. Make a note of the credentials for this user.
    2. Navigate to Functional Administrator → Core Services → Profiles, and make the following changes:
    3. Search for the Profile with code APPS_SSO; change its site value from SSWA to SSWA w/SSO.
    4. Search for the Profile with the code APPS_AUTH_AGENT; change its site value to the full URL (FQDN) of the miniOrange Oracle EBS SSO connector (e.g. http://ebsauth.example.com/ebsauth).
    5. Search for the Profile with the name Oracle Applications Session Cookie Domain; change its value from Host to Domain.
    6. Bounce the Application Tier of the Oracle E-Business Suite to reflect the changes.

- Generate a DBC file with the miniOrange Oracle EBS SSO connector domain (e.g. ebsauth.example.com) using the AdminDesktop utility in EBS; make a note of the APPL_SERVER_ID value present in this newly generated file.

- Add your external data source (e.g. Active Directory) in the User Store section in your miniOrange Cloud/On-Premise installation; set this user store as the default user store (Prefer Step 2).

- Add an OpenID application in your miniOrange Cloud/On-Premise installation; the redirect URI should be as follows: http(s)://./ebsauth/redirect. For example, http://ebsauth.example.com/ebsauth/redirect.

- Make a note of the authorized endpoint (for external broker), token endpoint, and user info endpoint URLs.

- Deploy the miniOrange Oracle EBS SSO connector on your Tomcat server.

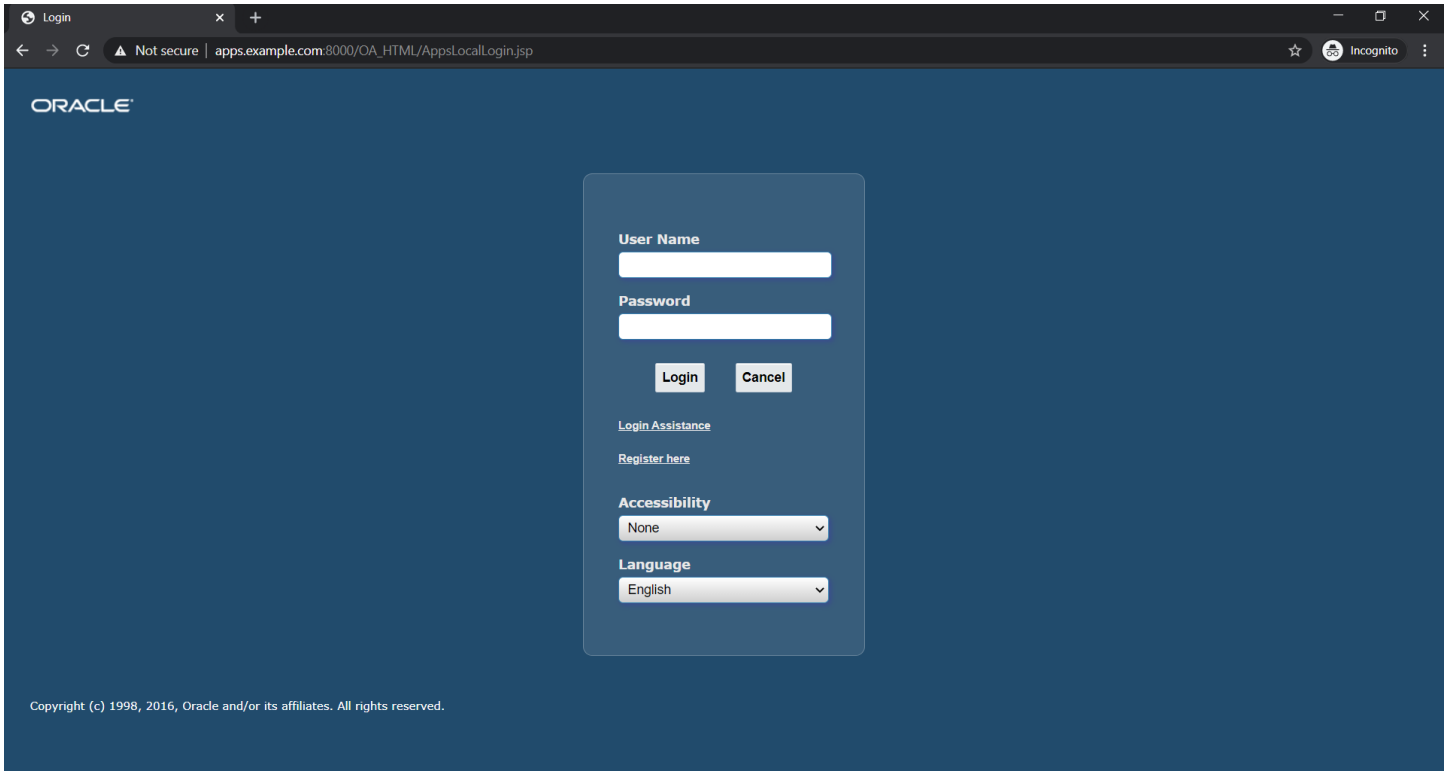
- Update the EBS connector.properties file in your miniOrange Oracle EBS Single Sign-On connector to reflect the credentials for the user created in step 2, the path of the DBC file & the APPL_SERVER_ID from step 3, and the endpoint URLs from step 5.

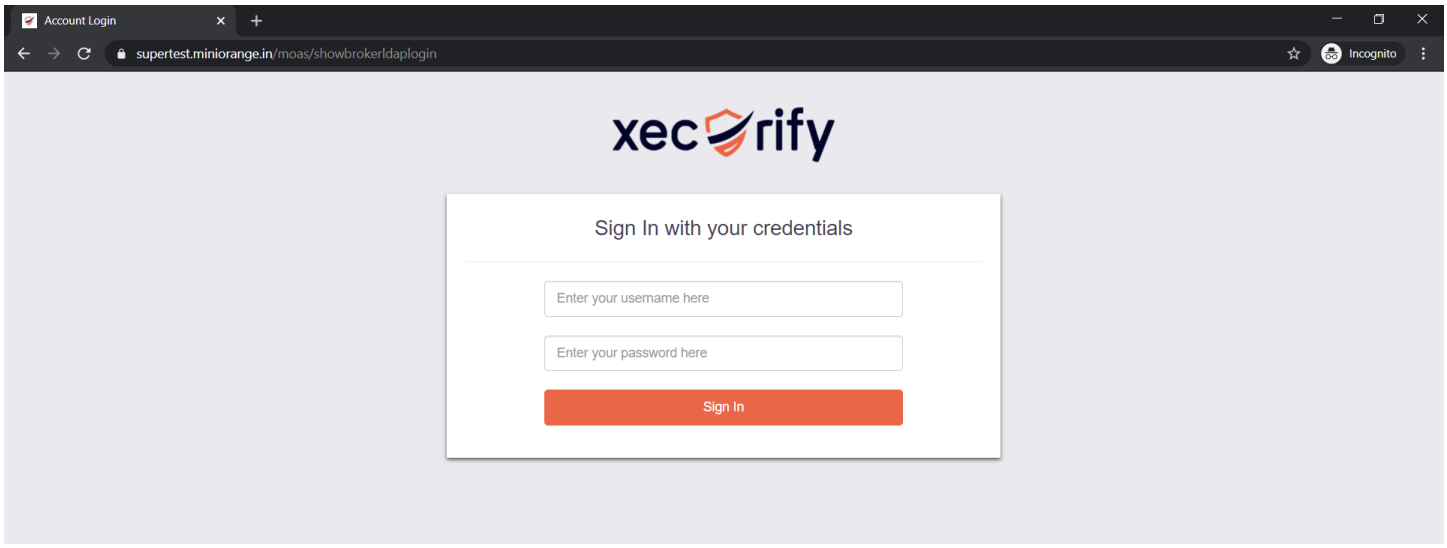
Visit Oracle EBS Single Sign-On| E-Business Suite SSO| SAML Integration to understand how you can set up your User Directory.

2. Oracle EBS Suite Login Flow

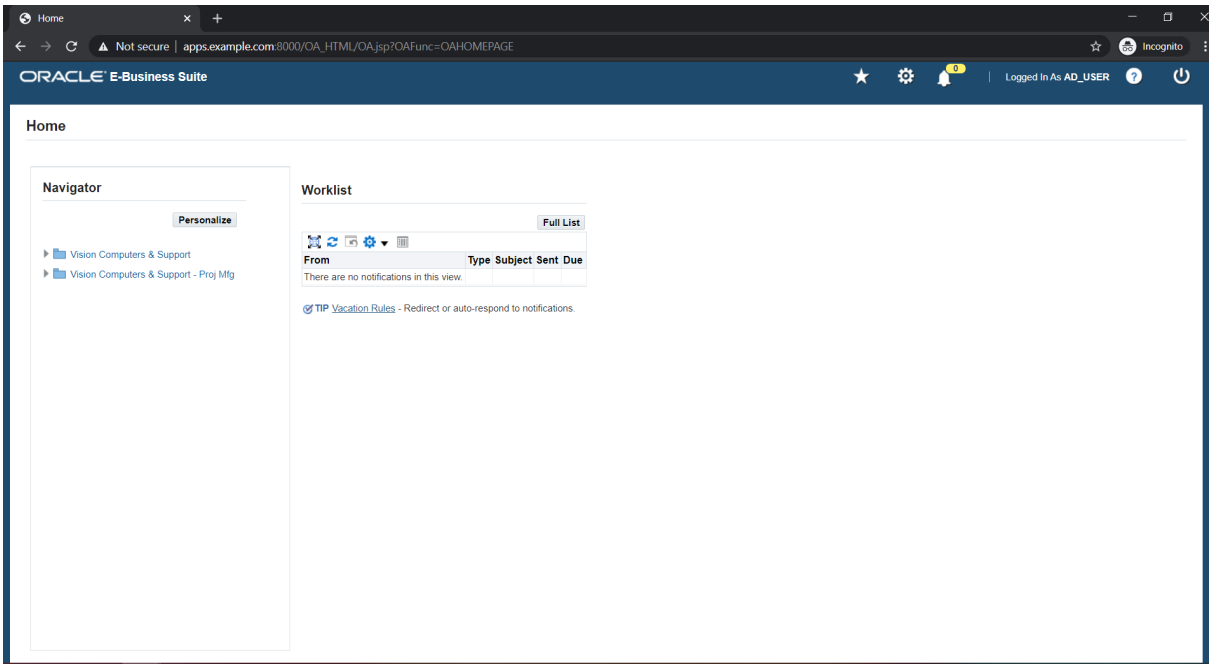
Scenario 1: User has not logged in, no session exists

When a user accesses any of their bookmarked Oracle E-Business Suite URLs without previously having logged in, a user from the original login (Oracle EBS login page) page will be redirected to the miniOrange login page.





- Here, the user will have to enter their Active Directory credentials - userPrincipalName and password.
- The miniOrange server will then authenticate the user against the Active Directory (AD), and perform authorization for accessing the user's username and email address.
- This username and email address will then be matched against the table of users in the Oracle E-Business Suite database (FND_USER), and the user will be logged in.



Scenario 2: User has logged in, session is active

When a user session already exists, the user can directly navigate to any of their bookmarked Oracle E-Business Suite URLs.

No authentication is required in this case; the user's session information is retrieved from the ICX session cookie that's present in the browser.

3. Oracle EBS (E-Business Suite) Provisioning with Active Directory

- Auto-Create user at the time of login authentication.
- Import Users from Active Directory and Sync them in Oracle EBS from miniOrange admin portal.
- Setup a scheduled sync to create/update/deactivate AD users in Oracle EBS on a daily basis.

THE END