Deploy Oracle E-Business Suite Across Oracle Cloud Infrastructure and Azure

SSO with Oracle Access Manager and Azure Active Directory

TECHNICAL PAPER / JUNE 7, 2019

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Revision History

The following revisions have been made to this paper:

Date	Revision
June 7, 2019	Initial publication

Table of Contents

Overview

This paper provides the details to configure SAML 2.0 federated single sign-on (SSO) for Oracle E-Business Suite R12 running in Microsoft Azure with Oracle Access Manager located on-premises. Although Oracle Access Manager can support various authentication methods with E-Business Suite, federation was chosen because it logically has the greatest integration support within the cloud when working with other cloud applications. Currently it's the only method tested for this use case.

The steps to integrate E-Business Suite and Oracle Access Manager are out of the scope of this document. However, details about how to integrate are published in various My Oracle Support documents that are referenced.

Architecture

The architecture is a hybrid approach of an already documented on-premises integration between Oracle Access Manager and E-Business Suite. What makes this a hybrid architecture?

- Placing E-Business Suite in Azure
- Using Azure Active Directory (Azure AD) as the federated identity provider (IDP) to authenticate a user to E-Business Suite
- Running Oracle Access Manager as the service provider (SP) on-premises with its backend LDAP server (either Oracle Unified Directory or Oracle Internet Directory)

This approach provides a way to be one step closer to moving some of your infrastructure to the cloud. It doesn't have to stop with just E-Business Suite—Oracle Access Manager and Oracle Unified Directory or Oracle Internet Directory can also be moved to the cloud.

Another key part of this architecture is the provisioning of user accounts. This paper assumes that Azure AD is the source of truth for user accounts. This means that a method of provisioning such as Oracle Directory Integration Platform synchronization or an identity management tool like Microsoft Identity Manager or Oracle Identity Manager should be used to provision user accounts into the Oracle Access Manager LDAP server (Oracle Unified Directory or Oracle Internet Directory). Then Oracle Directory Integration Platform used as a bi-directional synchronization service can synchronize that account into the E-Business Suite database. Certain key attributes that are critically important to SSO will be covered later in this paper.

Components

The components in this hybrid architecture are listed in the following table and shown in Figure 1.

ARCHITECTURE COMPONENTS

Data Center	Component
Azure	- Azure AD - Oracle E-Business Suite 12.2.*x* - Oracle HTTP Server 11g or 12c - Oracle WebGate 11g or 12c - Oracle AccessGate 11g or 12c
Oracle Cloud Infrastructure	Oracle E-Business Suite Database 12.2 or later
Customer on-premises	- Oracle Access Manager 11g or 12c - Oracle Unified Directory or Oracle Internet Directory 11g or 12c - Oracle Directory Integration Platform 11g or 12c - Oracle HTTP Server 11g or 12c (optional)

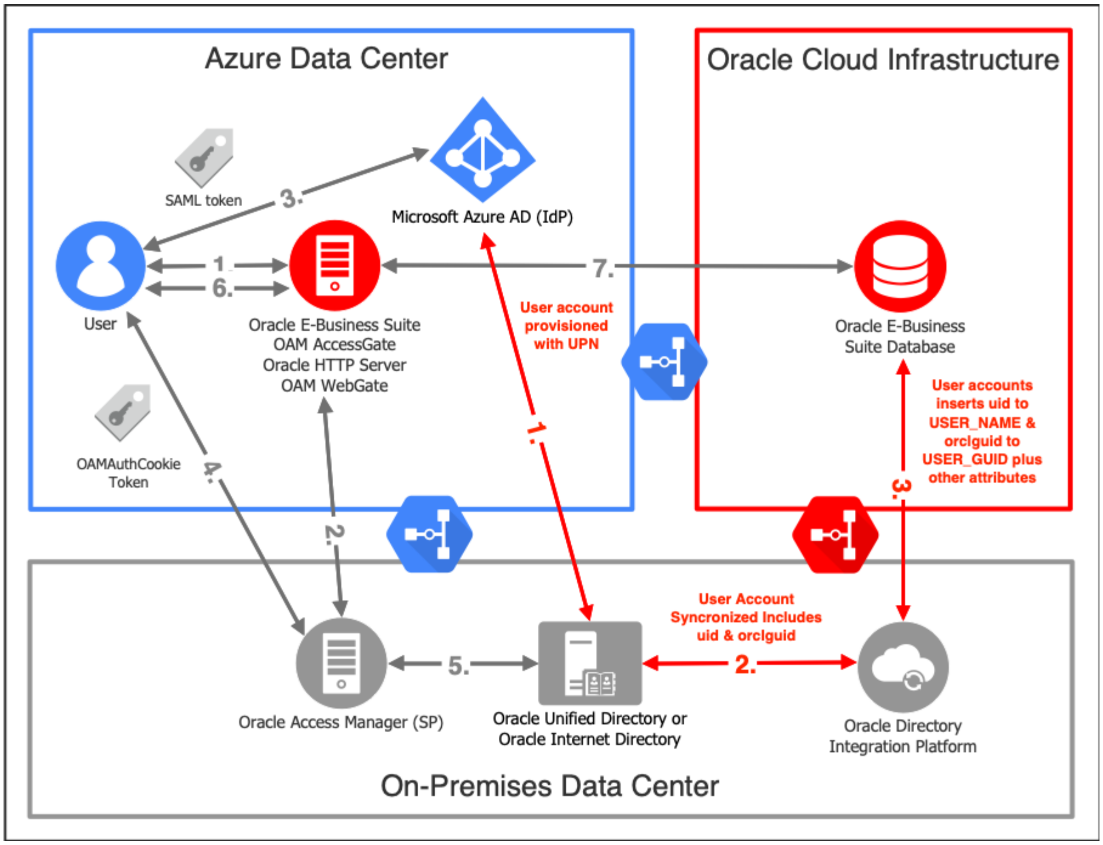

Azure Data Center
Oracle Cloud Infrastructure
SAML token
3.
Microsoft Azure AD (IdP)
User
1.
6.
7.
Oracle E-Business Suite
OAM AccessGate
Oracle HTTP Server
OAM WebGate
User account provisioned with UPN
Oracle E-Business Suite Database
User accounts inserts uid to USER_NAME & orclguid to USER_GUID plus other attributes
OAMAuthCookie Token
4.
2.
1.
3.
User Account Syncronized Includes uid & orclguid
5.
2.
Oracle Access Manager (SP)
Oracle Unified Directory or Oracle Internet Directory
Oracle Directory Integration Platform
On-Premises Data Center

Figure 1. Hybrid Architecture for E-Business Suite, Oracle Access Manager, and Azure AD Integration

Provisioning Flow

The provisioning flow is shown in Figure 1 with red arrows (1–3). This flow illustrates one example of how a user account is created in Azure AD, provisioned to the Oracle Access Manager LDAP server, and synchronized using Oracle Directory Integration Platform to the E-Business Suite database.

1. An initial user account that includes the user principal name (UPN) is provisioned from Azure AD to the Oracle Access Manager LDAP server (Oracle Unified Directory or Oracle Internet Directory). This provisioning is not the responsibility of Oracle Directory Integration Platform but instead done by some type of provisioning outside the scope of this paper.

2. Oracle Directory Integration Platform listens to Oracle Unified Directory change logs and provisions the user account to the E-Business Suite database.

3. Oracle Directory Integration Platform provisions the user account, mapping `uid` to USER_NAME and `orclguid` to USER_GUID, to the E-Business Suite database.

Federation Flow

The federation flow is shown in Figure 1 with black arrows (1–7). More detail about the federation flow in a service-provider-initiated federation is provided in “Understanding Azure AD and E-Business Suite Federation Flow” and in Figure 2.

1. The user requests E-Business Suite access, and WebGate checks for the OAMAuthCookie Token.

2. WebGate verifies that the user has no OAMAuthCookie Token, so it checks with Oracle Access Manager for a course of action.

3. Oracle Access Manager tells WebGate to redirect the user to Azure AD for federated authentication, and Azure AD prompts the user for login.

4. Azure AD validates the user’s credentials and then sends a SAML 2.0 assertion to Oracle Access Manager, using the mail attribute as the user mapping.

5. Oracle Access Manager accepts the SAML 2.0 assertion and returns the matching user in Oracle Unified Directory using the UPN. In the response, it provides the USER_NAME (uid) and USER_ORCLGUID (orclguid) from Oracle Unified Directory in the header defined in the policy.

6. WebGate redirects the user to E-Business Suite and sends the USER_NAME and USER_ORCLGUID as headers to AccessGate.

7. AccessGate looks up the USER_NAME and USER_ORCLGUID in the E-Business Suite database to verify that the user exists. On success, it sets its own session and returns the E-Business Suite portal page back to the user.

Prerequisites

This section explains important assumptions and details about key items that are required before you attempt the integration.

Assumptions

- All the components outlined in the Architecture section have been deployed and are working.
- Oracle E-Business Suite and Oracle Access Manager have been integrated. If they have not, follow the correct document referenced from the master list in My Oracle Support: *Using the Latest Oracle E-Business Suite AccessGate for Single Sign-On Integration with Oracle Access Manager* (Doc ID 2202932.1).
- A user account has been provisioned from Azure AD to the Oracle Access Manager LDAP server (see the following section). Provisioning implementation is out of the scope of this document because there can be more than one way to implement it.
- A user has been provisioned from the Oracle Access Manager LDAP server to the E-Business Suite database using Oracle Directory Integration Platform. This process is documented in one of the Oracle E-Business Suite SSO with Oracle Access Manager integration guides. See also the following section.
- Any high availability (HA) for Oracle E-Business Suite and Oracle Access Manager components have already been implemented. HA can be achieved, but it is out of the scope of this document.

Provisioning Critical User Attributes

Three user attributes are critical for integration: user principle name (UPN), USER_NAME, and USER_ORCLGUID. This section provides details about these attributes and how they are used.

Azure AD and Oracle Access Manager Integration

Following Azure AD best practices, the user principal name (UPN) is used as the federated user mapping attribute value. The UPN provides a unique value that is reliable for signing on to the user account and matching in Oracle Access Manager and E-Business Suite. As such, it’s the best choice for federation between Azure AD and Oracle Access Manager. For more information, see the Azure documentation.

The following table lists the minimal attributes that we recommend to provision from Azure AD to the Oracle Access Manager LDAP server.

RECOMMENDED MINIMUM USER ATTRIBUTES TO SYNCHRONIZE

Azure Attribute	LDAP Attribute	Example Value
userPrincipalName	mail	test.user1@mydomain.com
samAccountName	uid	test.user1@mydomain.com
displayName	cn	Test User1
givenName	givenName	Test
sn	sn	User1

Note: A password doesn't need to be provisioned

Oracle Access Manager and E-Business Suite Integration

As part of the E-Business Suite and Oracle Access Manager integration, USERNAME and ORCLGUID are critical unique user keys used between the Oracle Access Manager LDAP server and the E-Business Suite database. For example, the Oracle Access Manager LDAP server, whether Oracle Unified Directory or Oracle Internet Directory, typically uses the LDAP attribute `uid` for the username. However, when a user entry is created, the operational attribute `orclguid` is automatically created and stores a unique 32-character value. Similarly, in E-Business Suite, a username is stored in USER_NAME and an orclGUID is stored in USER_GUID. Both attributes must be unique.

In the authentication flow, the WebGate passes three headers, USER_NAME, USER_ORCLGUID, and OAM_LOCALE. The two most critical to authentication with E-Business Suite are USER_NAME and USER_ORCLGUID, which are retrieved from the Oracle Access Manager LDAP server. The attribute values must match between the Oracle Access Manager LDAP server and the E-Business Suite database user schema.

In regard to provisioning from Azure AD, you could use the samAccountName as the `uid` in the Oracle Access Manager LDAP server. It's more important that the samAccountName is also unique because, as part of the Oracle Access Manager and E-Business Suite integration, a uniqueness plugin is enabled to ensure that `uid` is unique. The `uid` attribute isn't important in the federation authentication, but it's important to ensure that the value is unique across the Oracle Access Manager LDAP server and the E-Business Suite database.

Configuring Integration and SSO

This section contains all the required steps to register a new federated service provider in Azure AD, register a new identity provider (E-Business Suite) in Oracle Access Manager, and make any required configuration changes to accomplish federated SSO authentication with Azure AD and E-Business Suite using Oracle Access Manager.

Understanding Azure AD and E-Business Suite Federation Flow

In this scenario, users access E-Business Suite with credentials stored in Azure AD. This access is achieved through a federated authentication setup with the SAML 2.0 protocol, in which Azure AD is the identity provider (IDP) and E-Business Suite is the service provider (SP). Because Oracle Access Manager is deployed in front of E-Business Suite for SSO, it's also the component that provides the federation capabilities to E-Business Suite. This section provides the required steps for implementing identity federation between Azure AD and Oracle Access Manager.

Note that we are mostly interested in a federation flow that's initiated on access to an E-Business Suite-protected endpoint. In SAML protocol terms, this is known as a service-provider-initiated (SP-initiated) flow, and is illustrated in Figure 2. In that flow, Oracle Access Manager (OAM) Server detects access to an E-Business Suite-protected resource, creates an authentication request (SAMLRequest), and redirects the browser to Azure AD for authentication. Azure AD challenges the user for credentials, validates them, creates a SAMLResponse as a response to the received authentication request, and sends it to Oracle Access Manager. In turn, Oracle Access Manager validates the assertion and asserts the user identification information embedded in the assertion, granting access to the protected resource.

Note that the configuration presented in this section also accounts for identity-provider-initiated (IdP-initiated) flow, where a request is initially made to Azure AD SAML intersite URL, which in turn sends an unsolicited SAMLResponse to the Oracle Access Manager Server.

SP-initiated single logout (where the logout flow is initiated by E-Business Suite) is also supported by the presented configuration. At the time this paper was initially published, IDP-initiated single logout (where the logout flow is initiated by the Azure portal) is not supported. See the "Known Issue" section at the end of this document for details.

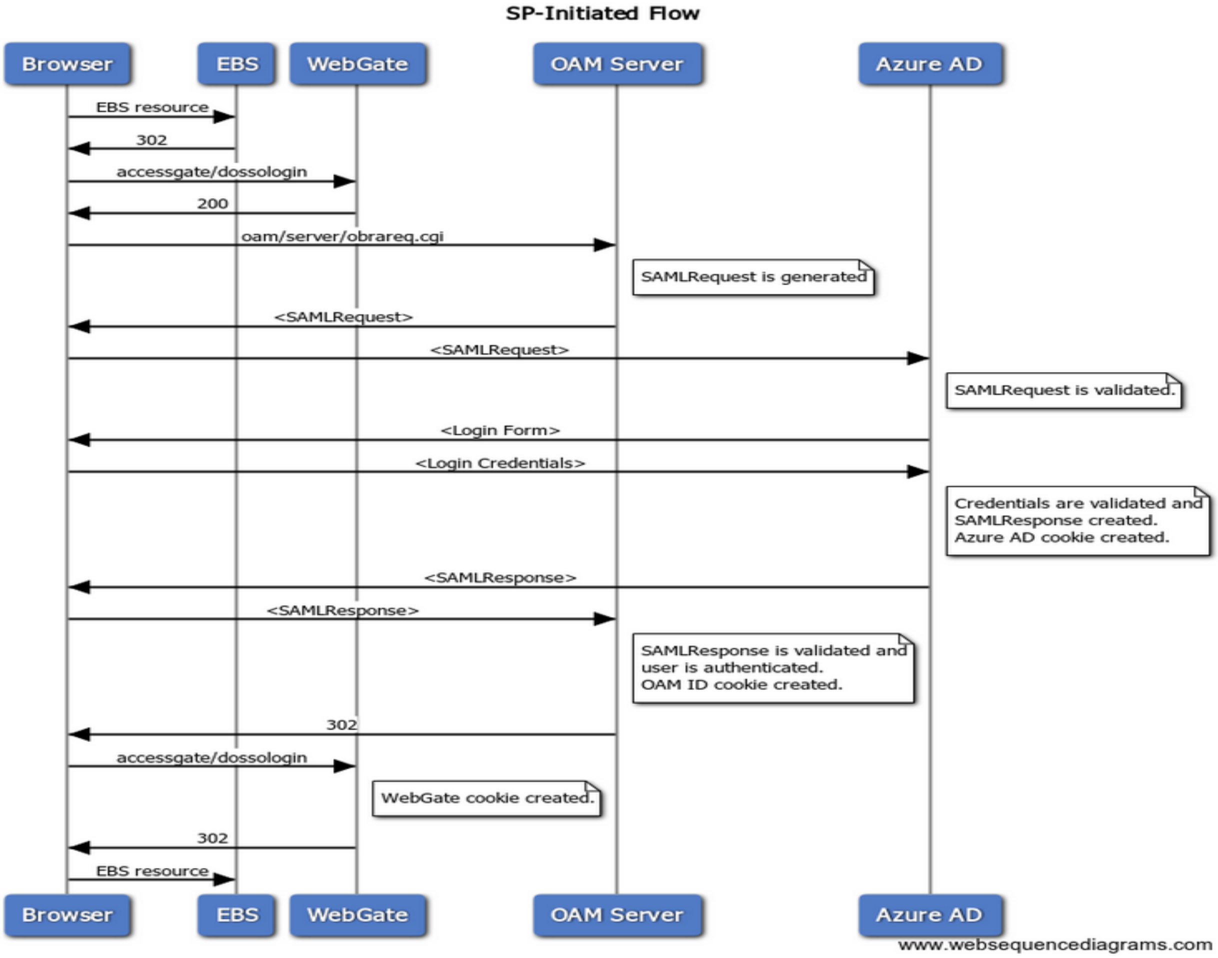
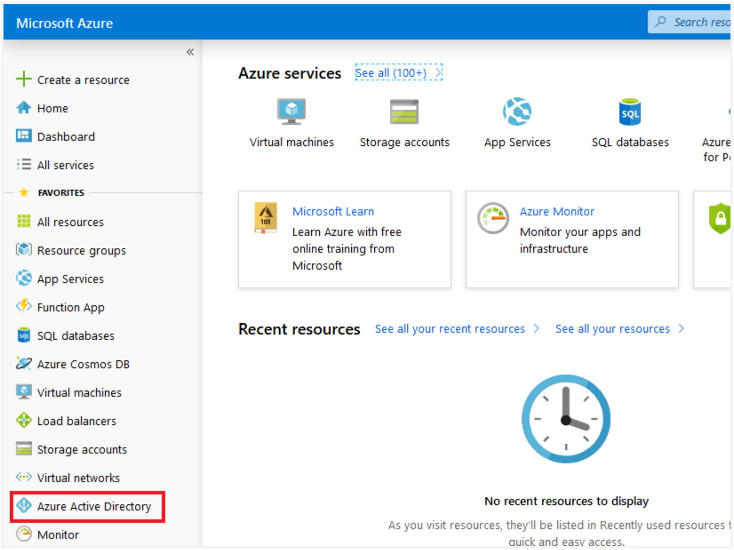


Figure 2. E-Business Suite SP-Initiated Federation Flow with Azure AD

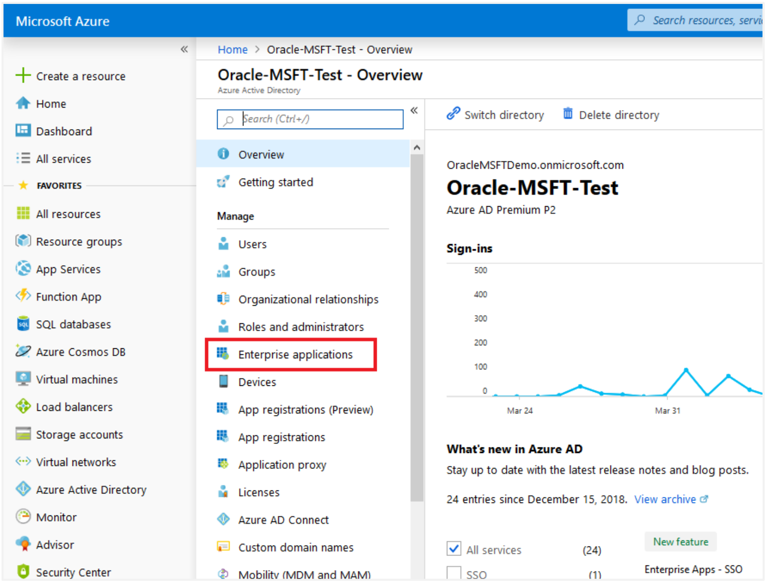
Configure Azure AD as the Identity Provider

1. Sign in to the Azure portal as a Domain Administrator.

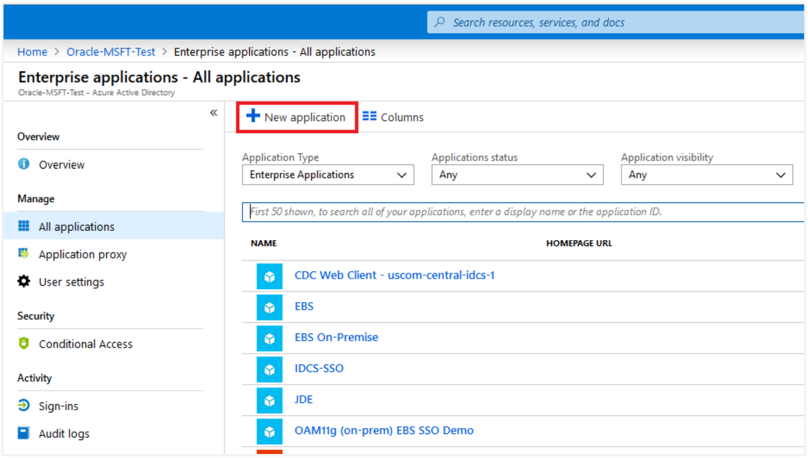
2. In the far-left navigation pane, click **Azure Active Directory**.



3. In the Azure Active Directory pane, click **Enterprise applications**.



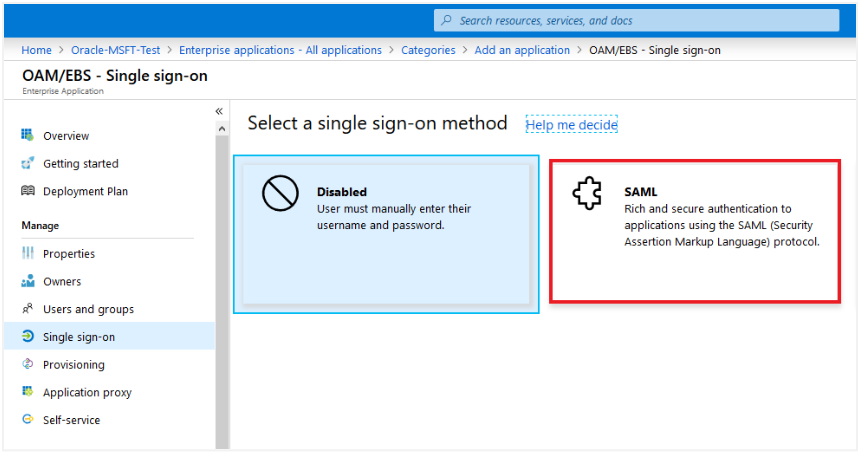
4. Click **New application**.


Search resources, services, and docs
Home > Oracle-MSFT-Test > Enterprise applications - All applications
Enterprise applications - All applications
Oracle-MSFT-Test - Azure Active Directory
New application
Columns
Overview
Overview
Manage
All applications
Application proxy
User settings
Security
Conditional Access
Activity
Sign-ins
Audit logs
Application Type
Enterprise Applications
Applications status
Any
Application visibility
Any
First 50 shown, to search all of your applications, enter a display name or the application ID.
NAME
HOMEPAGE URL
CDC Web Client - uscom-central-idcs-1
EBS
EBS On-Premise
IDCS-SSO
JDE
OAM11g (on-prem) EBS SSO Demo

5. In the **Add from Gallery** section, type **Oracle Access Manager for EBS** in the search box, select **Oracle Access Manager for EBS** from the resulting applications, and then click **Add**.

6. To configure Oracle Access Manager as a service provider for the application, click **Single sign-on**.

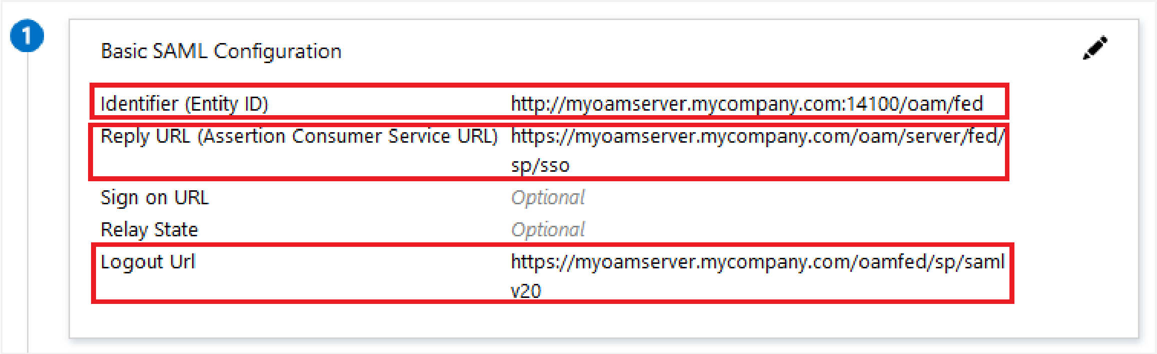
7. Select **SAML** as the single-sign-on method.


Search resources, services, and docs
Home > Oracle-MSFT-Test > Enterprise applications - All applications > Categories > Add an application > OAM/EBS - Single sign-on
OAM/EBS - Single sign-on
Enterprise Application
Overview
Getting started
Deployment Plan
Manage
Properties
Owners
Users and groups
Single sign-on
Provisioning
Application proxy
Self-service
Select a single sign-on method
Help me decide
Disabled
User must manually enter their username and password.
SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

The **Set up Single Sign-On with SAML** page is displayed, where you will enter the integration details in the following steps.

Some of the values that you need to enter come from Oracle Access Manager's SAML metadata. To get the metadata, go to `http(s)://<oam_hostname>:<port>/oamfed/sp/metadata`. The output is XML data, some of which you need in the next steps.

8. In the **Basic SAML Configuration** area of the **Set up Single Sign-On with SAML** page, provide values for **Identifier (Entity ID)**, **Reply URL (Assertion Consumer Service URL)**, and **Logout Url**.



1

Basic SAML Configuration

Identifier (Entity ID)	http://myoamserver.mycompany.com:14100/oam/fed
Reply URL (Assertion Consumer Service URL)	https://myoamserver.mycompany.com/oam/server/fed/sp/sso
Sign on URL	*Optional*
Relay State	*Optional*
Logout Url	https://myoamserver.mycompany.com/oamfed/sp/samlv20

- **Identifier (Entity ID)** corresponds to the `entityID` attribute of the `EntityDescriptor` element in the SAML metadata. At runtime, Azure AD adds the value to the `Audience` element of the SAML assertion, indicating the audience that is the expected destination of the assertion. Find the following value in the Oracle Access Manager metadata and enter that value:

```
<md:EntityDescriptor
…
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    ID="id-4TfauRP-ZeWyweEXkrqcBA0w0nRhe64hOPfnY2YR"
    cacheDuration="P30DT0H0M0S"
    entityID="http://myoamserver.mycompany.com:14100/oam/fed"
    validUntil="2029-03-19T21:13:40Z">
…
```

- **Reply URL (Assertion Consumer Service URL)** corresponds to the `Location` attribute of the `AssertionConsumerService` element in the SAML metadata. Be sure to pick the `Location` attribute that is relative to the HTTP_POST binding, as shown in the following example. The Reply URL is the SAML service endpoint in the federation partner that is expected to process the assertion.

```
<md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://myoamserver.mycompany.com/oam/server/fed/sp/sso"
index="1"/>
```

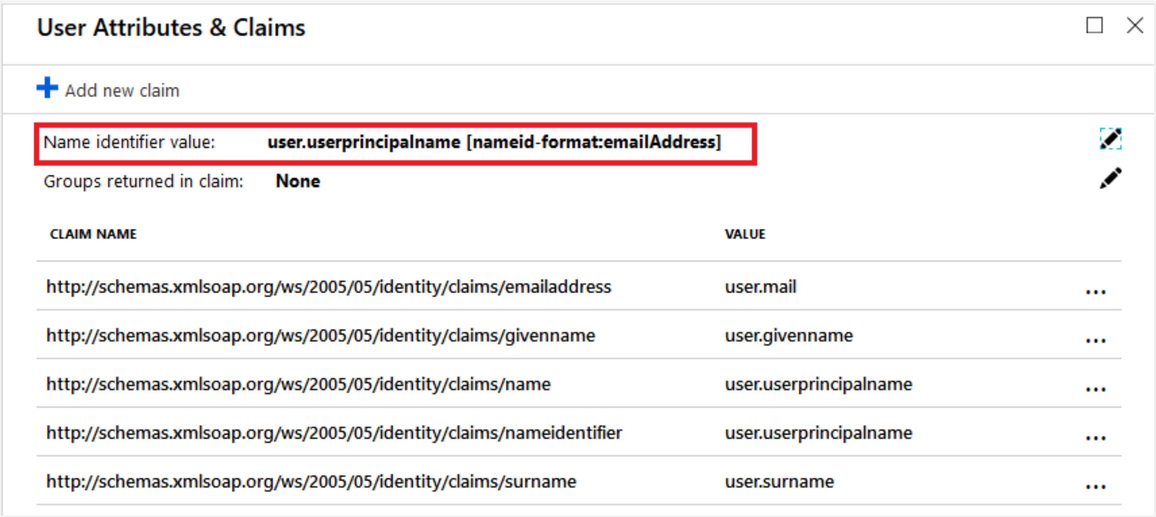
- The **Logout Url** corresponds to Oracle Access Manager's SAML logout endpoint. That value corresponds to the `Location` attribute of the `SingleLogoutService` element in Oracle Access Manager's SAML metadata. *This value is used exclusively in IdP-initiated logout flow.*

```
<md:SingleLogoutService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://myoamserver.mycompany.com/oamfed/sp/samlv20"
ResponseLocation="https://myoamserver.mycompany.com/oamfed/sp/samlv20"
/>
```

Note: The **Sign on URL** and **Relay State** properties aren't relevant to this scenario, so you can skip them.

9. In the **User Attributes and Claims** area, configure the user attributes that will be inserted in the SAML assertion and sent to Oracle Access Manager. For this scenario, it suffices to send some form of unique user identification.

   Leave the values as the default for the `Name identifier value: user.userprincipalname [nameid-format:emailAddress]` because `userprincipalname` is a unique attribute within Azure AD. The implication of such configuration is the need to import the `userprincipalname` value into the user entry in Oracle Access Manager's identity store (the LDAP server store).



User Attributes & Claims

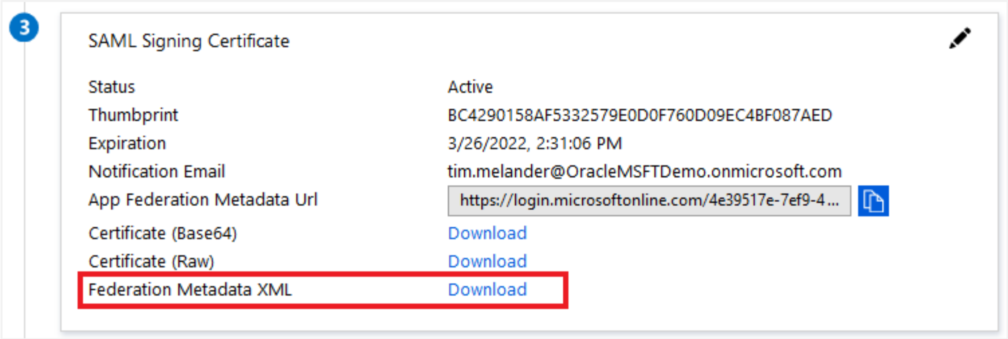
Name identifier value: **user.userprincipalname [nameid-format:emailAddress]**

Groups returned in claim: **None**

CLAIM NAME	VALUE
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname

Note: The properties **Groups returned in claim** and all the claims under **CLAIM NAME** aren't relevant to this scenario, so you can skip them.

10. In the **SAML Signing Certificate** area, click the **Download** link next to **Federation Metadata XML**, and save the file on your computer. You will use it later when configuring Oracle Access Manager as the service provider.



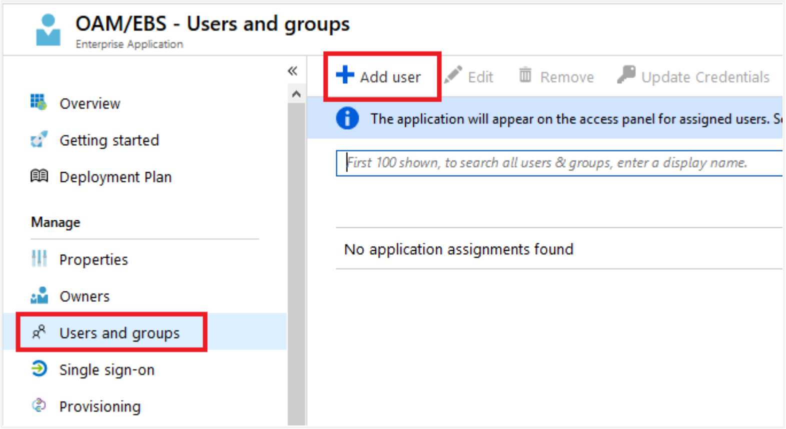
SAML Signing Certificate

Status	Active
Thumbprint	BC4290158AF5332579E0D0F760D09EC4BF087AED
Expiration	3/26/2022, 2:31:06 PM
Notification Email	tim.melander@OracleMSFTDemo.onmicrosoft.com
App Federation Metadata Url	https://login.microsoftonline.com/4e39517e-7ef9-4 ...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Assign Users to the Application

Only the users that you assign can log in to Azure AD after it receives an authentication request from the application.

1. From the Azure AD application that you created in the previous section, click **Users and groups**, and then click **Add user**.



OAM/EBS - Users and groups

Enterprise Application

The application will appear on the access panel for assigned users. S

First 100 shown, to search all users & groups, enter a display name.

No application assignments found

2. Select the **Users and groups: None Selected** option, and perform the following steps:

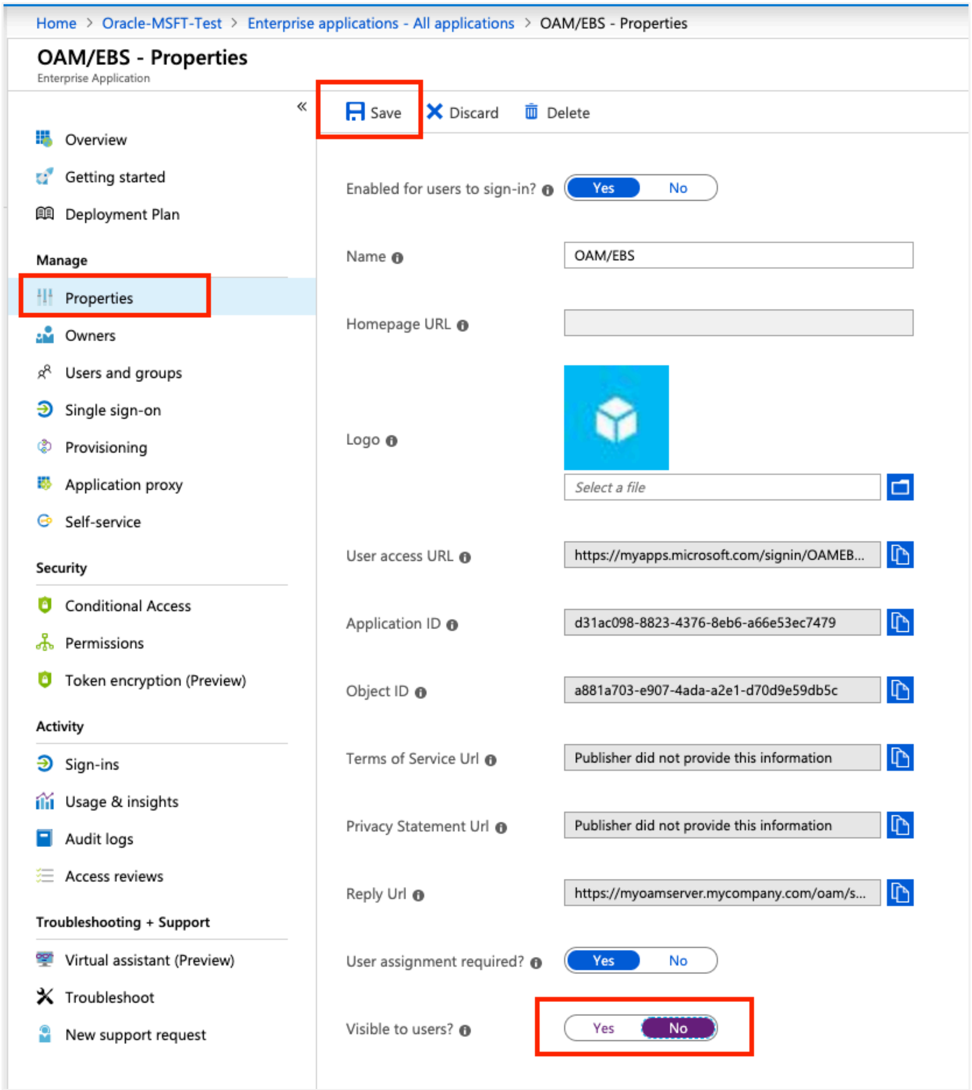
   A. In the **Select member or invite an external user** search box, enter the name of a user, and then press **Enter**.

   B. Select the user and then click **Select** to add the user.

   C. Click **Assign**.

   D. To add more users or groups, repeat these steps.

3. To prevent users from viewing this enterprise application that is meant only for SSO configuration, click **Properties**, change value of **Visible to users** to **No**, and click **Save**.



Enabled for users to sign-in? [✓ Yes] No

Name: OAM/EBS

Homepage URL:

Logo: Select a file

User access URL: https://myapps.microsoft.com/signin/OAMEB...

Application ID: d31ac098-8823-4376-8eb6-a66e53ec7479

Object ID: a881a703-e907-4ada-a2e1-d70d9e59db5c

Terms of Service Url: Publisher did not provide this information

Privacy Statement Url: Publisher did not provide this information

Reply Url: https://myoamserver.mycompany.com/oam/s...

User assignment required? [✓ Yes] No

Visible to users? Yes [✓ No]

Configure Oracle Access Manager for Federation with Azure AD

In this section, you create an identity provider partner to reference Azure AD.

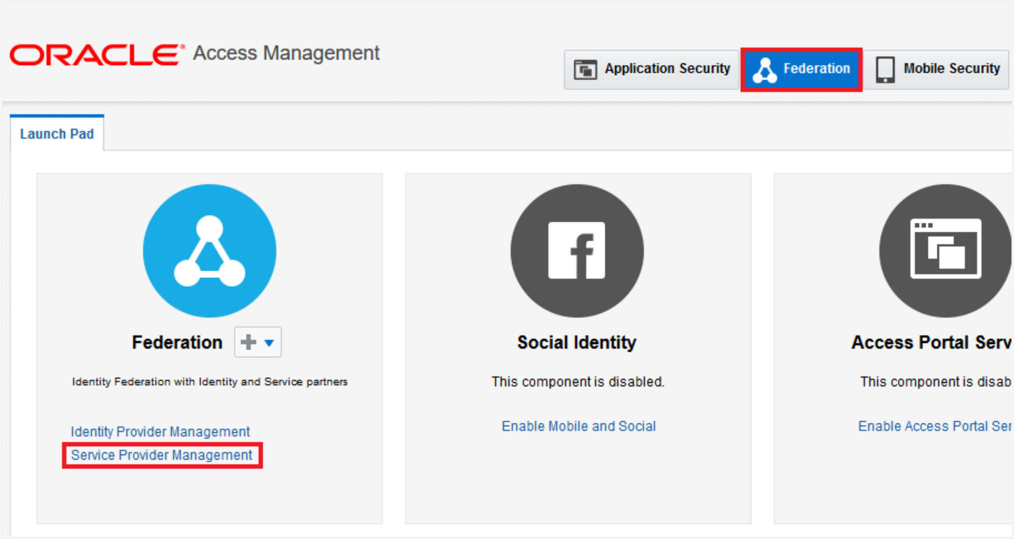
Create a New Identity Provider for Azure AD

This section assumes that Oracle Access Manager federation services have been enabled.

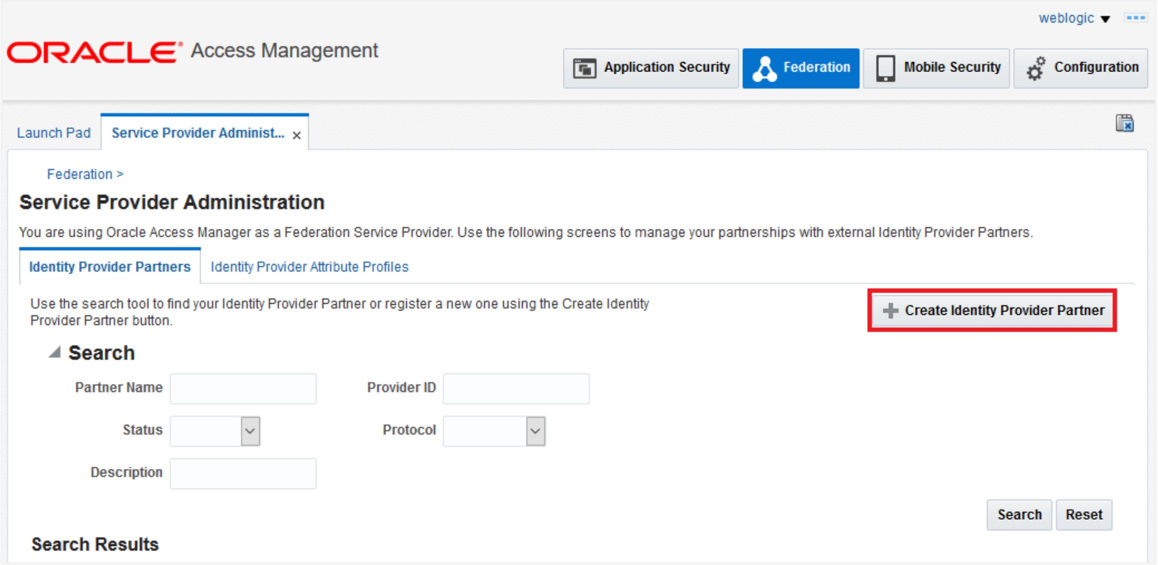
1. Sign to the Oracle Access Manager console as an Administrator.

2. Click the **Federation** tab at the top of the console.

3. In the **Federation** area of the **Launch Pad** tab, click **Service Provider Management.** For an explanation of why you select this option when creating an identity provider, see the OAM Federation: Identity Provider & Service Provider Management blog post.



4. On the **Service Provider Administration** tab, click **Create Identity Provider Partner.**



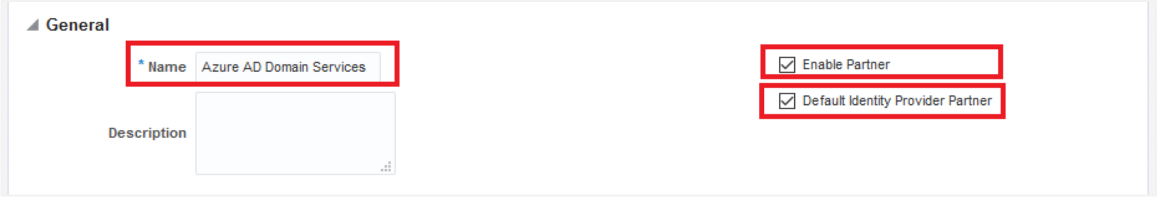
Service Provider Administration

You are using Oracle Access Manager as a Federation Service Provider. Use the following screens to manage your partnerships with external Identity Provider Partners.

Identity Provider Partners
Identity Provider Attribute Profiles

Use the search tool to find your Identity Provider Partner or register a new one using the Create Identity Provider Partner button.

5. In the **General** area, enter a name for the Identity Provider partner and select both the **Enable Partner** and **Default Identity Provider Partner** check boxes. Go to the next step before saving.



General

* Name: Azure AD Domain Services

Description:

☑ Enable Partner

☑ Default Identity Provider Partner

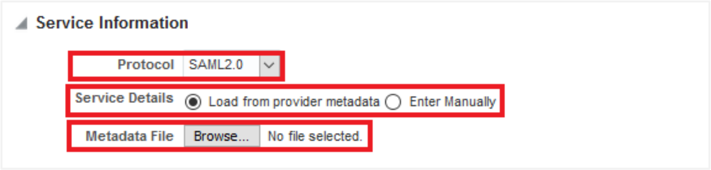
6. In the **Service Information** area:

   A. Select **SAML2.0** as the protocol.

   B. Select the **Load from provider metadata** option.

   C. Click **Browse** (for Windows) or **Choose File** (for Mac) and select the Azure AD SAML metadata file that you saved previously.

   D. Go to the next step before saving.



Service Information

Protocol: SAML2.0

Service Details: ● Load from provider metadata ○ Enter Manually

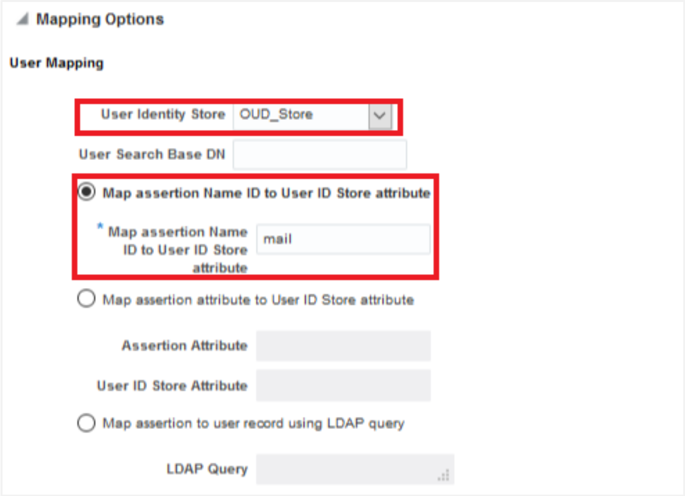
Metadata File: Browse... No file selected.

7. In the **Mapping Options** area:

   A. Select the **User Identity Store** option that will be used as the Oracle Access Manager LDAP identity store that is checked for E-Business Suite users. Typically, this is already configured as the Oracle Access Manager identity store.

   B. Leave the **User Search Base DN** field blank. The search base is automatically picked from the identity store configuration.

   C. Select the **Map assertion Name ID to User ID Store attribute** option and enter mail in the text box.



Mapping Options

User Mapping

User Identity Store: OUD_Store

User Search Base DN:

● Map assertion Name ID to User ID Store attribute

* Map assertion Name ID to User ID Store attribute: mail

○ Map assertion attribute to User ID Store attribute

Assertion Attribute:

User ID Store Attribute:

○ Map assertion to user record using LDAP query

LDAP Query:

Important: This configuration defines the user mapping between Azure AD and Oracle Access Manager. Oracle Access Manager will take the value of the NameID element in the incoming SAML assertion and try to look up that value against the mail attribute across all user entries in the configured identity store. Therefore, it's imperative that the Azure AD user principal name (in the Azure AD configuration shown previously) is synchronized with the `mail` attribute in Oracle Access Manager's identity store.

8. Click **Save** to save the identity provider partner.

9. After the partner is saved, come back to the **Advanced** area at the bottom of the tab. Ensure that the options are configured as follows:

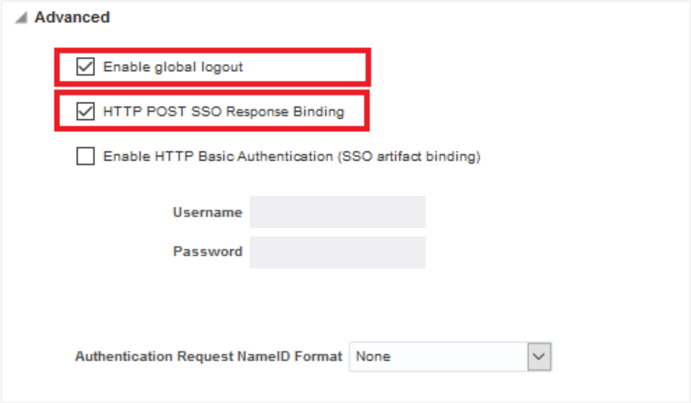
   - **Enable global logout** is selected.
   - **HTTP POST SSO Response Binding** is selected.

     This is an instruction that Oracle Access Manager sends in the authentication request telling Azure AD how it should transmit the SAML assertion back. If you inspect the authentication request that Oracle Access Manager sends, you would see something like the following example. Note the bold `ProtocolBinding` attribute of `AuthnRequest` element in the example.

```
<?xml version="1.0"?>
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
xmlns:enc="http://www.w3.org/2001/04/xmlenc#"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
Destination="https://login.microsoftonline.com/4e39517e-7ef9-45a7-
9751-6ef6f2d43429/saml2" ID="id-y5nmx61xB8QWXtDmYWcH7rPYs5zXtV-fcKRy-
yM9" IssueInstant="2019-04-23T17:01:25Z"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Version="2.0">
<saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">http://myoamserver.mycompany.com:14100/oam/fed</saml:Is
suer>
<dsig:Signature>
 <dsig:SignedInfo>
<dsig:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-
exc-c14n#"/>
<dsig:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<dsig:Reference URI="#id-y5nmx61xB8QWXtDmYWcH7rPYs5zXtV-fcKRy-yM9">
<dsig:Transforms>
<dsig:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<dsig:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
</dsig:Transforms>
<dsig:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<dsig:DigestValue>pa00UWdqfywm4Qb59HioA6BhD18=</dsig:DigestValue>
</dsig:Reference>
</dsig:SignedInfo>
<dsig:SignatureValue>X4eZRyFD6sznA0g3BJebU2c6ftunG2UvwbMptO+10wFky0aAL
nnr0Na+5fF83U4Ut99OvAIZ41K3YMNaR4A8zr37SSlBrb72X7CTtxjh2mAphWDRPmkJx4v
S0HACzZh0MHimdwq+qVXuFRbSLBE+9XNSGWJzGAh//WqGBlNrKnw=</dsig:SignatureV
alue>
</dsig:Signature>
</samlp:AuthnRequest>
```

- **Enable HTTP Basic Authentication (SSO artifact binding)** is *not* selected.

  This setting asks Azure AD to send the assertion via an HTTP POST request. When receiving a request like this, identity providers typically create an HTML form with the assertion as a hidden form element that is automatically posted to the service provider's Assertion Consumer Service (ACS).



Advanced

☑ Enable global logout

☑ HTTP POST SSO Response Binding

□ Enable HTTP Basic Authentication (SSO artifact binding)

Username

Password

Authentication Request NameID Format: None

10. In the **General** area, click the **Create Authentication Scheme and Module** button.

    An authentication scheme and module are created with the partner name. The only configuration left is attaching the authentication scheme to the E-Business Suite resources that require Azure AD credentials for authentication, which you will do in the next section.

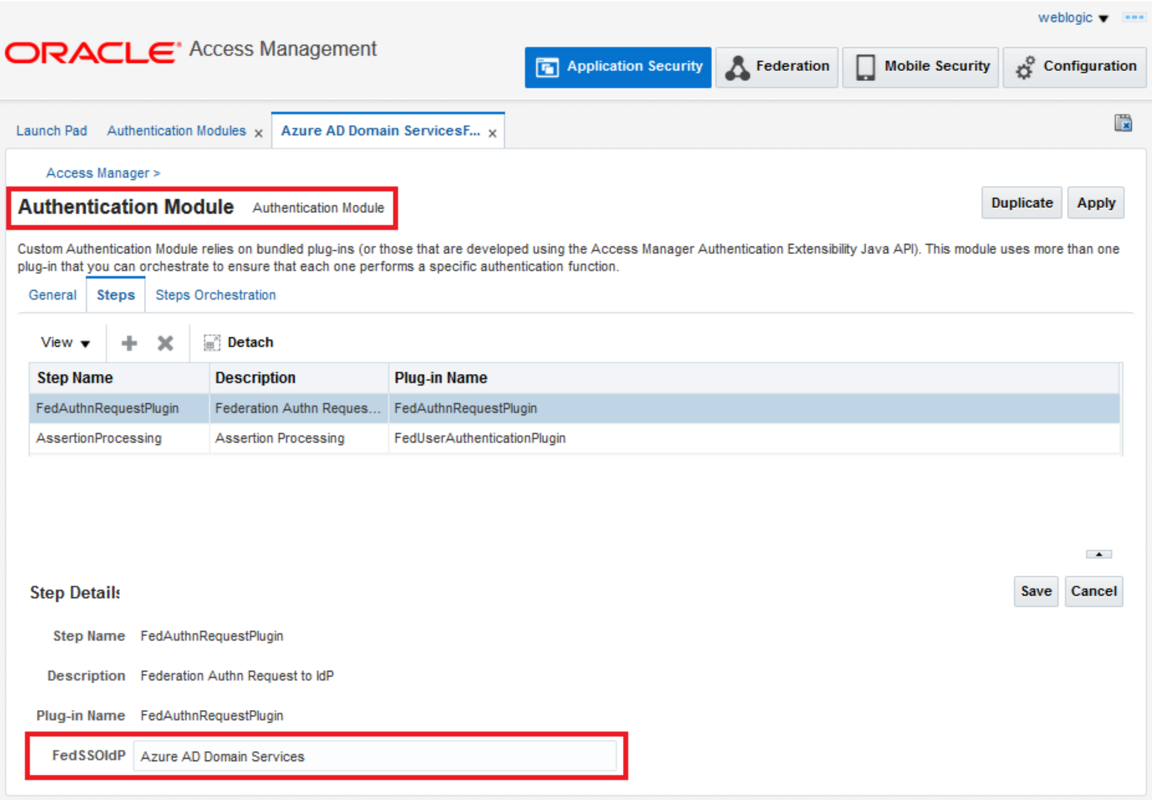
11. You can check the authentication module that was created by following these steps:

    A. Click the **Application Security** tab at the top of the console.

    B. Under **Plug-ins**, select **Authentication Modules**, click **Search**, and find your federation module.

    C. Select the module, and then click the **Steps** tab.

    D. Note that the value in the **FedSSOIdP** property is the identity provider partner.



Authentication Module Authentication Module

Custom Authentication Module relies on bundled plug-ins (or those that are developed using the Access Manager Authentication Extensibility Java API). This module uses more than one plug-in that you can orchestrate to ensure that each one performs a specific authentication function.

Step Name	Description	Plug-in Name
FedAuthnRequestPlugin	Federation Authn Reques...	FedAuthnRequestPlugin
AssertionProcessing	Assertion Processing	FedUserAuthenticationPlugin

Step Details

Step Name FedAuthnRequestPlugin

Description Federation Authn Request to IdP

Plug-in Name FedAuthnRequestPlugin

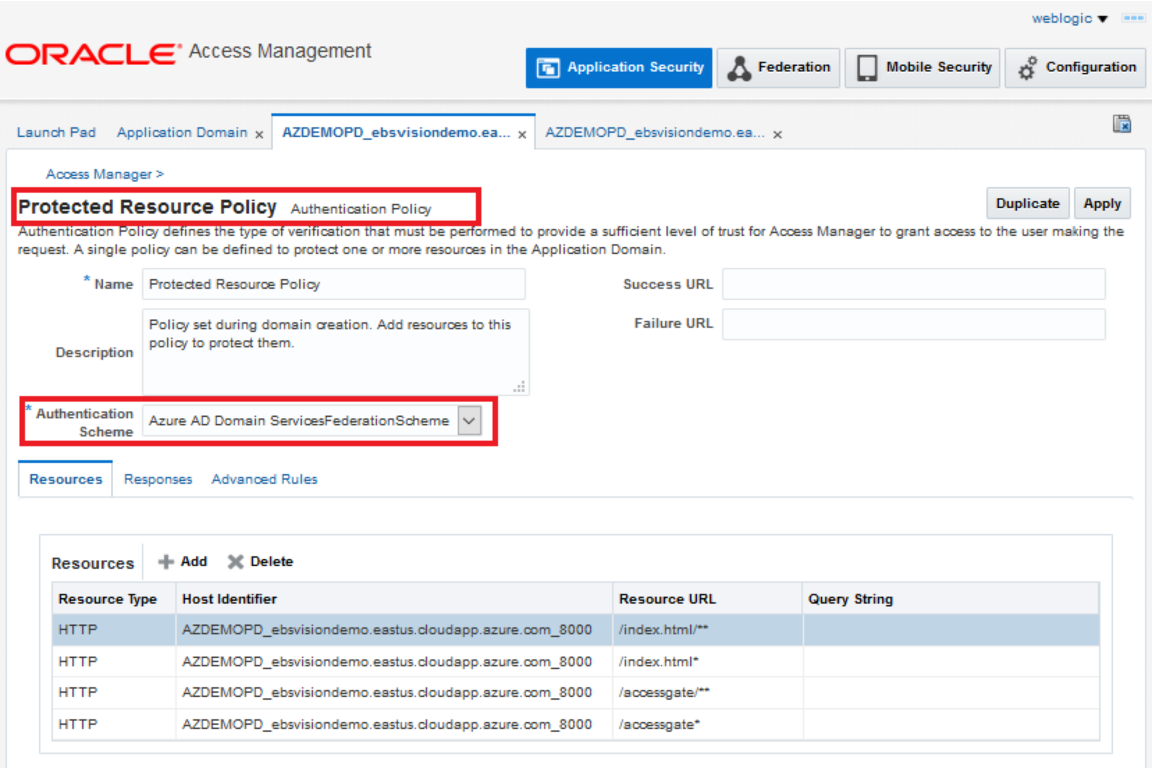
FedSSOIdP Azure AD Domain Services

Associate the E-Business Suite Resources with the Authentication Scheme

Perform these steps while logged in to the Oracle Access Manager console as an Administrator.

1. At the top of the console, click **Application Security**.
2. Under Access Manager, select **Application Domain**, click **Search**, and select the application domain that was created during E-Business Suite script execution for the integration that would have registered the E-Business Suite WebGate.
3. Click the **Authentication Policies** tab, and then click **Protected Resources Policy**.

   Change the **Authentication Scheme** by changing the previously created authentication scheme with the new federation authentication scheme. This is how Oracle Access Manager ties a protected resource to an identity provider.



Protected Resource Policy Authentication Policy

Authentication Policy defines the type of verification that must be performed to provide a sufficient level of trust for Access Manager to grant access to the user making the request. A single policy can be defined to protect one or more resources in the Application Domain.

* Name	Protected Resource Policy	Success URL	
Description	Policy set during domain creation. Add resources to this policy to protect them.	Failure URL	
* Authentication Scheme	Azure AD Domain ServicesFederationScheme		

Resources

Resource Type	Host Identifier	Resource URL	Query String
HTTP	AZDEMOPD_ebsvisiondemo.eastus.cloudapp.azure.com_8000	/index.html/**	
HTTP	AZDEMOPD_ebsvisiondemo.eastus.cloudapp.azure.com_8000	/index.html*	
HTTP	AZDEMOPD_ebsvisiondemo.eastus.cloudapp.azure.com_8000	/accessgate/**	
HTTP	AZDEMOPD_ebsvisiondemo.eastus.cloudapp.azure.com_8000	/accessgate*	

4. Click **Apply** to save the change.

Testing Federated Login and Logout

This section provides simple steps to verify that federation authentication works when initiated from the service provider (SP) and the identity provider (IDP). The steps in this section assume that a user has been created in Azure AD and has been provisioned to the Oracle Access Manager LDAP server and the E-Business Suite database.

Test SP-Initiated Login and Logout

1. In a browser, enter `https://<ebs_portal_hostname>:<port>/OA_HTML/OA.jsp?OAFunc=OAHOMEPAGE`.

2. When Azure AD prompts you for a username or to pick an account, enter the username.

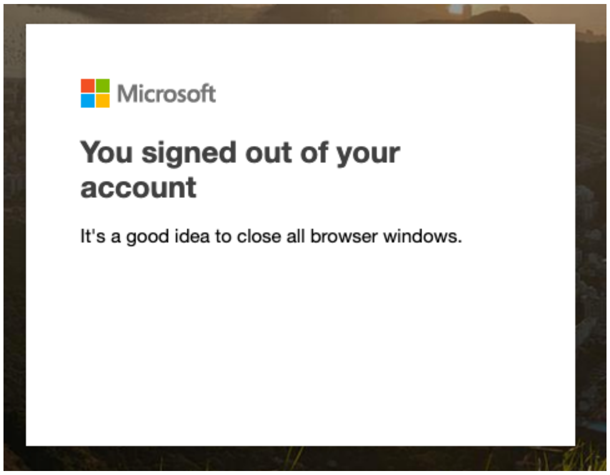
3. When you are prompted for a password, enter it and click **Sign in**.

4. If you are prompted to **Stay signed in?**, click **Yes**.

   If the login is successful, you are redirected to the E-Business Suite home page using your user credentials stored in Azure AD.

5. To log out, click the power button icon in the top-right corner of the E-Business Suite portal.

   You are redirected to the Oracle Access Manager host, your session is cleared, and a signed-out message appears.

   Microsoft

   You signed out of your account

   It's a good idea to close all browser windows.

Test IDP-Initiated Login and Logout

1. In a browser, enter `https://<azure_portal_hostname>/`.

2. When Azure AD prompts you for a username or to pick an account, enter the username.

3. When you are prompted for a password, enter it and click **Sign in**.

4. If you are prompted to **Stay signed in?**, click **Yes**.

   You are directed to your home page.

5. Click the E-Business Suite application icon.

   You are redirected to the E-Business Suite portal.

6. To log out of E-Business Suite, click the power button icon in the top-right corner of the portal.

   You are redirected to the Oracle Access Manager host, your session is cleared, and a signed-out message appears.

Known Issue

IDP-initiated logout doesn’t clear all sessions: There is a known problem when you try to log out in an IDP-initiated flow. Azure AD applies a transformation on the `NameID` value that it sent in the SAMLResponse when SSO was initially started. When you try to log out, the values between the authenticated user and the user in the logout request don’t match and logout fails. This issue is should be resolved later this year.

Conclusion

This paper provides the integration steps needed to federate SSO with Oracle E-Business Suite and Azure AD using Oracle Access Manager. In particular, it discusses three critical user attributes that are important to the authentication flow. As such, planning and designing the provisioning details, along with end-to-end testing, are important for this solution to work. The use of UPN in Azure is a recommendation, but how you design provisioning to the Oracle Access Manager LDAP server could be different. The important point is that all three critical attributes should be considered; design your provisioning requirements as needed for your enterprise.

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

- blogs.oracle.com/oracle
- facebook.com/oracle
- twitter.com/oracle
- oracle.com

Integrated Cloud Applications & Platform Services

Deploy Oracle E-Business Suite Across Oracle Cloud Infrastructure and Azure: SSO with Oracle Access Manager and Azure Active Directory
June 2019
Author: Tim Melander (Oracle) and Andre Correa (Oracle)