Microsoft Azure + ORACLE

Deploy Oracle Retail Merchandising Suite Across Oracle Cloud Infrastructure and Azure

SSO with Oracle Access Manager and Azure Active Directory

WHITE 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 white paper since its initial publication:

Date	Revision
June 7, 2019	Initial publication

You can find the most recent versions of the Oracle Cloud Infrastructure white papers at https://cloud.oracle.com/iaas/technical-resources.

Table of Contents

Overview

Oracle recognizes that many factors influence a retailer’s move to the cloud. A single cloud provider is not always an option for retailers. Oracle Retail has partnered with Microsoft to create a reference architecture that splits Oracle Retail Merchandising Suite version 16.0.2 and later components between Oracle Cloud Infrastructure and Microsoft Azure. Using both clouds gives customers added flexibility as they move to the cloud.

This cross-cloud solution for Retail Merchandising Suite places the database tier on Oracle Cloud Infrastructure and the middleware tier, F tier (firewall, proxies, and load balancer), and DS tier on Microsoft Azure. Additionally, this architecture uses Azure Active Directory (Azure AD) as the federated identity provider (IDP) to authenticate a user to the Retail Merchandising Suite, while Oracle Access Manager is the service provider (SP).

The following Merchandising applications are configured in a highly available, active-active clustered environment in the cross-cloud model:

- Oracle Retail Merchandising System (RMS)
- Oracle Retail Invoice Matching (ReIM)
- Oracle Retail Allocation
- Oracle Retail Sales Audit (ReSA)
- Oracle Retail Price Management (RPM)

The following Retail Integration Suite applications are certified to run on a single-node in the cross-cloud model:

- Retail Integration Bus (RIB)
- Retail Service Bus (RSB)
- Java Messaging Service (JMS)
- Integration Gateway Services (IGS)
- Retail Service-Oriented Architecture Enabler (RSE)
- RIB Hospital Administration (RIHA)

This document provides high-level instructions for installing the Retail Merchandising Suite in the cross-cloud model and configuring SAML 2.0 federated single sign-on (SSO) with Azure AD, through Oracle Access Manager. A general understanding of Oracle Retail Merchandising cross-cloud architecture is necessary to understand this authorization integration.

Retail Merchandising Suite Cross-Cloud Architecture

This section describes both the logical and physical architecture of the Retail Merchandising Suite in the cross-cloud solution.

Logical Architecture

The Retail Merchandising Suite consists of the following functional components:

- Retail Merchandising System is used to run core merchandising activities, including merchandise management, inventory replenishment, purchasing, vendor management, and financial tracking.
- Retail Price Management is a pricing and promotions system that lets retailers define, maintain, and review price changes, clearances, and promotions.
- Retail Allocation helps retailers determine the inventory requirements at the item, store, and week level by using real-time inventory information.
- Retail Invoice Matching supports the verification of merchandise invoice costs, quantities, and taxes before payment.
- Retail Integration Suite consists of applications to support message, service, and bulk integration.

The Retail Merchandising Suite reference architecture consists of the following logical tiers:

- **Web tier:** Oracle ADF-based UIs that are accessible from a web browser
- **Application tier:**
  - Retail Merchandising Suite applications
  - Retail Integration Suite (including Retail Integration Bus, Retail Service Bus, and Retail Bulk Data Integration)
  - Identity Management through Oracle's Identity Management stack (Oracle Access Manager, Oracle Identity Manager, and Oracle Internet Directory)
  - Connections for transferring files with SFTP and other integrations
- **Data tier:** Merchandising and Integration Pluggable DBs on an Oracle RAC Database

Figure 1 illustrates this logical architecture.

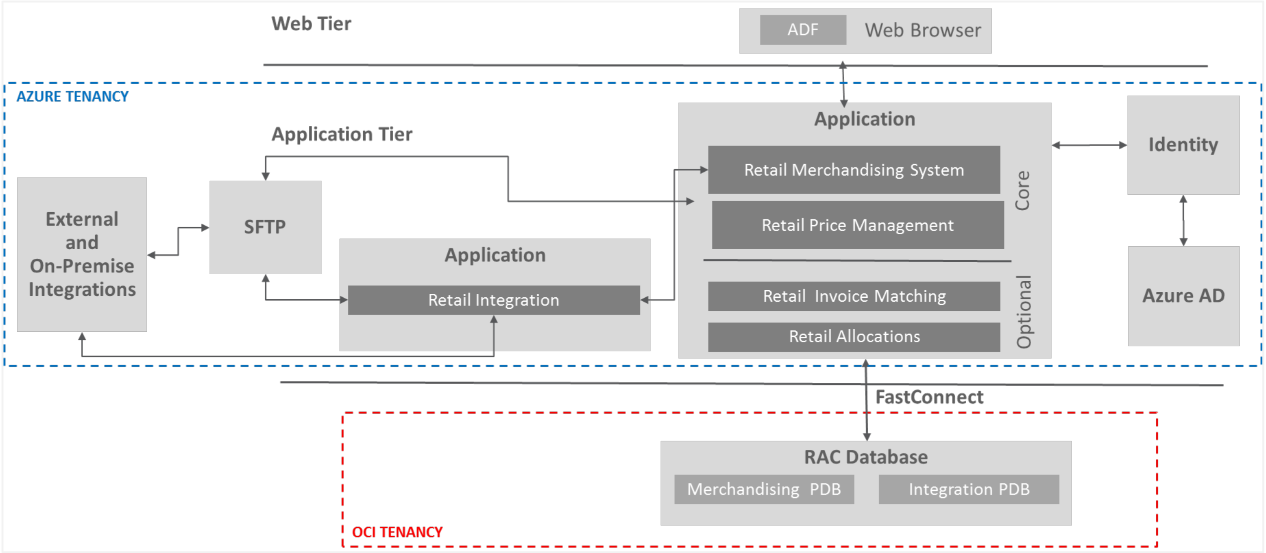


Figure 1. High-Level Logical Architecture

Physical Architecture

At a high level, the cross-cloud model lets retailers deploy their data tier in Oracle Cloud Infrastructure and their application tier in Microsoft Azure. The reference architecture clusters database and compute nodes to produce a highly scalable, highly available architecture. FastConnect between Oracle Cloud Infrastructure and Azure ensures reliable performance that meets SLAs.

The supported reference architecture deploys the tiers as follows:

- Database tier on Oracle Cloud Infrastructure (OCI)
- Middleware tier (with a high-performance network file system) on Azure
- F tier (firewall, proxies, and load balancer) on Azure
- DS tier (SFTP) on Azure

Figure 2 illustrates this physical architecture.

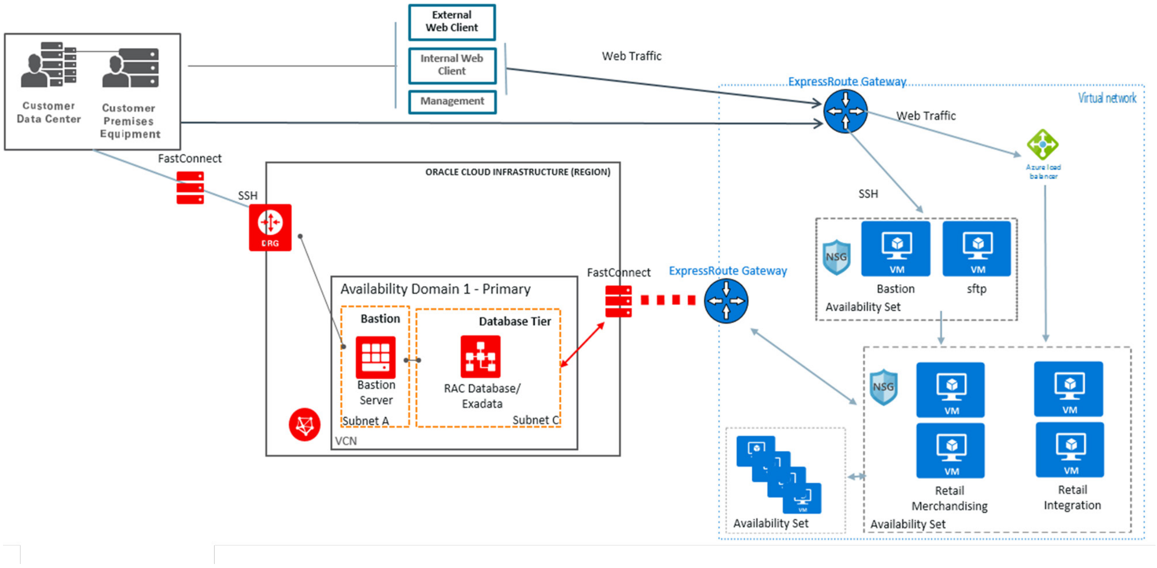


Figure 2. High-Level Physical Architecture

Authentication and Authorization Architecture

The authentication and authorization architecture is based on an integration between Oracle Access Manager and Retail Merchandising Suite. Oracle Access Manager requires the backend LDAP store to be Oracle Unified Directory or Oracle Internet Directory. In this architecture, the system of record for users is Azure AD. Oracle Directory Integration Platform, used as a bi-directional synchronization service, synchronizes that account to Oracle Internet Directory.

Figure 3 illustrates this authentication and authorization architecture.

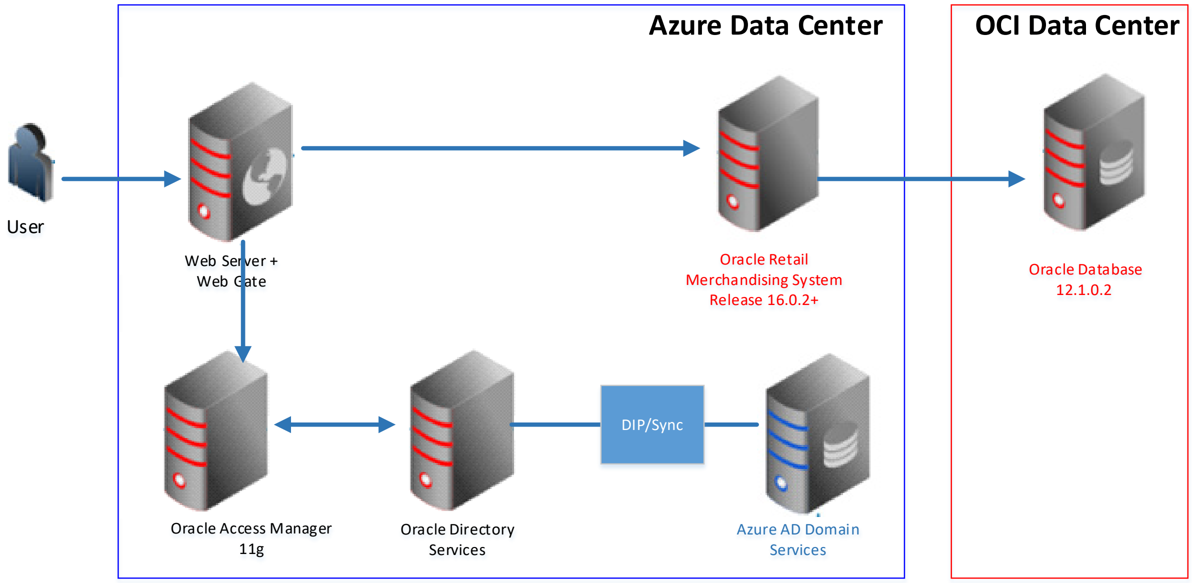


Figure 3. High-Level Authentication and Authorization Architecture

Oracle has verified and supports this cross-cloud deployment architecture for Retail Merchandising Suite 16.0.2 and later, including federated SSO through the processes described in this document.

Merchandising Suite Installation Overview

This section provides high-level information about installing Retail Merchandising Suite to use the cross-cloud model.

Prerequisites

To use the cross-cloud reference architecture, retailers must meet the following requirements:

- Software licenses for Retail Merchandising Suite version 16.0.2 or later
- Capacity and software requirements as described in the next section

Components

For a complete list of requirements and information about installing each individual application, see the 16.0.2 application installation guides.

REQUIRED COMPONENTS

Server Type	Description
Database software	Oracle Database Enterprise Edition 12cR1 (12.1.0.2)
Database hardware (Oracle Cloud Infrastructure location) **Note:** Perform a full capacity-planning exercise to determine if more database capacity or storage is required for your retail enterprise workloads.	2-node RAC DB system or Exadata DB system sized appropriately to the retailer's volumes (minimum 8 VCPU and 60-GB RAM)
Middleware software	Oracle Fusion Middleware 12.2.1.3.0 **Components:** • FMW 12.2.1.3.0 Infrastructure (WLS and ADF included) • Oracle Enterprise Manager Fusion Middleware Control 12.2.1.3.0 • BI Publisher 12.2.1.3.0 for legacy reports • Oracle Identity Management 11g Release 1 (11.1.1.9) **Java:** JDK 1.8+ 64 bit **Single sign-on (SSO):** • Oracle Web Tier (12.2.1.3.0) • Oracle Access Manager 11g Release 2 (11.1.2.3) Oracle Access Manager Agent (WebGate) 11g Release 2 (11.1.2.3)
Minimum middleware hardware (Azure location) **Note:** Perform a full capacity-planning exercise to determine if more database capacity or storage is required for your retail enterprise workloads.	• Four 2-node Cluster Azure Compute and 300-GB Storage for Retail Merchandising and Retail Integration applications • Four 2-node Cluster Azure Compute and 300-GB Storage for BI and IDM components • One VS Azure Compute for SFTP server

Database Installation

The Retail Merchandising and Retail Integration applications have been validated against a 12.1.0.2 RAC database on Oracle Cloud Infrastructure.

Installing the Merchandising Database

The Merchandising release contains an installer package that is used to install the database objects for the Merchandising applications.

1. Extract the `rms16installer.zip` file in a staging directory, and verify that the required Merchandising tablespaces and schemas are created.

2. Ensure that the shared NFS is mounted across the cluster nodes to install the Merchandising database in silent mode.

3. Create a wallet in the RETAIL_HOME path with all of the required aliases to be used in the `ant.install.properties` file.

4. Export the Oracle environment variables (ORACLE_HOME, ORACLE_SID, PATH, and so on).

5. Run the `install.sh` script to start the installer in silent mode. For example:

   ```
   ./install.sh silent
   ```

Installing the Retail Integration Database

Create the required user schemas to install the Retail Integration Bus applications and grant necessary permissions.

Applications Installation

The Retail Merchandising System is deployed on a WebLogic cluster in Azure. Requests from the load balancer pass through the Oracle HTTP web server hosted on each clustered node and are proxied to the active-active horizontal WebLogic cluster.

This section assumes that all middleware software has been installed as required in Azure.

Installing the Merchandising Applications

1. Create a WebLogic domain for each Merchandising and Retail Integration application and configure SSL certificates for secure communication. Configure the Oracle Internet Directory provider in the WebLogic domain, and load required LDIF files for authenticating application requests.

2. Configure Oracle Access Manager with the Oracle HTTP server for single sign-on authentication.

3. Extract the installer zip file for each Merchandising and Retail Integration application into the respective application staging directory on the shared NFS mounted across cluster nodes.

4. Create a wallet in the RETAIL_HOME path for each application with all of the required aliases to be used in the `ant.install.properties` file.

5. Set the environment variables (J2EE_ORACLE_HOME, J2EE_DOMAIN_HOME, JAVA_HOME, and so on).

6. Run the `install.sh` script to start the application installers in silent mode.

7. Verify that application SSO URLs are accessible through load balancer IP addresses over secure communication.

Installing Retail Integration Applications

The Retail Integration applications are deployed to a WebLogic server in Azure.

1. Extract the Retail Integration applications in a staging directory on the file system.

2. Modify the `properties` files under the `conf` directory with the appropriate environment information.

3. Compile and set up security wallets by using the shell scripts available in the `bin` directory.

4. Deploy the Retail Integration applications (RIB, RSB, JMS, IGS, RSE, and RIHA) on each WebLogic server.

5. Configure the Oracle Internet Directory provider in the WebLogic domain, and load the required LDIF files for authenticating application requests.

6. Verify that the application SSO URLs are accessible through load balancer IP addresses over secure communication.

Integrating Oracle Access Manager and Azure AD for Retail Merchandising

This section describes how to configure Oracle Access Manager and Azure AD to support federated SSO for Retail Merchandising.

SSO with Oracle Access Manager and Azure AD

Retail Merchandising uses Oracle Access Manager for authorization (AuthZ). For more information about Retail Merchandising integration with Oracle Access Manager, see the Retail documentation.

Oracle Access Manager itself delegates authentication (AuthN) to a backend LDAP store. In this architecture, that store is Oracle Internet Directory. However, the system of record for users is Azure AD. Oracle Directory Integration Platform serves as a bridge between Oracle Internet Directory and Azure AD by synchronizing user information from Azure AD to Oracle Internet Directory. This synchronization allows Oracle Internet Directory to continue to act as the backing store for Oracle Access Manager, which in turn allows the existing integration between Oracle Access Manager and Retail Merchandising to function as in all other deployment models. In this cross-cloud model, Azure AD performs authentication and Oracle Access Manager performs authorization.

Provisioning Critical User Attributes

Following Azure AD best practices, the user principal name (UPN) is used as the federated user mapping attribute value. The UPN provides a reliable unique value for signing on to the user account and matching in Oracle Access Manager. 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. A password doesn't need to be provisioned.

RECOMMENDED MINIMUM USER ATTRIBUTES TO SYNCHRONIZE

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

Understanding the Federation Flow

In this scenario, users access Retail Merchandising applications 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). Because Oracle Access Manager is deployed in front of Retail Merchandising Suite for SSO, it’s also the component that provides the federation capabilities. This section provides the required steps for implementing identity federation between Azure AD and Oracle Access Manager.

The primary use case is a federation flow that is initiated on access to a Retail Merchandising Suite endpoint. As shown in Figure 4, the Oracle Access Manager server (OAM Server) detects access to Retail Merchandising, 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 back 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.

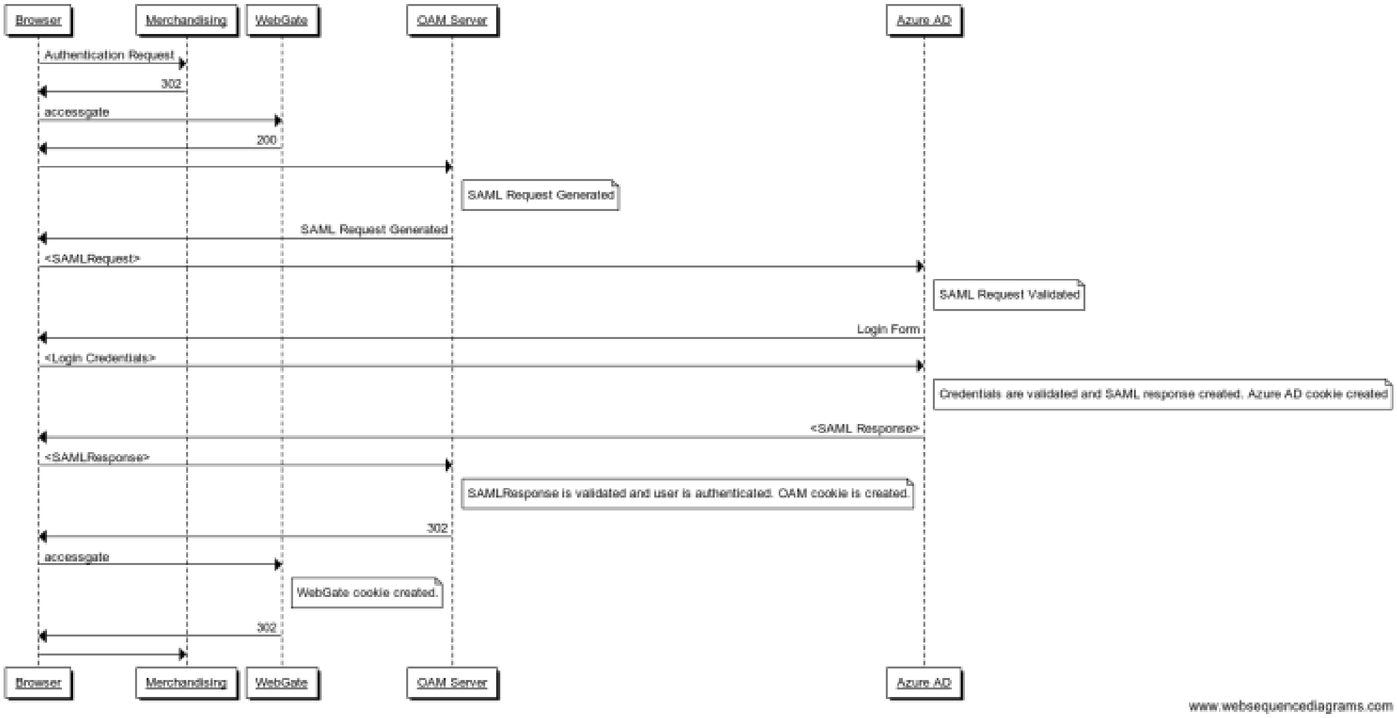
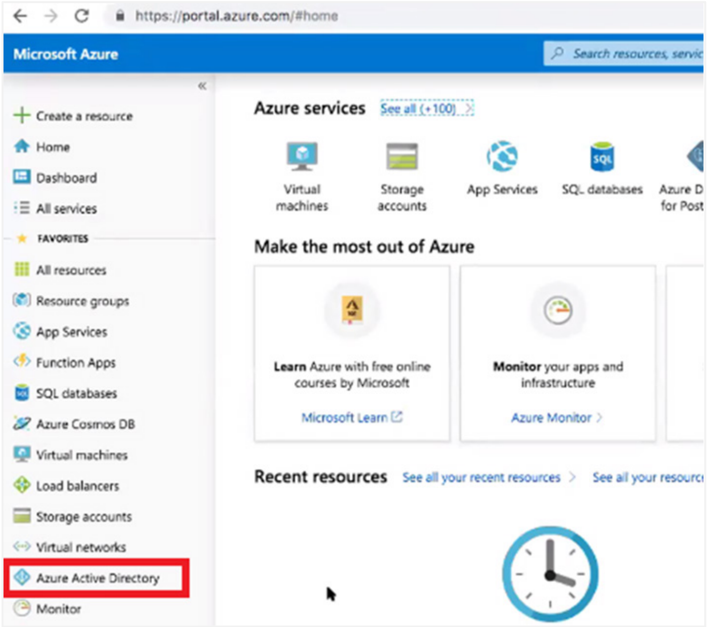


Figure 4. Federation Flow

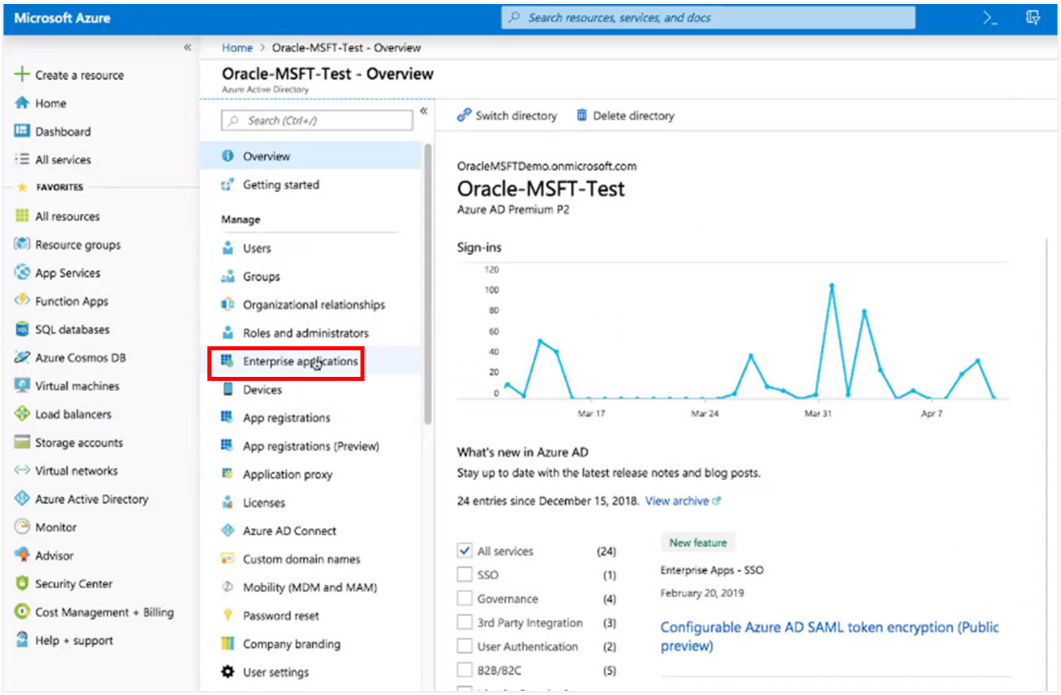
Configuring Azure AD as the Identity Provider

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

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



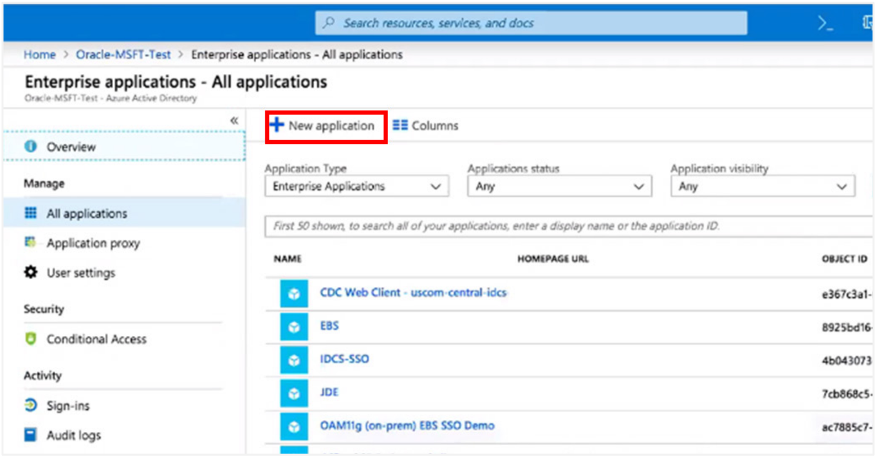
3. In the Azure Active Directory pane, click **Enterprise applications**.



Stay up to date with the latest release notes and blog posts.

24 entries since December 15, 2018. View archive

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
Overview
Manage
All applications
Application proxy
User settings
Security
Conditional Access
Activity
Sign-ins
Audit logs
New application
Columns

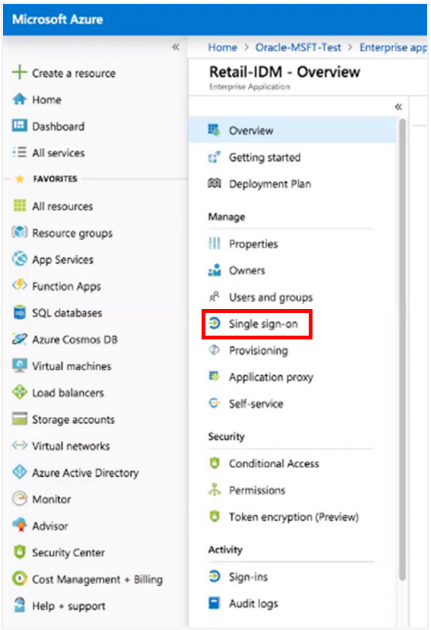
Application Type: Enterprise Applications
Applications status: Any
Application visibility: Any

First 50 shown, to search all of your applications, enter a display name or the application ID.

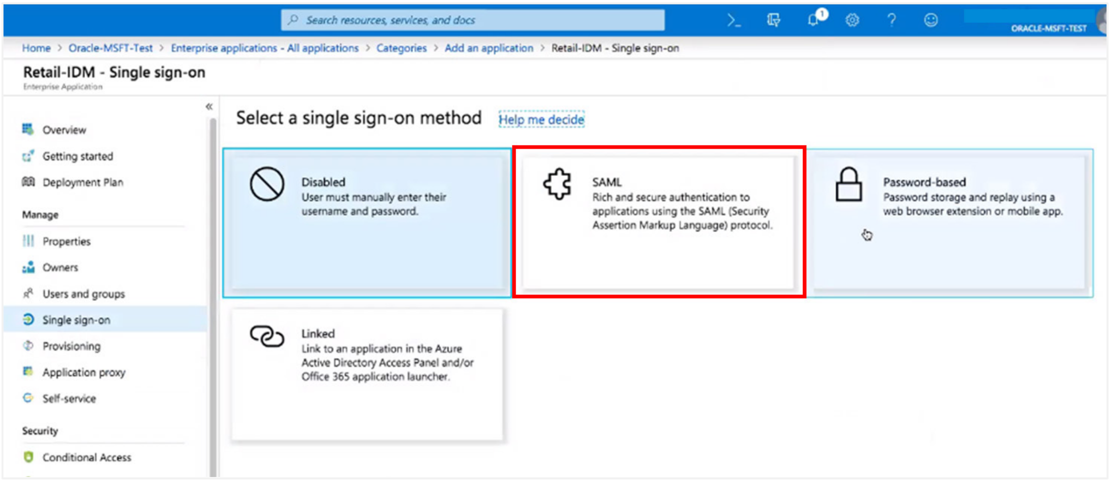
NAME	HOMEPAGE URL	OBJECT ID
CDC Web Client - uscom-central-idcs		e367c3a1-
EBS		8925bd16-
IDCS-SSO		4b043073
JDE		7cb868c5-
OAM11g (on-prem) EBS SSO Demo		ac7885c7-

5. In the **Add from the gallery** section, type **Retail-IDM** in the search box, and then click **Add**.

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



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



Select a single sign-on method

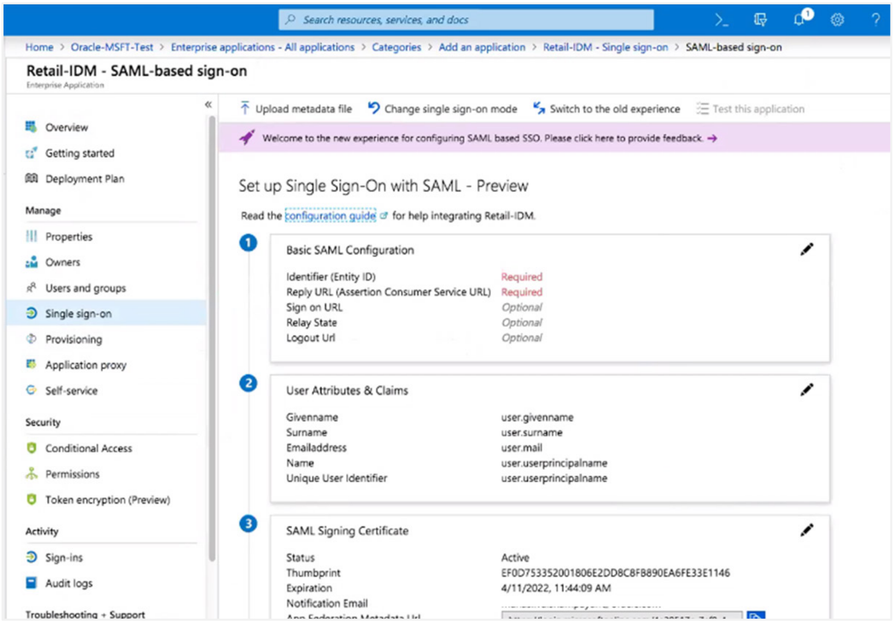
Disabled
User must manually enter their username and password.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Password-based
Password storage and replay using a web browser extension or mobile app.

Linked
Link to an application in the Azure Active Directory Access Panel and/or Office 365 application launcher.

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


Search resources, services, and docs
Home > Oracle-MSFT-Test > Enterprise applications - All applications > Categories > Add an application > Retail-IDM - Single sign-on > SAML-based sign-on
Retail-IDM - SAML-based sign-on
Enterprise Application
Overview
Getting started
Deployment Plan
Manage
Properties
Owners
Users and groups
Single sign-on
Provisioning
Application proxy
Self-service
Security
Conditional Access
Permissions
Token encryption (Preview)
Activity
Sign-ins
Audit logs
Troubleshooting + Support
Upload metadata file
Change single sign-on mode
Switch to the old experience
Test this application

Welcome to the new experience for configuring SAML based SSO. Please click here to provide feedback. →

Set up Single Sign-On with SAML - Preview

Read the configuration guide for help integrating Retail-IDM.

1 Basic SAML Configuration

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Optional
Relay State	Optional
Logout Url	Optional

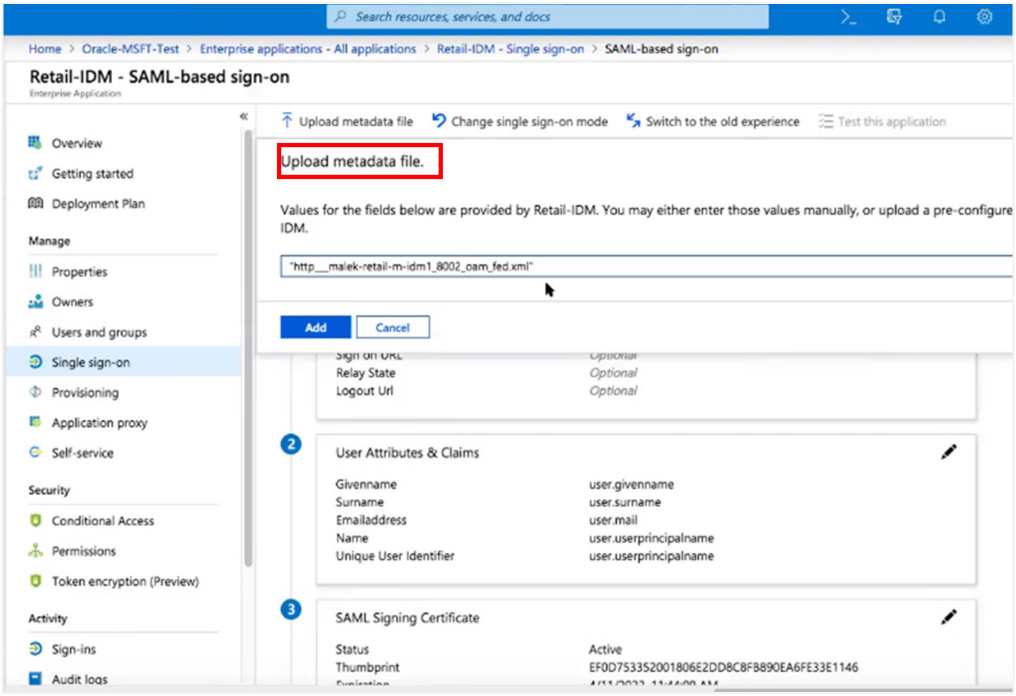
2 User Attributes & Claims

Givenname	user.givenname
Surname	user.surname
Emailaddress	user.mail
Name	user.userprincipalname
Unique User Identifier	user.userprincipalname

3 SAML Signing Certificate

Status	Active
Thumbprint	EF0D753352001806E2DD8C8FB890EA6FE33E1146
Expiration	4/11/2022, 11:44:09 AM
Notification Email	

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. One option is to upload this metadata into Azure AD, by clicking **Upload metadata file**.



Retail-IDM - SAML-based sign-on

Enterprise Application

Upload metadata file.

Values for the fields below are provided by Retail-IDM. You may either enter those values manually, or upload a pre-configure IDM.

"http__malek-retail-m-idm1_8002_oam_fed.xml"

Sign on URL	Optional
Relay State	Optional
Logout Url	Optional

User Attributes & Claims

Givenname	user.givenname
Surname	user.surname
Emailaddress	user.mail
Name	user.userprincipalname
Unique User Identifier	user.userprincipalname

SAML Signing Certificate

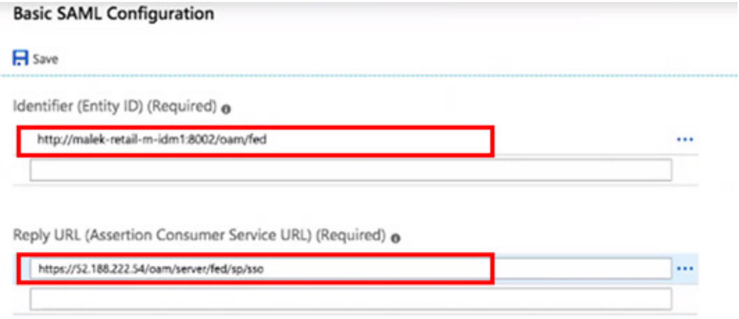
Status	Active
Thumbprint	EF0D753352001806E2DD8C8FB890EA6FE33E1146
Expiration	4/11/2022 11:44:00 AM

8. In the Basic SAML Configuration area, the **Identifier (Entity ID)** and **Reply URL (Assertion Consumer Service URL)** fields require values. If you uploaded the SAML metadata XML, the values are entered automatically. If not, enter them manually.

    - **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 ……… entityID="http://....../>
      ```

    - **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. The Reply URL is the SAML service endpoint in the federation partner that is expected to process the assertion.



Basic SAML Configuration

Save

Identifier (Entity ID) (Required)

http://malek-retail-m-idm1:8002/oam/fed

Reply URL (Assertion Consumer Service URL) (Required)

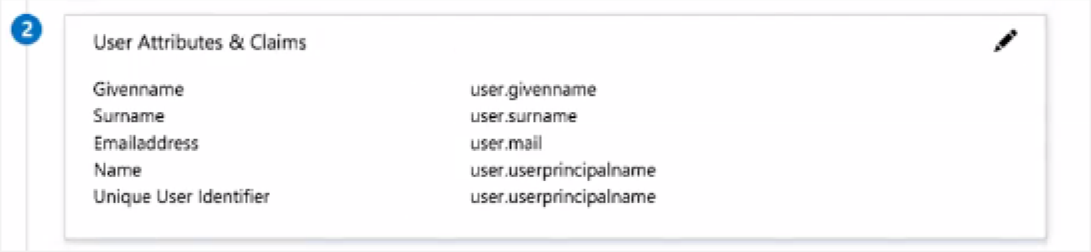
https://52.188.222.54/oam/server/fed/sp/sso

Note: The **Sign on URL**, **Relay State**, and **Logout Url** 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).



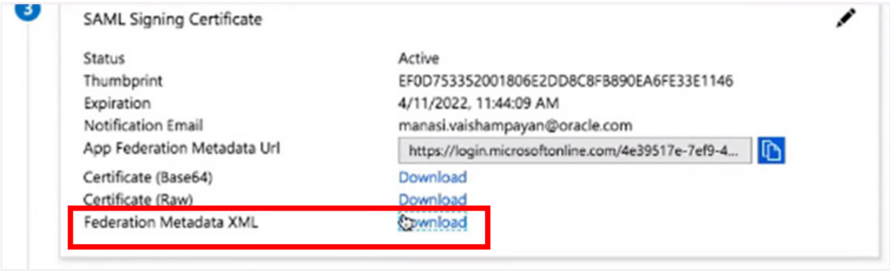
User Attributes & Claims

Givenname	user.givenname
Surname	user.surname
Emailaddress	user.mail
Name	user.userprincipalname
Unique User Identifier	user.userprincipalname

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.



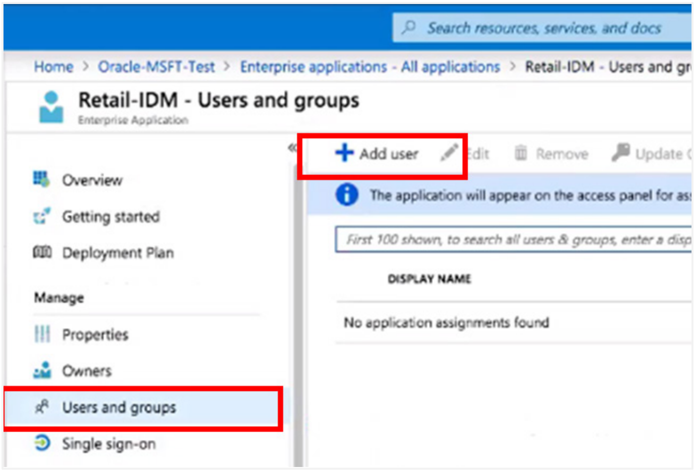
SAML Signing Certificate

Status	Active
Thumbprint	EF0D753352001806E2DD8C8FB890EA6FE33E1146
Expiration	4/11/2022, 11:44:09 AM
Notification Email	manasi.vaishampayan@oracle.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 Oracle Access Manager for Retail Merchandising

Only the users that you assign can log in to Azure AD after it receives an authentication request from Oracle Access Manager for Retail Merchandising.

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



Search resources, services, and docs
Home > Oracle-MSFT-Test > Enterprise applications - All applications > Retail-IDM - Users and gr
Retail-IDM - Users and groups
Enterprise Application
Add user
Edit
Remove
Update
Overview
Getting started
Deployment Plan
Manage
Properties
Owners
Users and groups
Single sign-on
DISPLAY NAME

The application will appear on the access panel for as

First 100 shown, to search all users & groups, enter a disp

No application assignments found

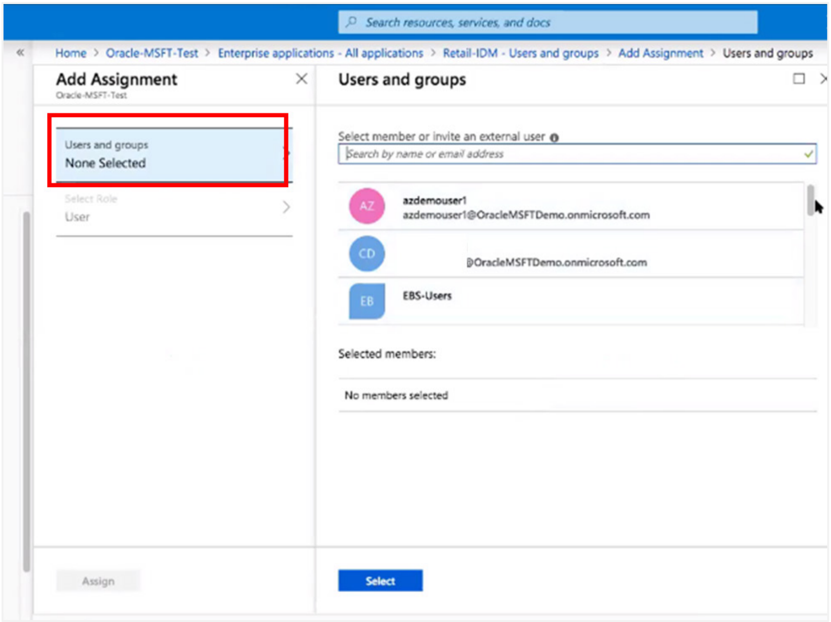
2. Select the **Users and groups: None Selected** option, and the perform the following steps:

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

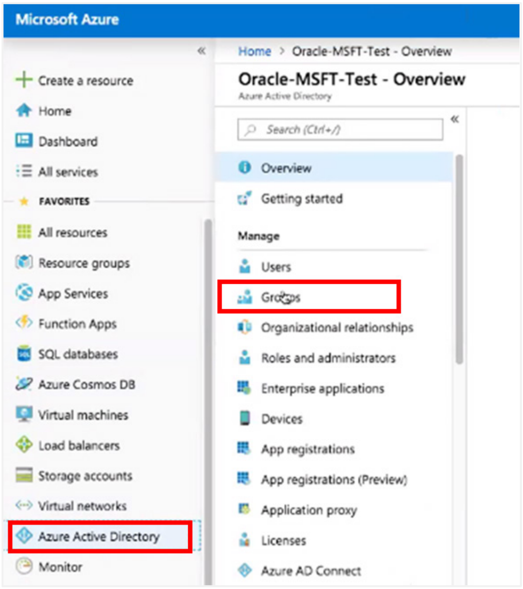
   B. Select the user and then click **Select** to add the user.

   C. Click **Assign**.

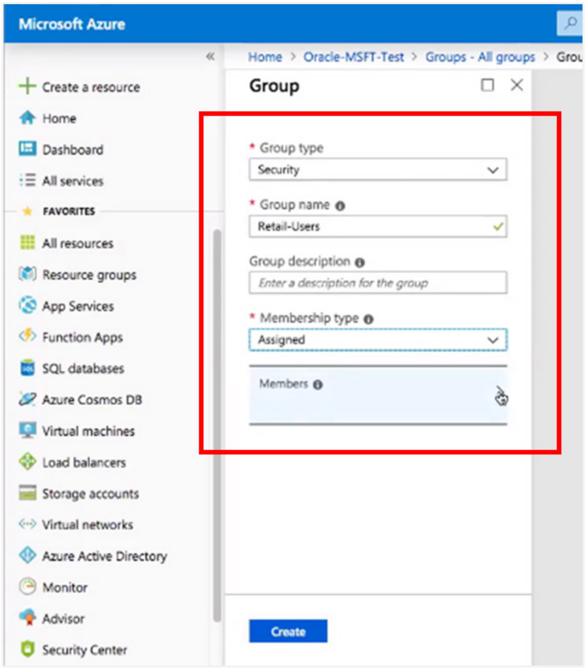
   D. To add more users or groups, repeat these steps.


Search resources, services, and docs
Home > Oracle-MSFT-Test > Enterprise applications - All applications > Retail-IDM - Users and groups > Add Assignment > Users and groups
Add Assignment
Oracle-MSFT-Test
Users and groups
None Selected
Select Role
User
Assign
Users and groups
Select member or invite an external user
Search by name or email address
AZ
azdemouser1
azdemouser1@OracleMSFTDemo.onmicrosoft.com
CD
@OracleMSFTDemo.onmicrosoft.com
EB
EBS-Users
Selected members:
No members selected
Select

3. If no appropriate security group exists, create one. In the far-left navigation pane, click **Azure Active Directory** and then click **Groups**.



4. Click **New Group**, specify **Security** as the type, and then add users to the group by selecting or inviting them. Click **Create**.



Group

* Group type: Security

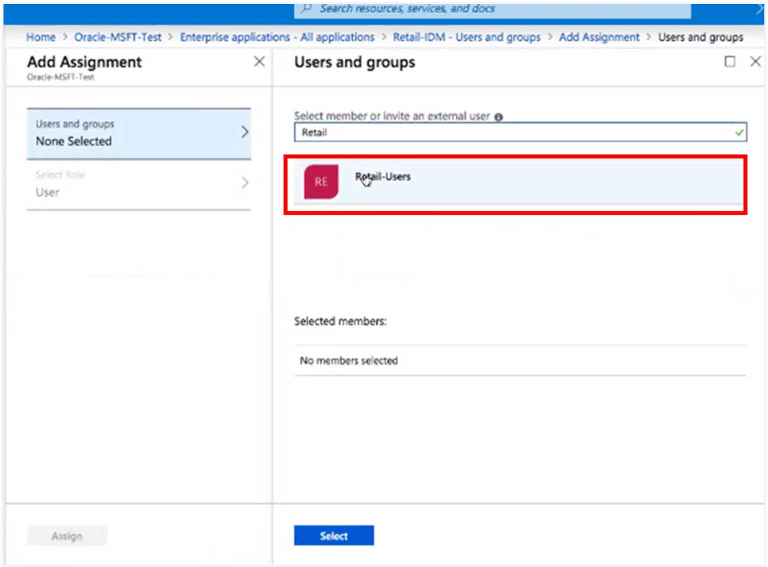
* Group name: Retail-Users

Group description: Enter a description for the group

* Membership type: Assigned

Members

5. Assign the group to the Azure-AD enterprise application.


Search resources, services, and docs
Home > Oracle-MSFT-Test > Enterprise applications - All applications > Retail-IDM - Users and groups > Add Assignment > Users and groups
Assign
Select

Add Assignment
Oracle-MSFT-Test

Users and groups: None Selected

Select Role: User

Users and groups

Select member or invite an external user: Retail

RE Retail-Users

Selected members:

No members selected

6. 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**.

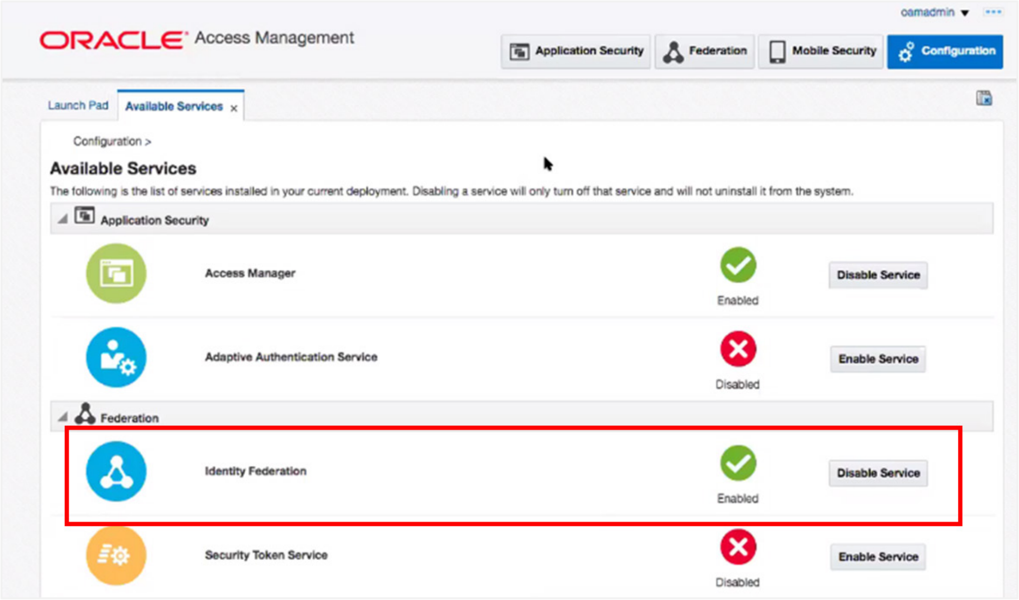
Configuring Oracle Access Manager for Federation with Azure AD

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

Create a New Identity Provider for Azure AD

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

2. Ensure that **Identity Federation** is enabled. If it isn't, click **Enable Service**.



Configuration >

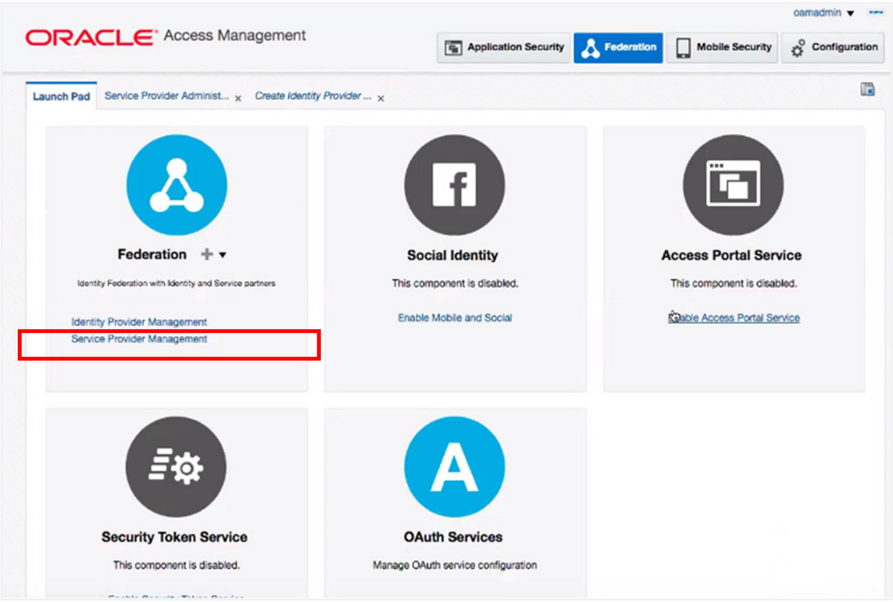
Available Services

The following is the list of services installed in your current deployment. Disabling a service will only turn off that service and will not uninstall it from the system.

Application Security		
Access Manager	✓ Enabled	Disable Service
Adaptive Authentication Service	✗ Disabled	Enable Service
Federation		
Identity Federation	✓ Enabled	Disable Service
Security Token Service	✗ Disabled	Enable Service

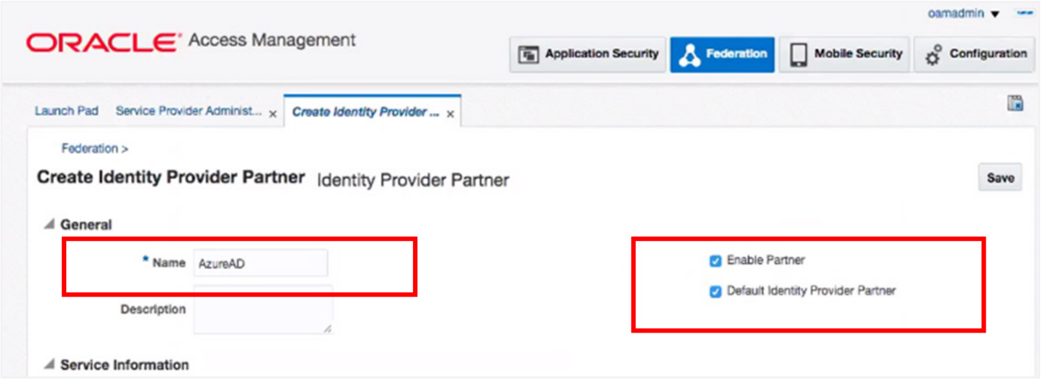
3. Click the **Federation** tab at the top of the console.

4. In the **Federation** area of the **Launch Pad** tab, click **Service Provider Management**. Oracle Access Manager is acting as a service provider in this case. For more information about Oracle Access Manager's role as a service provider in federated identity scenarios, see the OAM Federation: Identity Provider & Service Provider Management blog post.


ORACLE Access Management
oamadmin
Application Security
Federation
Mobile Security
Configuration
Launch Pad
Service Provider Administ...
Create Identity Provider ...
Federation
Identity Federation with Identity and Service partners
Identity Provider Management
Service Provider Management
Social Identity
This component is disabled.
Enable Mobile and Social
Access Portal Service
This component is disabled.
Enable Access Portal Service
Security Token Service
This component is disabled.
OAuth Services
Manage OAuth service configuration

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

6. 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.



* Name AzureAD

Description

☑ Enable Partner

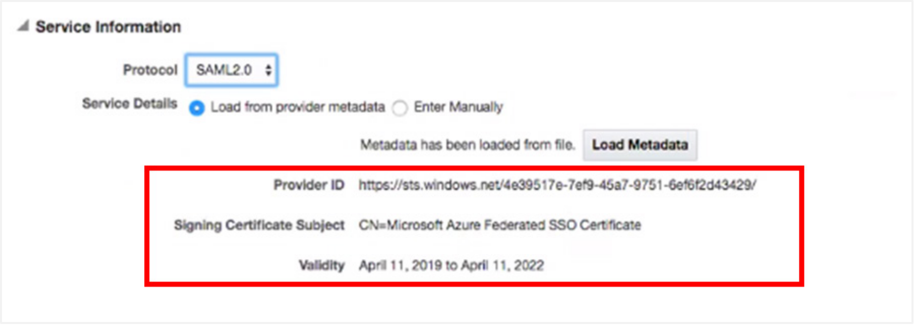
☑ Default Identity Provider Partner

7. 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. Note that Oracle Access Manager will populate the provider ID and certificate information.



◢ Service Information

Protocol: SAML2.0

Service Details: ● Load from provider metadata ○ Enter Manually

Metadata has been loaded from file.

Provider ID: https://sts.windows.net/4e39517e-7ef9-45a7-9751-6ef6f2d43429/

Signing Certificate Subject: CN=Microsoft Azure Federated SSO Certificate

Validity: April 11, 2019 to April 11, 2022

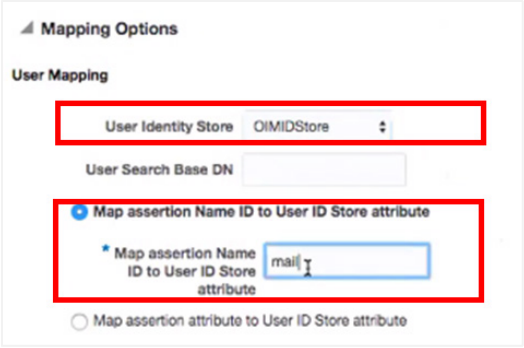
D. Go to the next step before saving.

8. 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 Retail Merchandising 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: OIMIDStore

User Search Base DN:

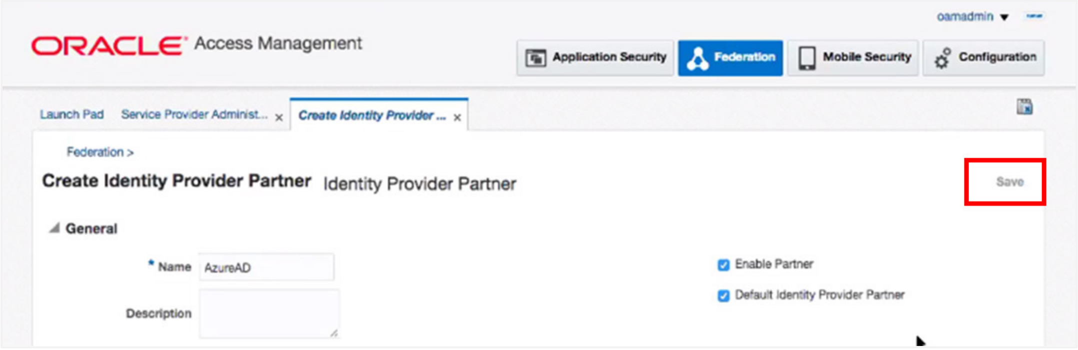
● Map assertion Name ID to User ID Store attribute

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

○ Map assertion attribute to User ID Store attribute

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.

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



* Name AzureAD

Description

☑ Enable Partner

☑ Default Identity Provider Partner

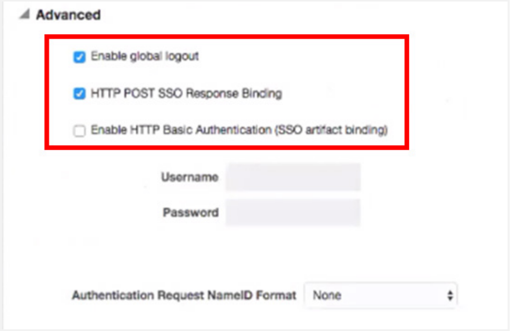
10. After the partner is saved, come back to the **Advanced** area at the bottom of the tab. Ensure that the options are configured as follows:

- **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.

- **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).



☑ Enable global logout

☑ HTTP POST SSO Response Binding

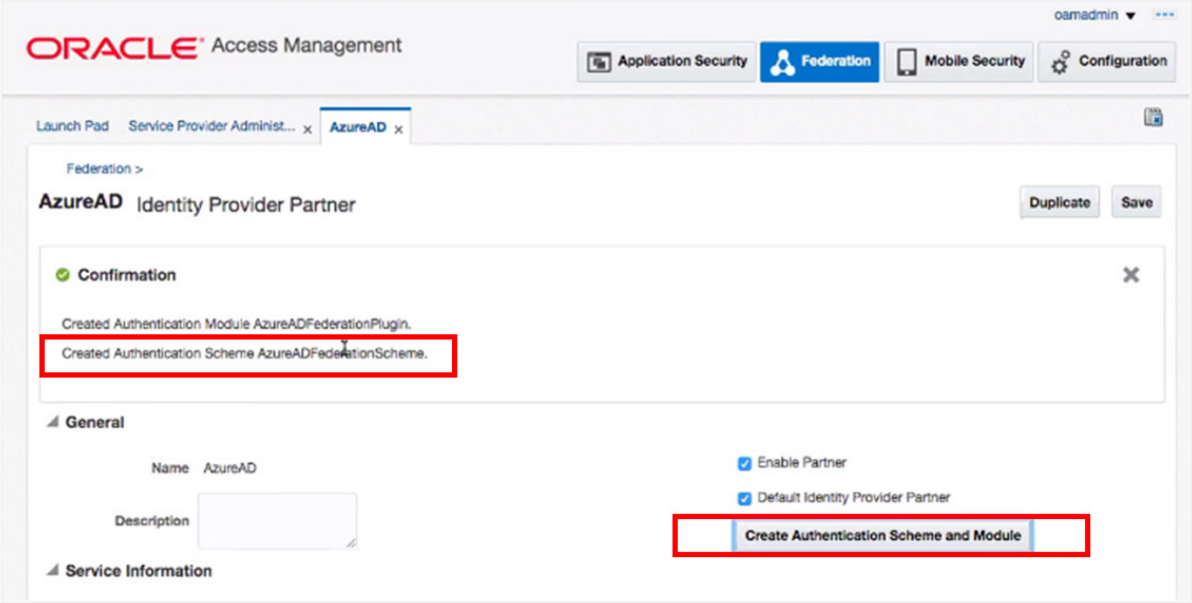
☐ Enable HTTP Basic Authentication (SSO artifact binding)

Username

Password

Authentication Request NameID Format None

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



AzureAD Identity Provider Partner

Confirmation

Created Authentication Module AzureADFederationPlugin.

Created Authentication Scheme AzureADFederationScheme.

Name AzureAD

Description

☑ Enable Partner

☑ Default Identity Provider Partner

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

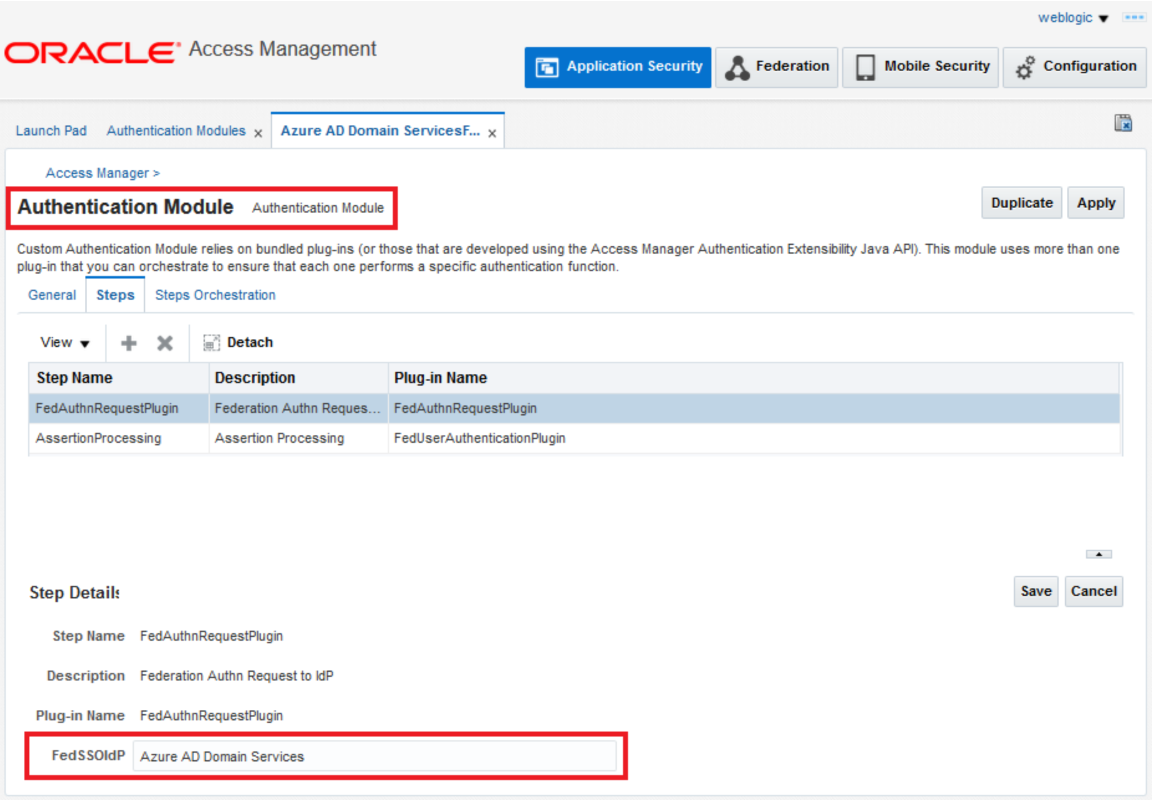
12. You can check the authentication module that was created by following these steps:

    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

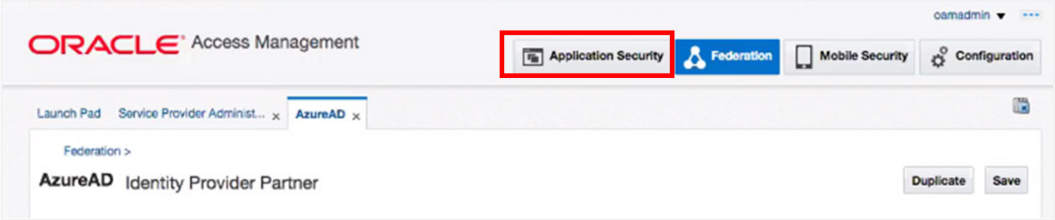
Plug-in Name FedAuthnRequestPlugin

FedSSOIdP Azure AD Domain Services

Associate the Retail Merchandising Resources with the Authentication Scheme

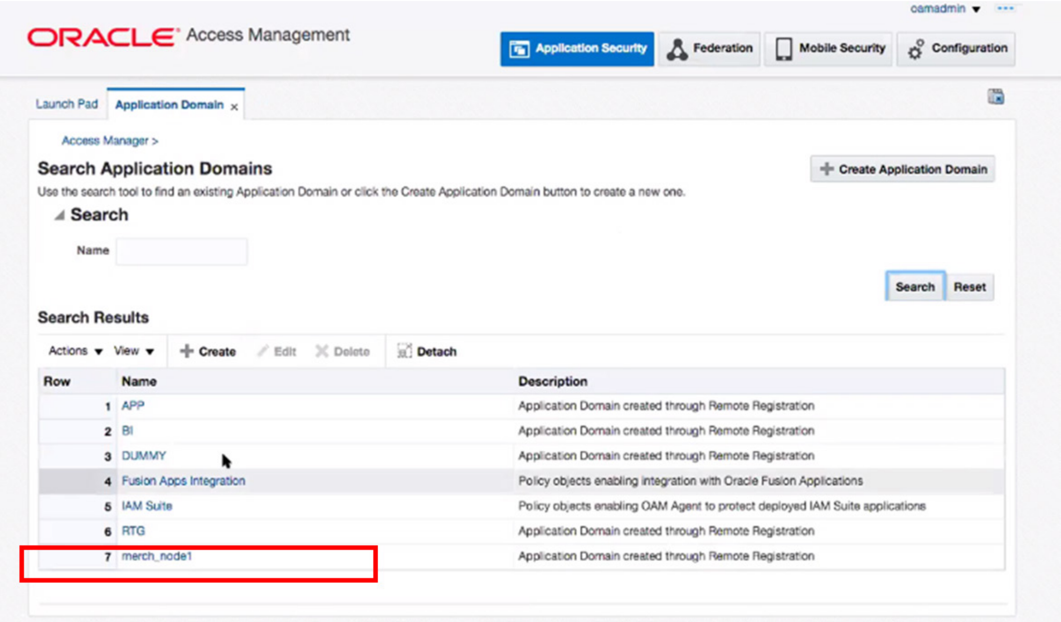
Perform these steps while logged in to the Oracle Access Manager console as an Administrator.

1. At the top of the console, click **Application Security**.



AzureAD Identity Provider Partner

2. Under **Access Manager**, click **Application Domain**, click **Search**, and select the application domain that was created during Retail Merchandising installation that would have registered the Retail Merchandising WebGate.



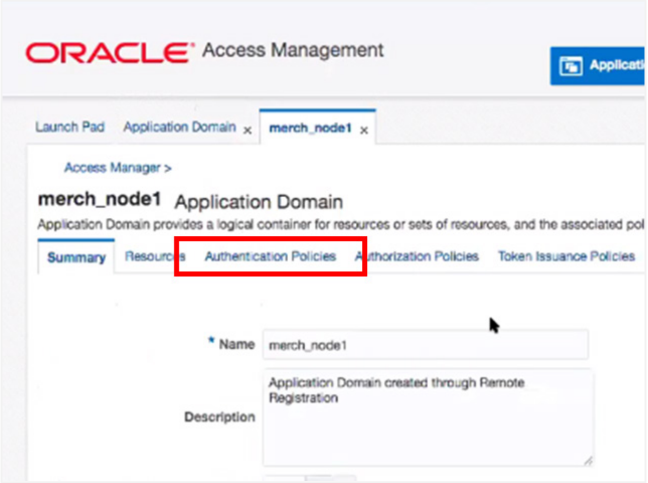
Search Application Domains

Use the search tool to find an existing Application Domain or click the Create Application Domain button to create a new one.

Search Results

Row	Name	Description
1	APP	Application Domain created through Remote Registration
2	BI	Application Domain created through Remote Registration
3	DUMMY	Application Domain created through Remote Registration
4	Fusion Apps Integration	Policy objects enabling integration with Oracle Fusion Applications
5	IAM Suite	Policy objects enabling OAM Agent to protect deployed IAM Suite applications
6	RTG	Application Domain created through Remote Registration
7	merch_node1	Application Domain created through Remote Registration

3. Click the **Authentication Policies** tab.



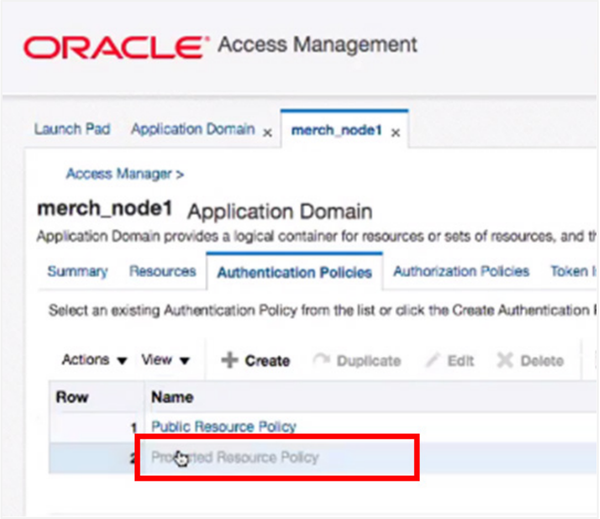
merch_node1 Application Domain

Application Domain provides a logical container for resources or sets of resources, and the associated pol

* Name: merch_node1

Description: Application Domain created through Remote Registration

4. Click **Protected Resources Policy**.



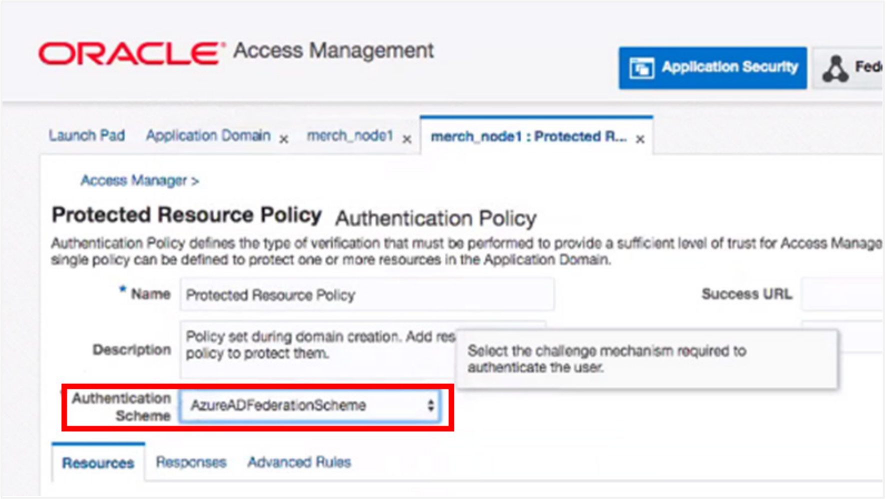
merch_node1 Application Domain

Application Domain provides a logical container for resources or sets of resources, and th

Select an existing Authentication Policy from the list or click the Create Authentication I

Row	Name
1	Public Resource Policy
2	Protected Resource Policy

5. Change the **Authentication Scheme** value by changing the previously created authentication scheme to 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 Manage
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 res policy to protect them.

Select the challenge mechanism required to authenticate the user.

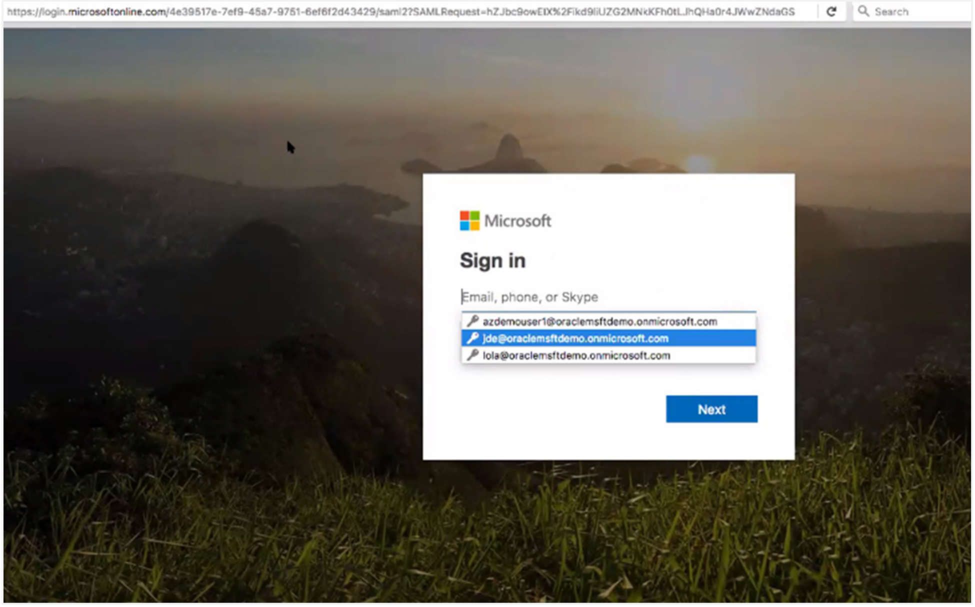
Authentication Scheme: AzureADFederationScheme

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

Testing Federated Login and Logout

This section provides simple steps to verify that federated authentication works when initiated from the service provider. The steps in this section assume that a user has been created in Azure AD and has been provisioned to the Oracle Internet Directory server. To perform various business processing within Retail Merchandising, the user must be further be associated with the appropriate functional roles in Oracle Access Manager.

1. In a browser, enter the Retail Merchandising URL.
2. When Azure AD prompts you for a username or to pick an account, enter the username.



https://login.microsoftonline.com/4e39517e-7ef9-45a7-9751-6ef6f2d43429/saml2?SAMLRequest=hZJbc9owEIX%2Fikd9liUZG2MNkKFh0tLJhQHa0r4JWwZNdaGS

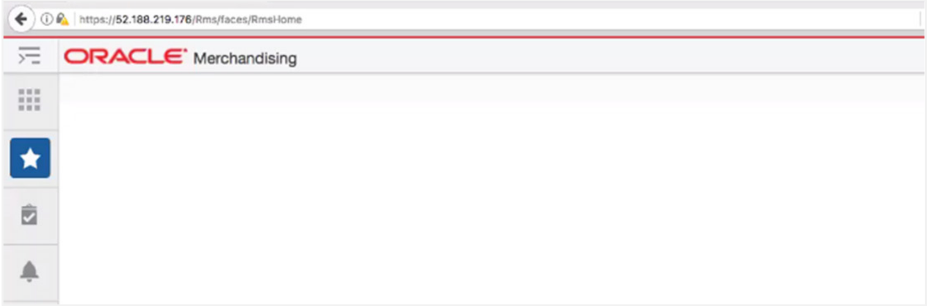
Sign in

Email, phone, or Skype

azdemouser1@oraclemsftdemo.onmicrosoft.com
jde@oraclemsftdemo.onmicrosoft.com
lola@oraclemsftdemo.onmicrosoft.com

3. When prompted for the password, enter it and then click **Sign in**.
4. If you are prompted to **Stay signed in?** click **Yes**.

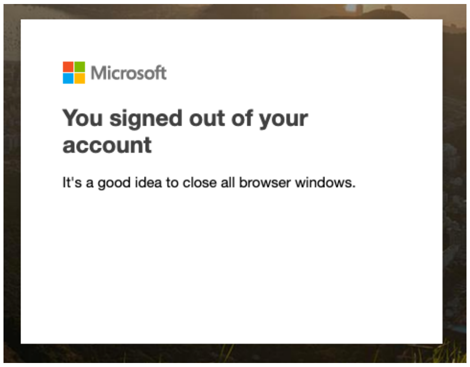
   If the login is successful, you are redirected to the Retail Merchandising home page using your user credentials stored in Azure AD.



https://52.188.219.176/Rms/faces/RmsHome

5. To log out, select **Logout** from the **User** menu in the top-right corner.

   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.

Conclusion

This document describes the cross-cloud architecture for Oracle Retail Merchandising Suite and how to implement federated SSO using Azure AD and Oracle Access Manager. In this cross-cloud model, Azure AD performs authentication (AuthN) and Oracle Access Manager performs authorization (AuthZ), giving retailers the benefit of the rich functional authorization integration between Retail Merchandising and Oracle Access Manager. Federated SSO in the cross-cloud model is straightforward as long as critical user attributes are synchronized between the systems.

Oracle Retail Merchandising is fully supported in the cross-cloud model with federated SSO via Azure AD and Oracle Access Manager.

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 Retail Merchandising Suite Across Oracle Cloud Infrastructure and Azure: SSO with Oracle Access Manager and Azure Active Directory
June 2019
Author: Siobhan Mcmahon (Oracle)

Oracle is committed to developing practices and products that help protect the environment