Microsoft Azure + ORACLE

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

SSO with Oracle Identity Cloud Service 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

Most customers who use Oracle E-Business Suite integrate it in production with their corporate identity and access management (IAM) solution to achieve single sign-on (SSO). Because E-Business Suite doesn't support SSO protocols like SAML 2.0 and OpenID Connect, a set of external components (for example, Oracle Identity Cloud Service with E-Business Suite Asserter, or Oracle Access Manager with Oracle Internet Directory or Oracle Unified Directory) is needed to enable E-Business Suite to integrate with an enterprise SSO solution like Microsoft Azure Active Directory (Azure AD).

This paper provides a reference SSO architecture and configuration details for end users who are accessing Oracle E-Business Suite running on Azure by using Oracle Identity Cloud Service. This setup enables users who have already logged in to Azure AD to navigate to E-Business Suite without logging in again. Enterprises that deploy this solution gain the benefits of SSO, including a single set of credentials, an improved login experience, improved security, and reduced help-desk cost.

Use Cases

Following are common use cases for using SSO with E-Business Suite and Azure AD:

- Users log in to Azure AD, access E-Business Suite through the My Apps portal (myapps.microsoft.com), and get seamless access to E-Business Suite.
- E-Business Suite users with a bookmarked E-Business Suite or AppsLogin URL are redirected to Azure AD to log in, and get access to the application after successful authentication.
- Users who log out of E-Business Suite are also logged out of the My Apps portal.

Benefits

The benefits for using SSO with E-Business Suite and Azure AD are as follows:

- Lightweight E-Business Suite SSO solution
- Single set of credentials
- Seamless login and logout experience
- Secure end-user access provided by the security features of Azure AD and Identity Cloud Service

Assumptions

User synchronization between Azure AD and E-Business Suite is a prerequisite for SSO to work. User synchronization is out of the scope of this white paper, but enterprises can use different strategies to achieve it. Typically, enterprises have an identity provisioning system that synchronizes users among Azure AD, Identity Cloud Service, and E-Business Suite. Also, Identity Cloud Service has a feature to keep users synchronized between Azure AD and Identity Cloud Service. For more information, see the “Enabling Synchronization” section in the Identity Cloud Service documentation.

High-Level Architecture

Figure 1 shows a high-level architecture diagram for this SSO solution. The Oracle E-Business Suite application tier is deployed in Azure, and the database tier is deployed in Oracle Cloud Infrastructure (OCI). The connectivity between the application tier and the database tier is set up during E-Business Suite installation. The connection between the E-Business Suite Asserter and the data tier follows the same route.

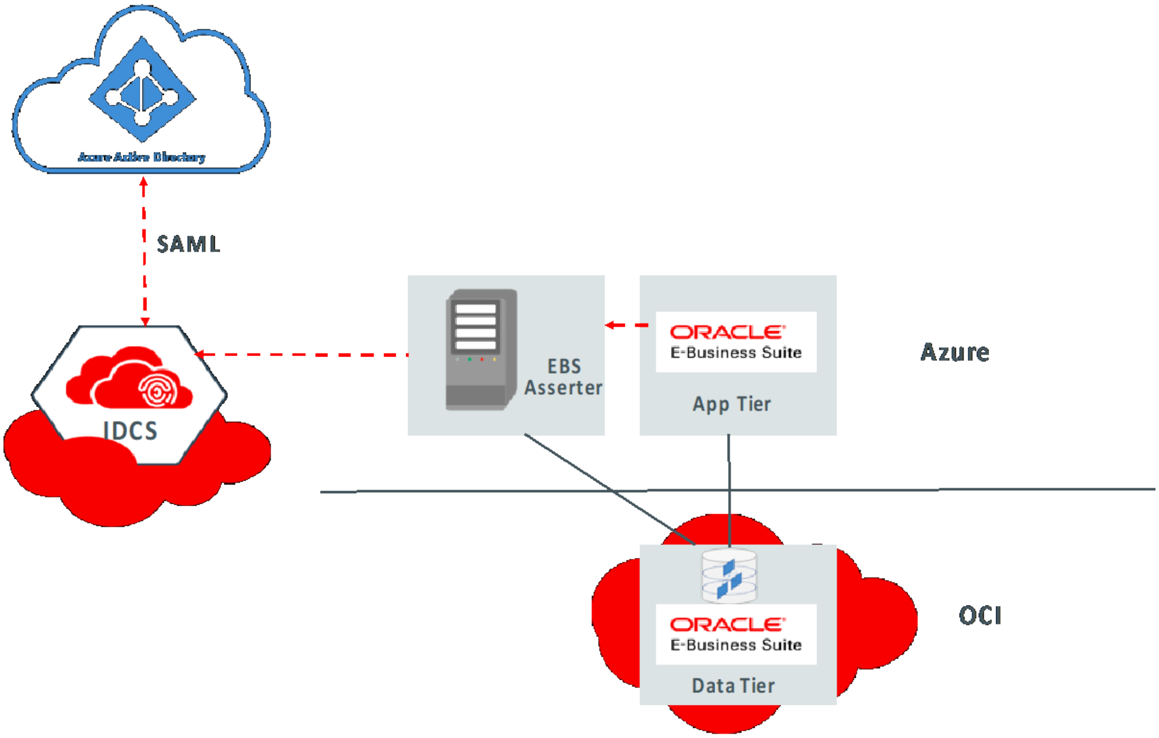


Figure 1. SSO High-Level Architecture

In this configuration, Azure AD is the identity provider (IDP), which holds user credentials (username, password, and any other factors). The authentication flows as follows:

- Azure AD performs user authentication and generates an authentication token.
- Identity Cloud Service (IDCS) consumes the authentication token and generates an OpenID Connect (OIDC) token.
- E-Business Suite (EBS) Asserter consumes the OpenID Connect token, validates it, and then creates a session for the user in E-Business Suite.

Figure 2 shows this authentication flow in detail.

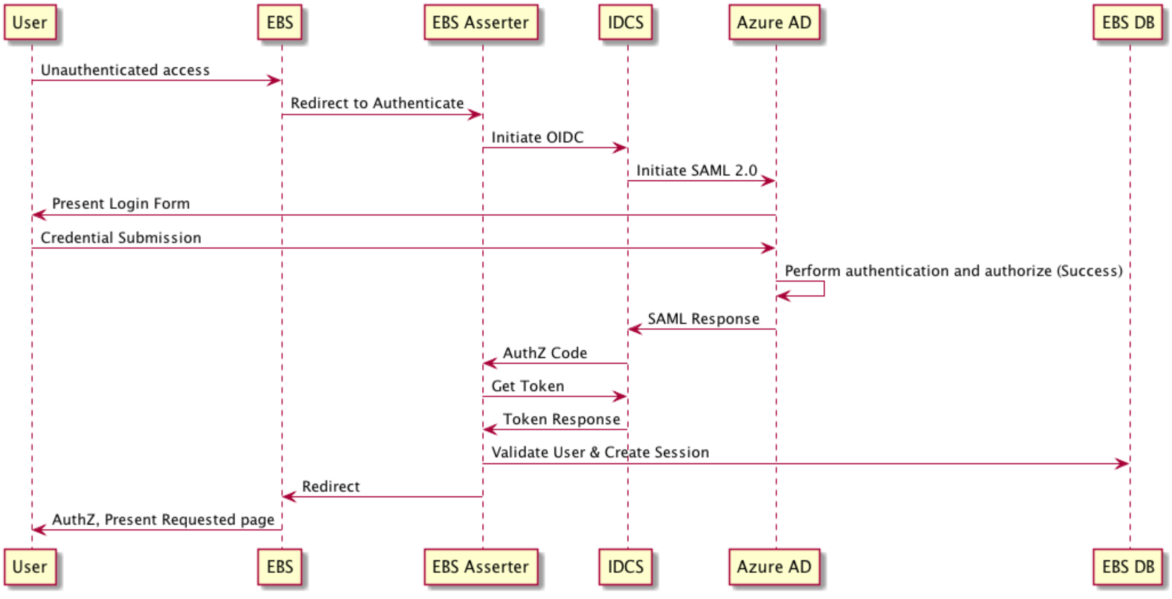


Figure 2. Authentication Flow

A user accesses the E-Business Suite app directly by going to the E-Business Suite AppsLogin page or the My Apps portal.

Network Security and High Availability of E-Business Suite Asserter

To communicate with Identity Cloud Service, the E-Business Suite Asserter VM must have a public IP address. For added security, we recommend placing the E-Business Suite Asserter VM in its own subnet within the Azure Virtual Network (VNet) and configuring the network security group (NSG) to control the network traffic flow. Figure 3 shows this configuration in detail.

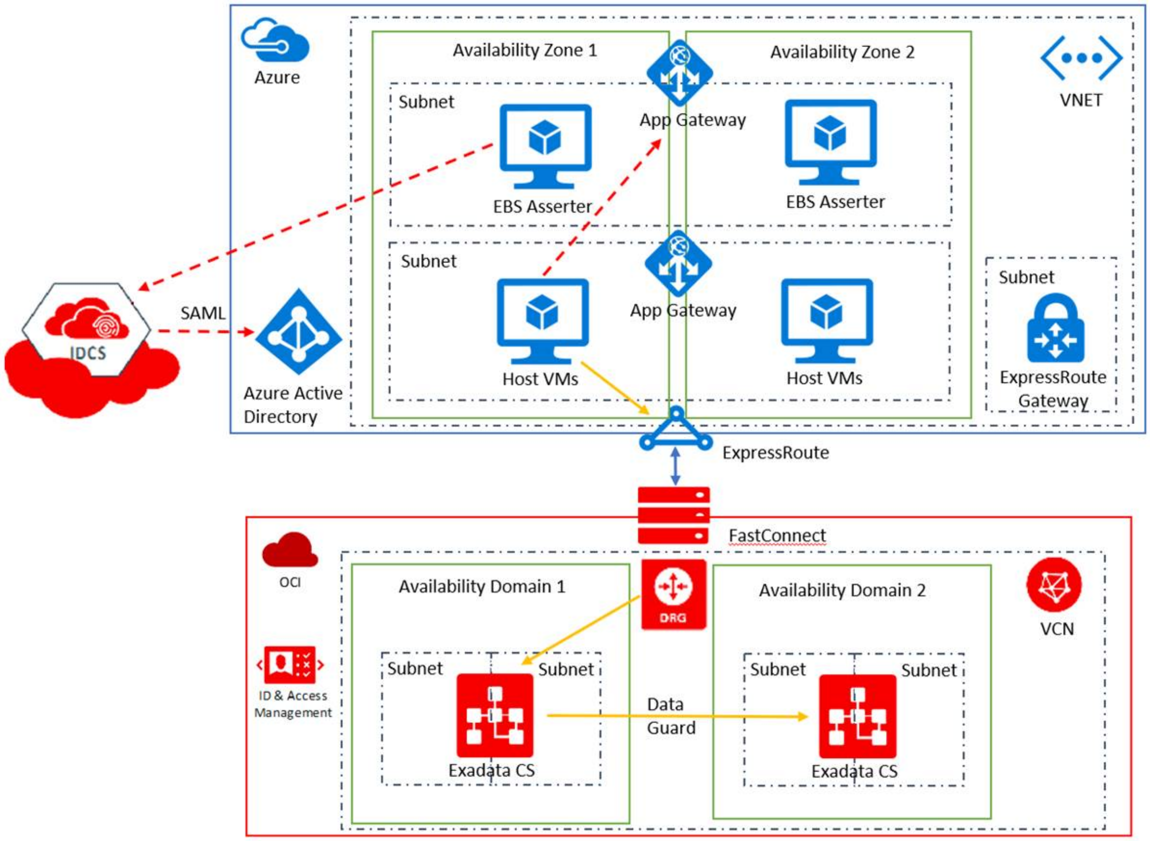


Figure 3. Security and Availability Configuration

Configuring SSO

This section provides detailed steps for configuring SSO with E-Business Suite and Azure AD.

Prerequisites

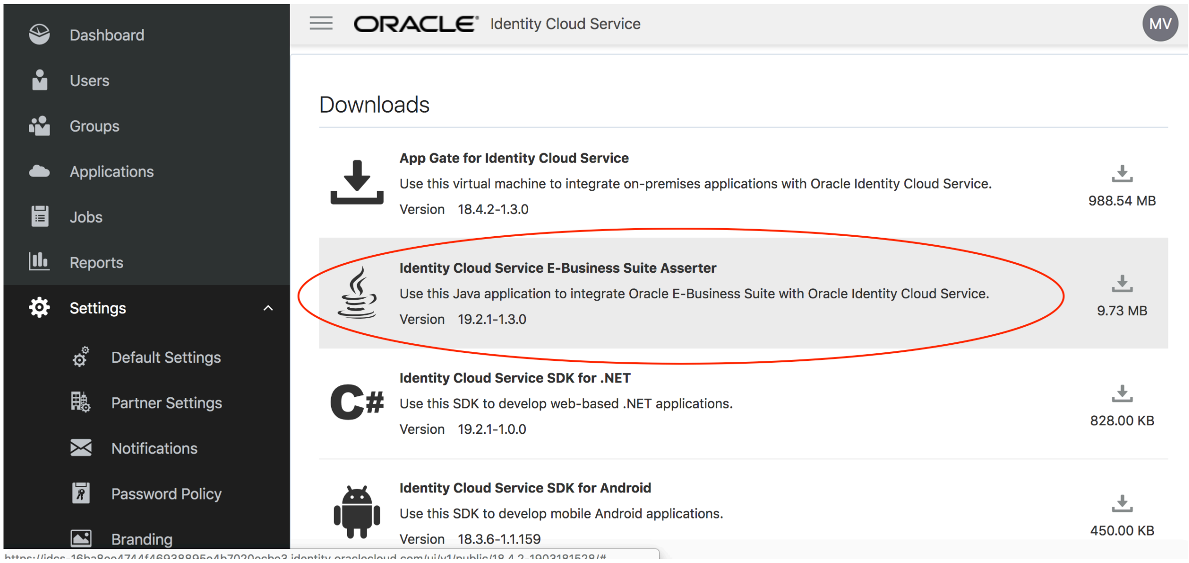
- An Identity Cloud Service tenancy and a user with the Security Administrator or Identity Domain Administrator role
- Oracle E-Business Suite application with a Sys account
- Azure subscription with a Contributor or greater privileged account
- Azure AD subscription and a user with the Global Administrator role

High-Level Steps

1. Integrate Identity Cloud Service and E-Business Suite by using E-Business Suite Asserter.
2. Set up SAML 2.0 federation trust between Azure AD and Identity Cloud Service.
3. Add E-Business Suite as a non-gallery application in Azure AD.

Integrate Identity Cloud Service and E-Business Suite by Using E-Business Suite Asserter

1. Download the E-Business Suite Asserter web application from the Identity Cloud Service admin console.



App Gate for Identity Cloud Service
Use this virtual machine to integrate on-premises applications with Oracle Identity Cloud Service.
Version 18.4.2-1.3.0
988.54 MB

Identity Cloud Service E-Business Suite Asserter
Use this Java application to integrate Oracle E-Business Suite with Oracle Identity Cloud Service.
Version 19.2.1-1.3.0
9.73 MB

Identity Cloud Service SDK for .NET
Use this SDK to develop web-based .NET applications.
Version 19.2.1-1.0.0
828.00 KB

Identity Cloud Service SDK for Android
Use this SDK to develop mobile Android applications.
Version 18.3.6-1.1.159
450.00 KB

2. Deploy E-Business Suite Asserter on an Oracle WebLogic server.

   You can install a WebLogic server from scratch, or use the Azure Marketplace **Oracle WebLogic Server 12.1.2** option and install and use JDK 1.8 during domain configuration.

   If you create a VM to install a WebLogic server, the OS of the VM should be compatible as described in the Fusion Middleware Certification Matrix that applies to your version.

3. Configure Oracle E-Business Suite to use Identity Cloud Service for SSO.

   The linked document provides details on deploying a single instance of E-Business Suite Asserter. You can scale the architecture for high availability (HA) by having multiple E-Business Suite Asserter deployments with a load balancer on the front end. For failover support, follow the application failover guidelines in Azure. See the following Azure topics for HA and failover details:

- Availability Zones
- Load Balancer

Set Up SAML 2.0 Federation Trust Between Azure AD and Identity Cloud Service

This step has several parts:

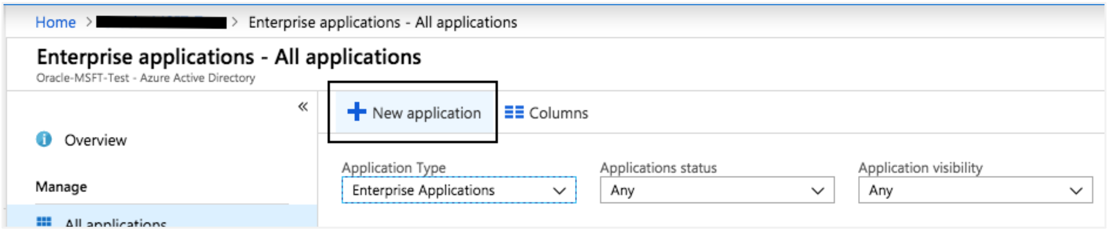
1. Add Identity Cloud Service as a gallery application in Azure AD.
2. Add Azure AD as an IDP in Identity Cloud Service.
3. Complete single sign-on configuration in Azure AD.

Add Identity Cloud Service as a Gallery Application in Azure AD

1. Log in to your Identity Cloud Service (IDCS) tenancy with admin credentials, go to your tenancy-specific metadata URL, and download the metadata. The URL looks as follows:

   ```
   https://<your_tenancy>.identity.oraclecloud.com/fed/v1/metadata
   ```

2. In the Azure portal, navigate to **Azure Active Directory** > **Enterprise applications** > **All applications**, and then click **New application**.



Home > [redacted] > Enterprise applications - All applications

Enterprise applications - All applications

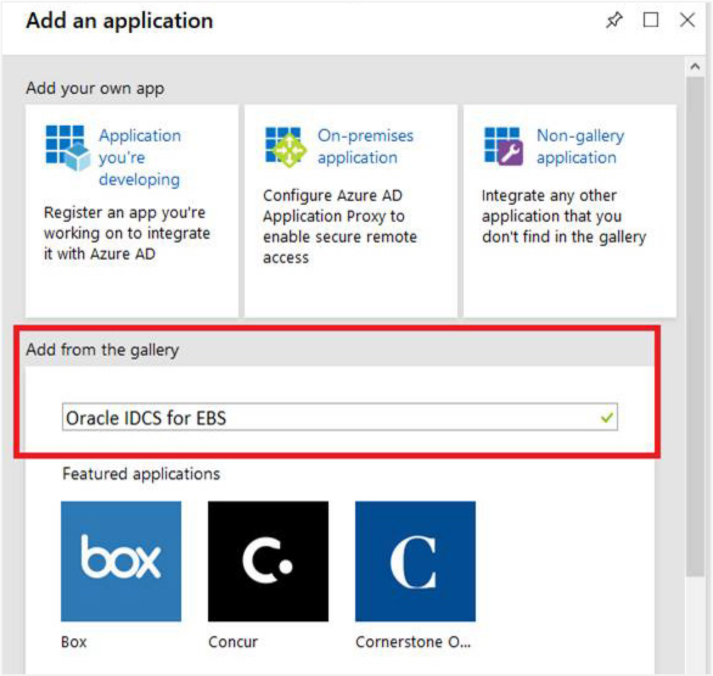
Oracle-MSFT-Test - Azure Active Directory

Application Type: Enterprise Applications

Applications status: Any

Application visibility: Any

3. Type **Oracle IDCS for EBS** in the search box, and select **Oracle IDCS for EBS** from the resulting applications.



Add an application

Add your own app

Application you're developing
Register an app you're working on to integrate it with Azure AD

On-premises application
Configure Azure AD Application Proxy to enable secure remote access

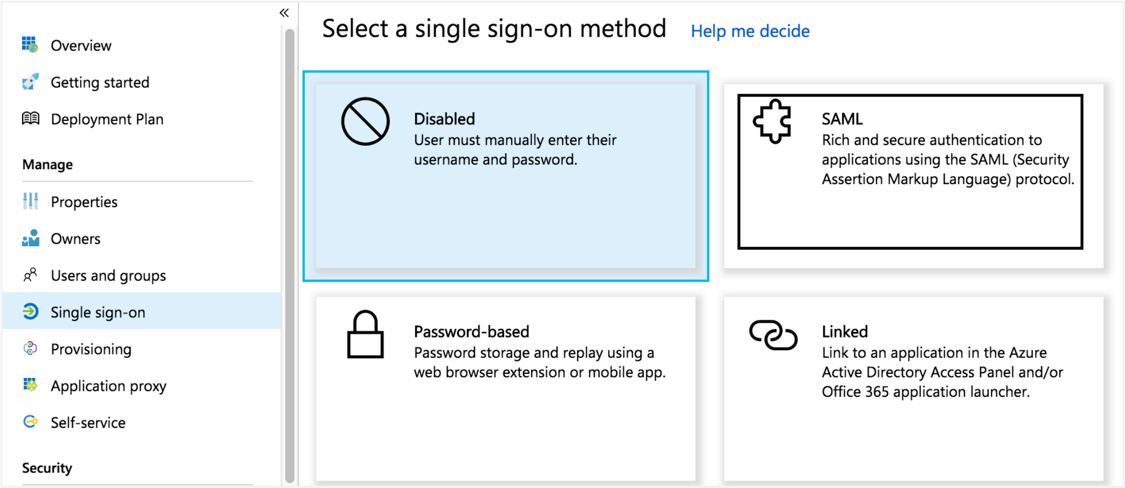
Non-gallery application
Integrate any other application that you don't find in the gallery

Add from the gallery

Oracle IDCS for EBS

Featured applications

4. For the new application, navigate to **Single sign-on** and select **SAML** as the single sign-on method.



Select a single sign-on method Help me decide

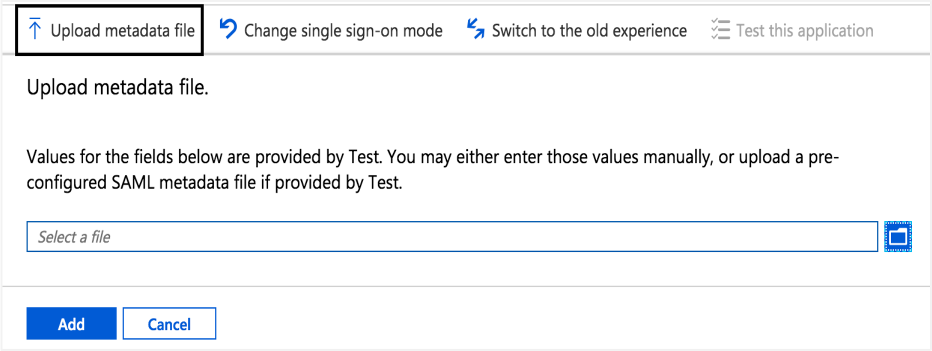
Disabled
User must manually enter their username and password.

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

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.

5. Click **Upload metadata file**.



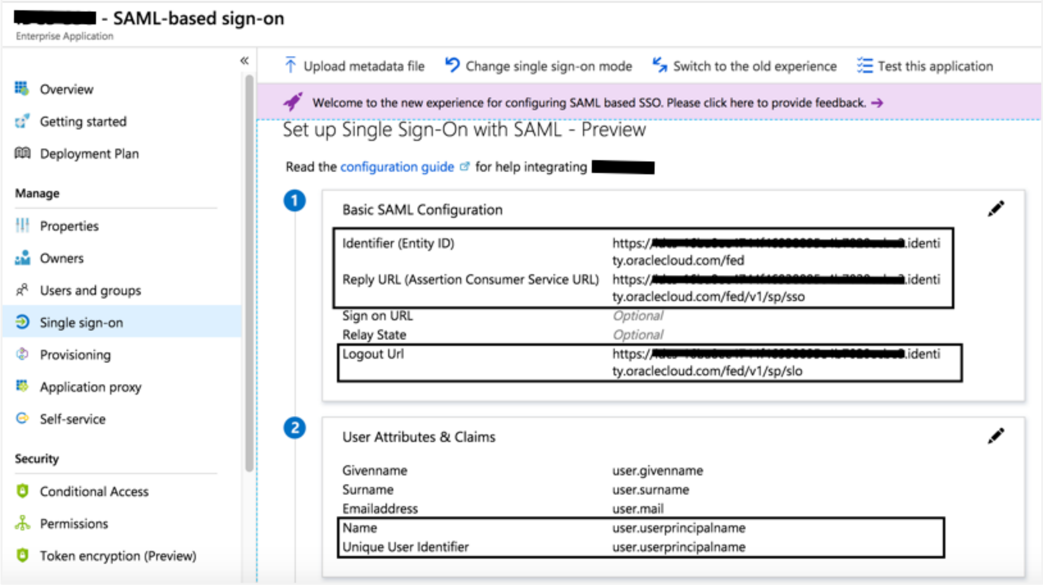
Upload metadata file.

Values for the fields below are provided by Test. You may either enter those values manually, or upload a pre-configured SAML metadata file if provided by Test.

Select a file

6. Select the Identity Cloud Service metadata file that you downloaded in step A, and then click **Add**.

7. Verify the SAML configuration. Add the Oracle Identity Cloud Service **Logout Url**, if it's missing. In the **User Attributes & Claims** section, keep the default values.



[redacted] - SAML-based sign-on

Enterprise 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 [redacted]

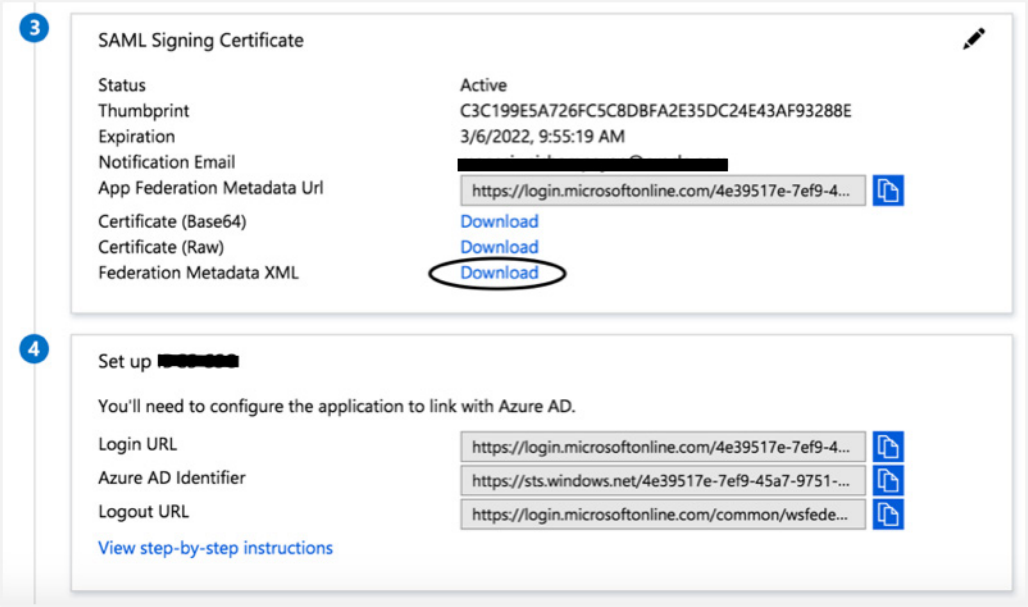
Basic SAML Configuration

Identifier (Entity ID)	https://[redacted].identity.oraclecloud.com/fed
Reply URL (Assertion Consumer Service URL)	https://[redacted].identity.oraclecloud.com/fed/v1/sp/sso
Sign on URL	Optional
Relay State	Optional
Logout Url	https://[redacted].identity.oraclecloud.com/fed/v1/sp/slo

User Attributes & Claims

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

8. In the **SAML Signing Certificate** section, click **Download** next to **Federation Metadata XML**.



3 SAML Signing Certificate

Status	Active
Thumbprint	C3C199E5A726FC5C8DBFA2E35DC24E43AF93288E
Expiration	3/6/2022, 9:55:19 AM
Notification Email	[redacted]
App Federation Metadata Url	https://login.microsoftonline.com/4e39517e-7ef9-4...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

4 Set up [redacted]

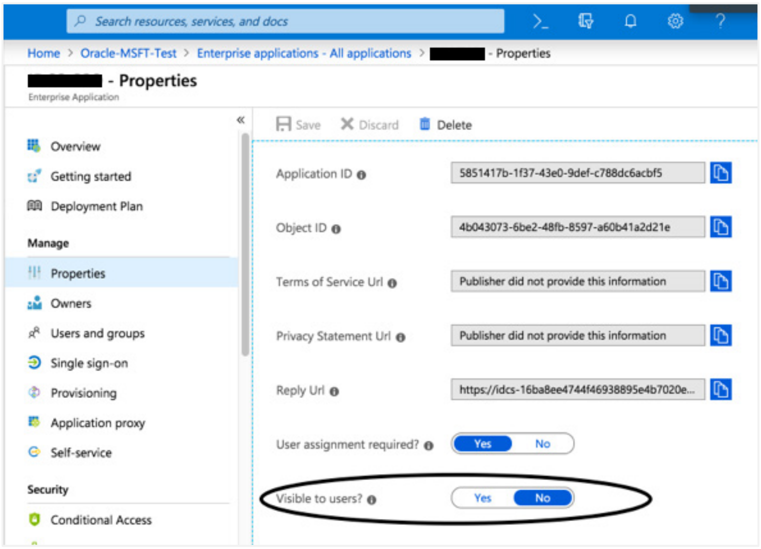
You'll need to configure the application to link with Azure AD.

Login URL	https://login.microsoftonline.com/4e39517e-7ef9-4...
Azure AD Identifier	https://sts.windows.net/4e39517e-7ef9-45a7-9751-...
Logout URL	https://login.microsoftonline.com/common/wsfede...

View step-by-step instructions

This application provides a SAML 2.0 federation link between Azure AD and Identity Cloud Service, but E-Business Suite application users should see only the E-Business Suite application in the My Apps portal.

9. To hide the **Oracle IDCS for EBS** application in the My Apps portal, set the **Visible to users?** property to **No**.



[redacted] - Properties

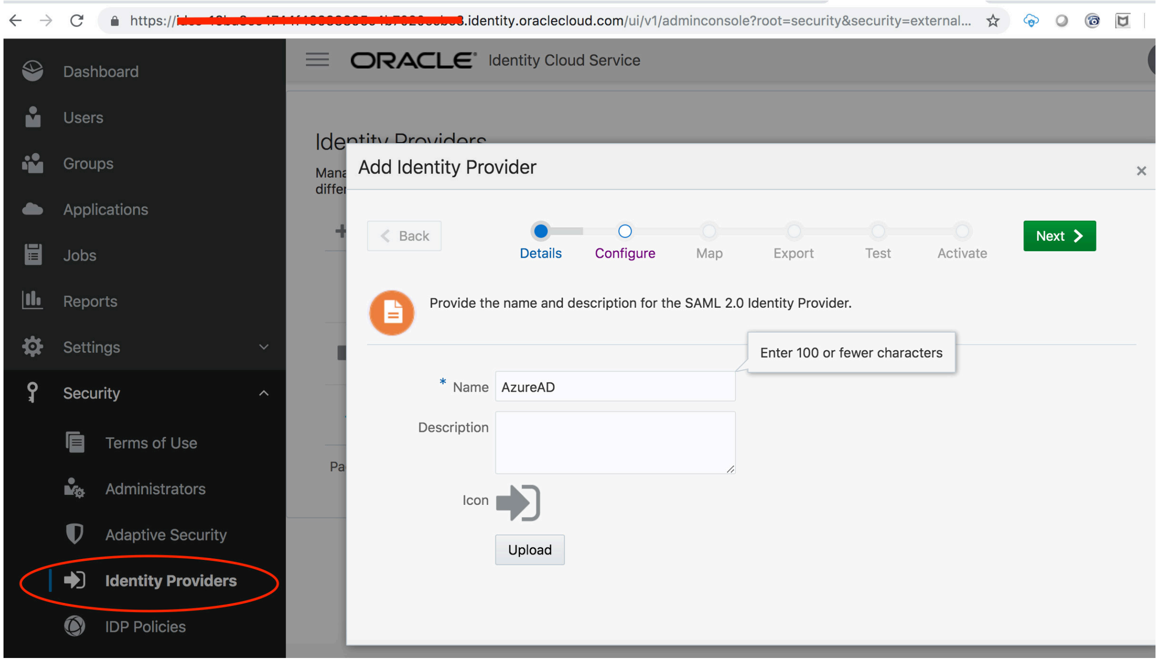
Application ID	5851417b-1f37-43e0-9def-c788dc6acbf5
Object ID	4b043073-6be2-48fb-8597-a60b41a2d21e
Terms of Service Url	Publisher did not provide this information
Privacy Statement Url	Publisher did not provide this information
Reply Url	https://idcs-16ba8ee4744f46938895e4b7020e...
User assignment required?	[✓ Yes] No
Visible to users?	Yes [✓ No]

Add Azure AD as an IDP in Identity Cloud Service

1. Log in to the Identity Cloud Service admin console.

2. In the navigation pane, click **Security**, click **Identity Providers**, and then add an IDP.

3. In the wizard, enter a name for the IDP, and then click **Next**.



https://[redacted].identity.oraclecloud.com/ui/v1/adminconsole?root=security&security=external...

Provide the name and description for the SAML 2.0 Identity Provider.

Enter 100 or fewer characters

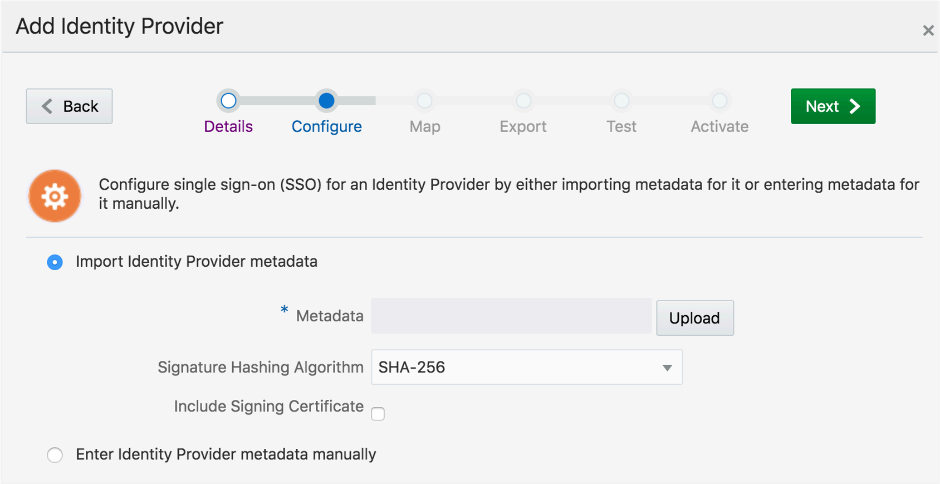
* Name: AzureAD

Description:

Icon

Upload

4. Import the Azure AD Federation Metadata file that you downloaded in the previous section.



Configure single sign-on (SSO) for an Identity Provider by either importing metadata for it or entering metadata for it manually.

● Import Identity Provider metadata

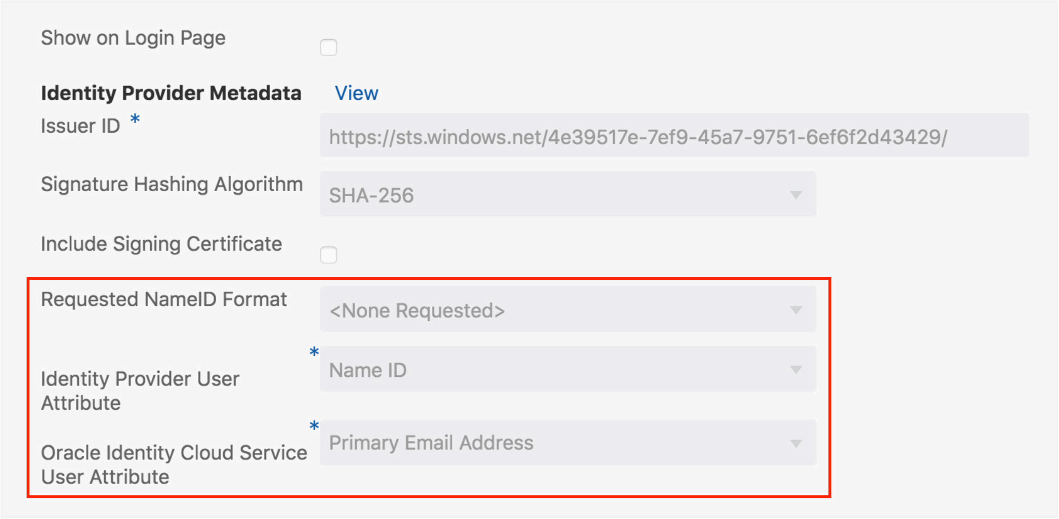
* Metadata: Upload

Signature Hashing Algorithm: SHA-256

Include Signing Certificate □

○ Enter Identity Provider metadata manually

5. Use the default value for **Requested NameID Format**. The value for **Identity Provider User Attribute** should be **Name ID**. Set the value for **Oracle Identity Cloud Service User Attribute** to **Primary Email Address** or to any other attribute in Identity Cloud Service that might hold the user's principal name in Azure AD.



Show on Login Page	□
Identity Provider Metadata	View
Issuer ID *	https://sts.windows.net/4e39517e-7ef9-45a7-9751-6ef6f2d43429/
Signature Hashing Algorithm	SHA-256
Include Signing Certificate	□
Requested NameID Format	<None Requested>
Identity Provider User Attribute *	Name ID
Oracle Identity Cloud Service User Attribute *	Primary Email Address

6. Click **Save**.

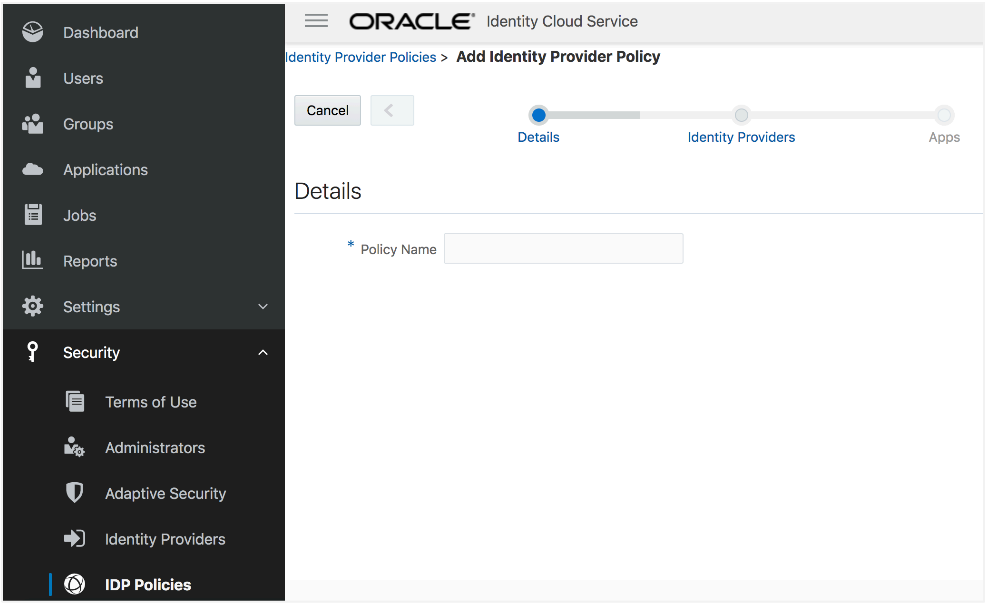
   For more information about adding an IDP to Identity Cloud Service, see the documentation.

7. Set up an IDP policy and add each app that might use Azure AD for authentication.

   A. In the navigation pane, click **Security**, and then click **IDP Policies**.

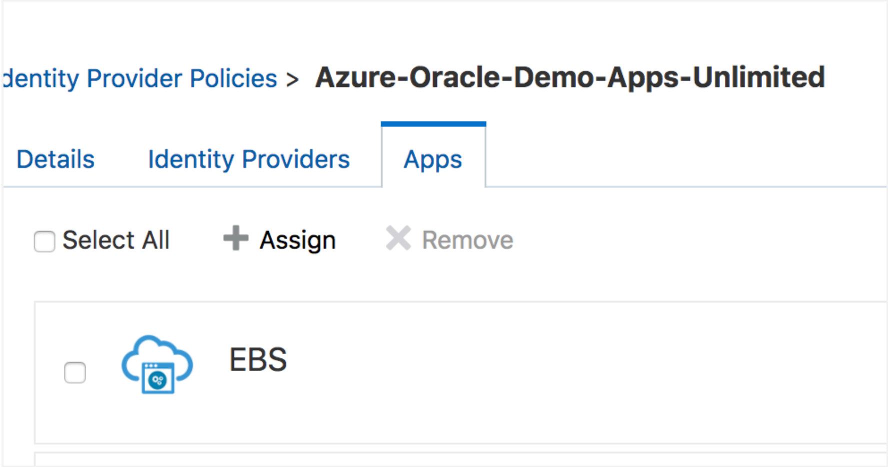
   B. Click **Add**.

   C. In the wizard, enter the name for the policy, and then click **Next**.



D. Click **Assign**, select **Azure AD IDP** from the list, and then click **Next**.

E. Assign one or more applications that might use this IDP, such as E-Business Suite (EBS).

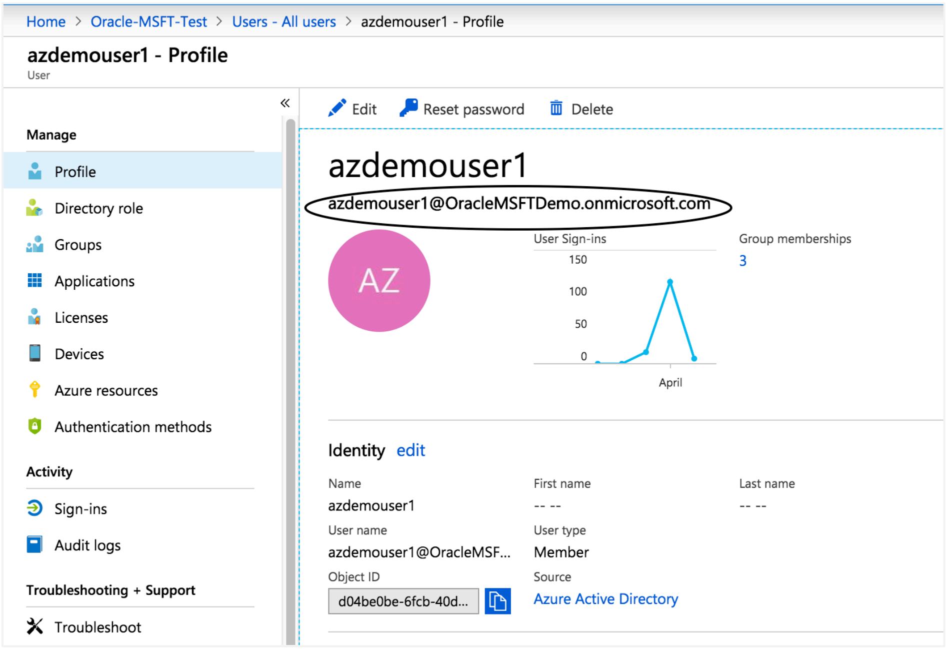

dentity Provider Policies > Azure-Oracle-Demo-Apps-Unlimited
Details
Identity Providers
Apps
□ Select All
Assign
Remove
□
EBS

Complete Single Sign-On Configuration in Azure AD

1. Sign in to the Azure portal.

2. Create a security group, for example, **EBS-Users**.

3. Create a test user.



azdemouser1

azdemouser1@OracleMSFTDemo.onmicrosoft.com

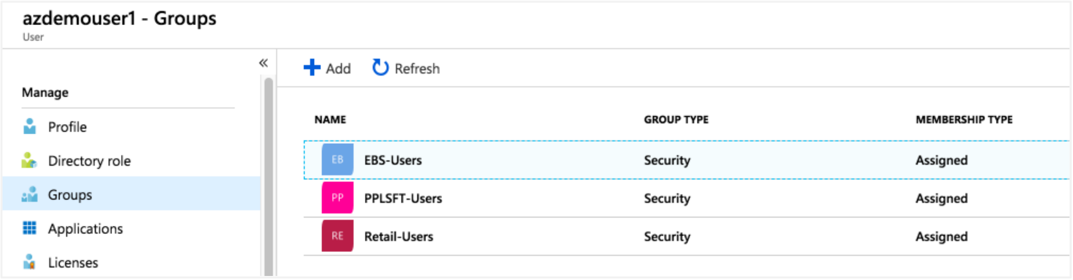
Group memberships: 3

Name	First name	Last name
azdemouser1	-- --	-- --

User name	User type
azdemouser1@OracleMSF...	Member

Object ID	Source
d04be0be-6fcb-40d...	Azure Active Directory

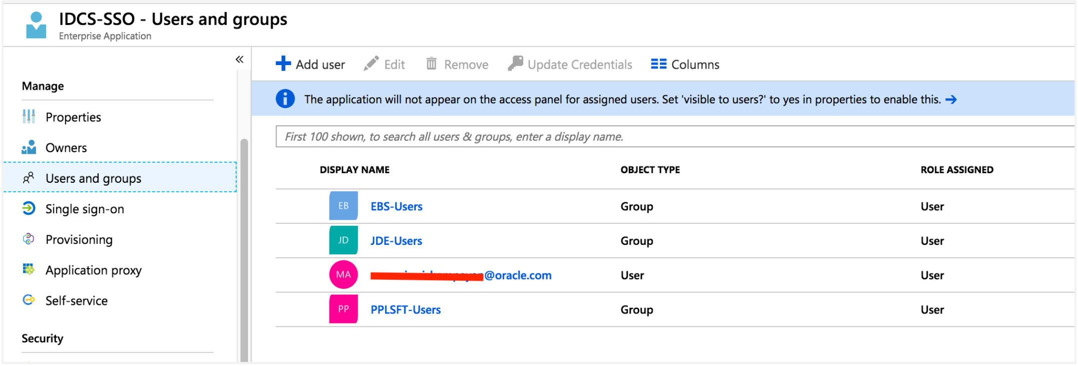
4. Add the user to the group.



NAME	GROUP TYPE	MEMBERSHIP TYPE
EB EBS-Users	Security	Assigned
PP PPLSFT-Users	Security	Assigned
RE Retail-Users	Security	Assigned

5. Assign the group to the **Oracle IDCS for EBS** application.

   For example, the **EBS-Users** group contains all the users who might access the E-Business Suite application through Identity Cloud Service. A user can belong to multiple groups.



IDCS-SSO - Users and groups
Enterprise Application

The application will not appear on the access panel for assigned users. Set 'visible to users?' to yes in properties to enable this. →

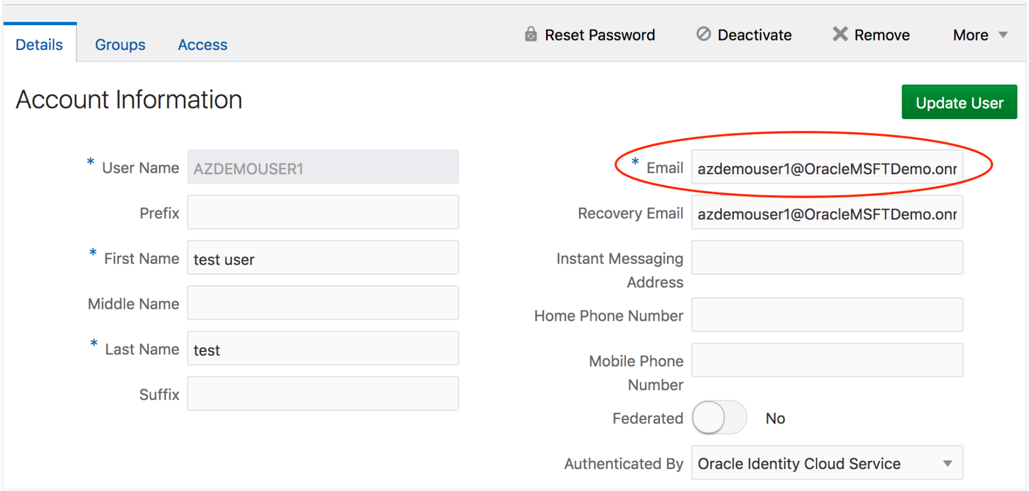
First 100 shown, to search all users & groups, enter a display name.

DISPLAY NAME	OBJECT TYPE	ROLE ASSIGNED
EB EBS-Users	Group	User
JD JDE-Users	Group	User
MA [redacted]@oracle.com	User	User
PP PPLSFT-Users	Group	User

6. Open the Identity Cloud Service admin console.

   For testing purposes, you can either create a user in Identity Cloud Service manually or synchronize Azure AD users in Identity Cloud Service.

   The users should be created or synchronized such that a user principal name in Azure AD matches the user's primary email address (or some other attribute) in Identity Cloud Service. For example, **joe.smith@example.com** would be the user's principal name in Azure AD and the Identity Cloud Service primary email address.



Account Information

* User Name	AZDEMOUSER1	* Email	azdemouser1@OracleMSFTDemo.onr
Prefix		Recovery Email	azdemouser1@OracleMSFTDemo.onr
* First Name	test user	Instant Messaging Address	
Middle Name		Home Phone Number	
* Last Name	test	Mobile Phone Number	
Suffix		Federated	No
		Authenticated By	Oracle Identity Cloud Service

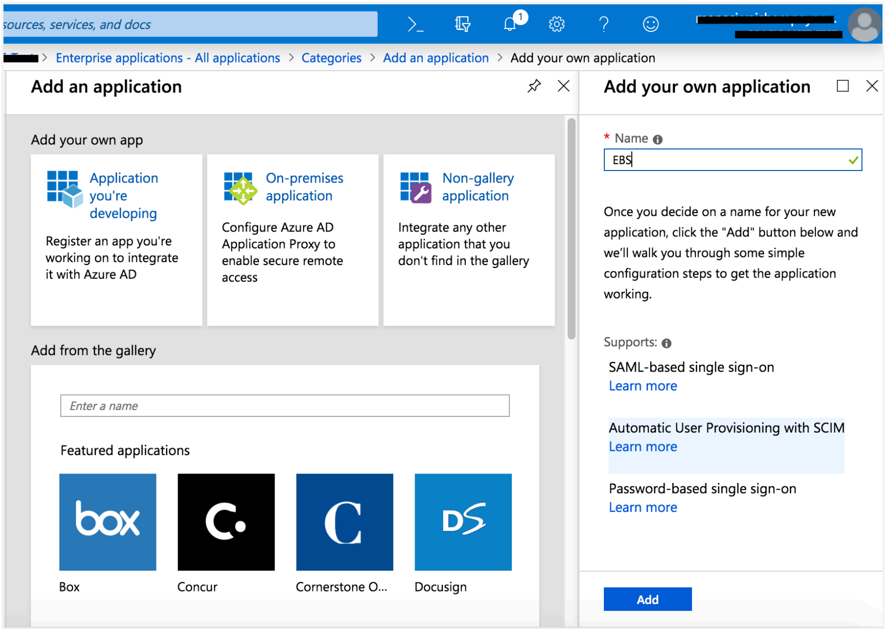
7. In Azure AD, navigate to the Oracle IDCS for EBS enterprise application and test single sign-on by using the test account.

Add E-Business Suite as a Non-Gallery Application in Azure AD

1. In the Azure portal, navigate to **Azure Active Directory** > **Enterprise applications** > **All applications**, and then click **New application**.

2. Click **Non-gallery application**.

3. Type **EBS** in the **Name** box, and then click **Add**.



sources, services, and docs [redacted]

[redacted] > Enterprise applications - All applications > Categories > Add an application > Add your own application

Add an application

Add your own app

Application you're developing
Register an app you're working on to integrate it with Azure AD

On-premises application
Configure Azure AD Application Proxy to enable secure remote access

Non-gallery application
Integrate any other application that you don't find in the gallery

Add from the gallery

Enter a name

Featured applications

Box · Concur · Cornerstone O... · Docusign

Add your own application

* Name: EBS

Once you decide on a name for your new application, click the "Add" button below and we'll walk you through some simple configuration steps to get the application working.

Supports:

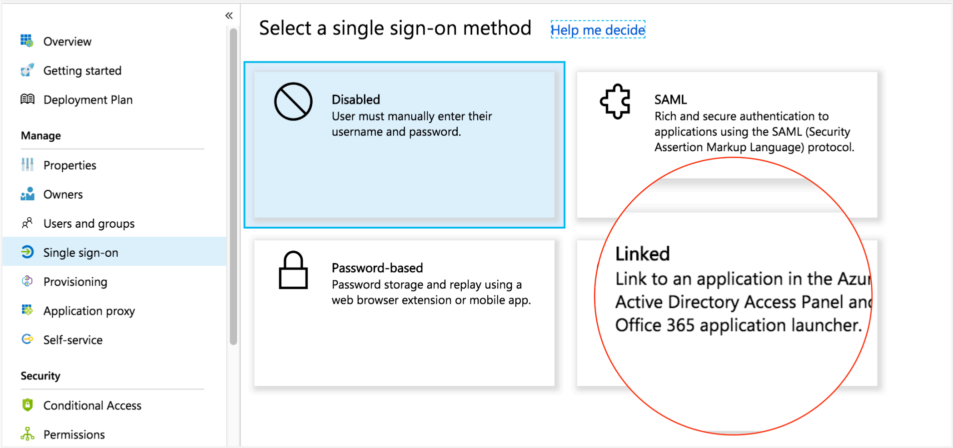
SAML-based single sign-on
Learn more

Automatic User Provisioning with SCIM
Learn more

Password-based single sign-on
Learn more

Add

4. For the new application, navigate to **Single sign-on** and select **Linked** as the single sign-on method.



Select a single sign-on method Help me decide

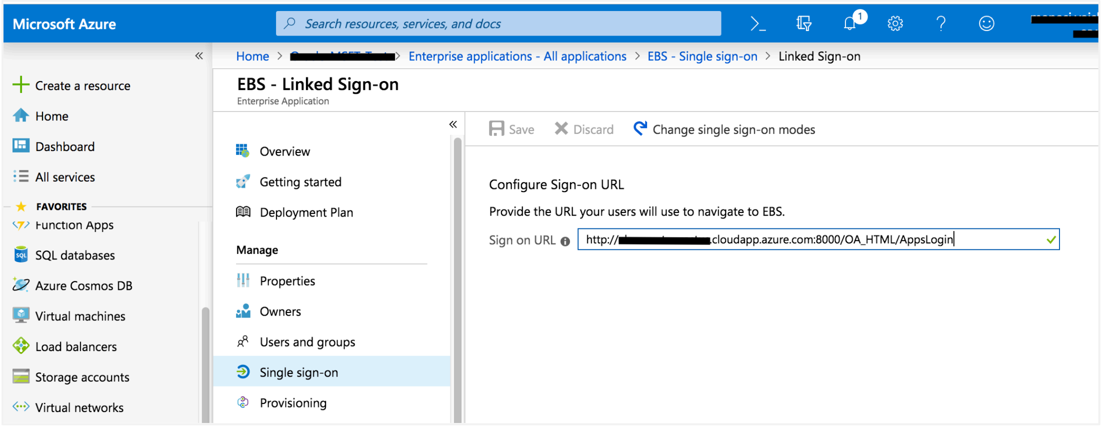
Disabled
User must manually enter their username and password.

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

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

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

5. Enter the URL of the application to link to, and then click **Save**.

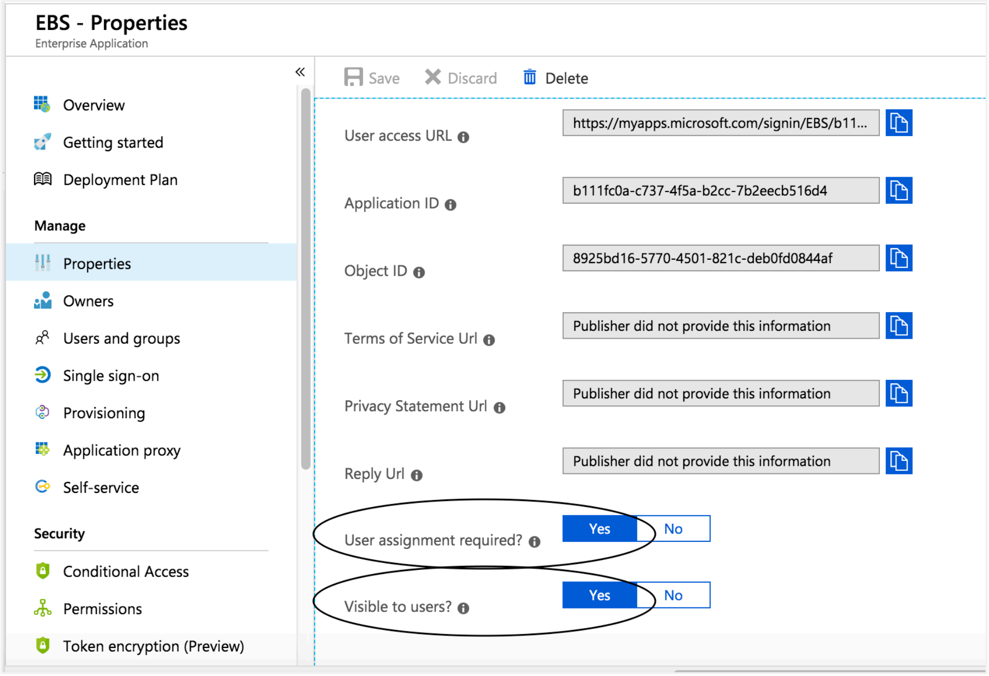


Configure Sign-on URL

Provide the URL your users will use to navigate to EBS.

Sign on URL: http://[redacted]cloudapp.azure.com:8000/OA_HTML/AppsLogin

6. In the properties for the application, verify that **User assignment required?** and **Visible to users?** are set to **Yes**.



User access URL: https://myapps.microsoft.com/signin/EBS/b11...

Application ID: b111fc0a-c737-4f5a-b2cc-7b2eecb516d4

Object ID: 8925bd16-5770-4501-821c-deb0fd0844af

Terms of Service Url: Publisher did not provide this information

Privacy Statement Url: Publisher did not provide this information

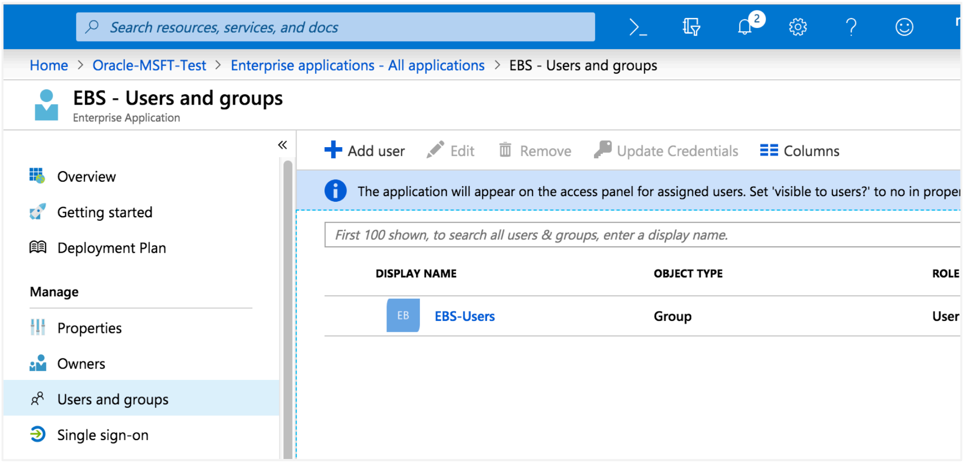
Reply Url: Publisher did not provide this information

User assignment required? [✓ Yes] No

Visible to users? [✓ Yes] No

7. [Create users, security groups, and group memberships in Azure](#).

8. Assign group-based access to the application in Azure AD.



The application will appear on the access panel for assigned users. Set 'visible to users?' to no in proper

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

DISPLAY NAME	OBJECT TYPE	ROLE
EB EBS-Users	Group	User

For more information about configuring single sign-on to non-gallery apps in Microsoft, see the Microsoft documentation.

9. After the E-Business Suite application is configured, you can configure conditional access policies in Azure AD to enhance the sign-on security for E-Business Suite.

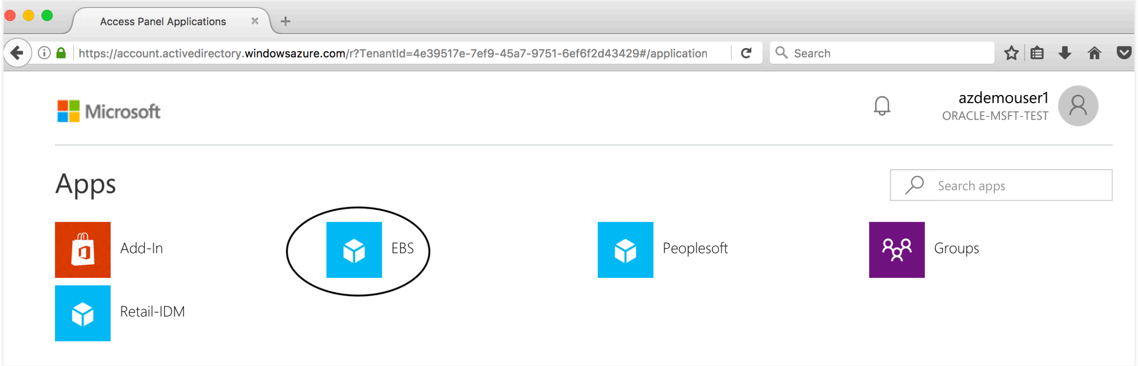
Verifying SSO

You can verify SSO that is initiated from the IDP and from the service provider (SP).

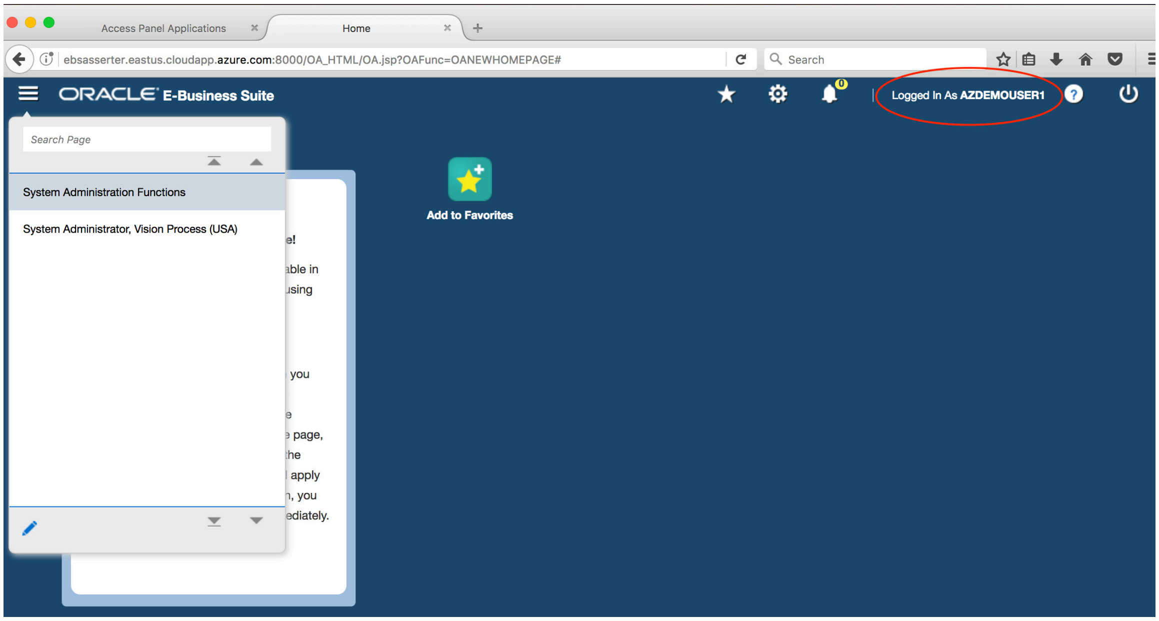
Verify IDP-Initiated SSO

1. Log in to the My Apps portal with a test user account that is also a member of the E-Business Suite (EBS) security group.

2. Click the E-Business Suite (EBS) application.


Access Panel Applications
https://account.activedirectory.windowsazure.com/r?TenantId=4e39517e-7ef9-45a7-9751-6ef6f2d43429#/application
Search
Microsoft
azdemouser1
ORACLE-MSFT-TEST
Apps
Search apps
Add-In
EBS
Peoplesoft
Groups
Retail-IDM

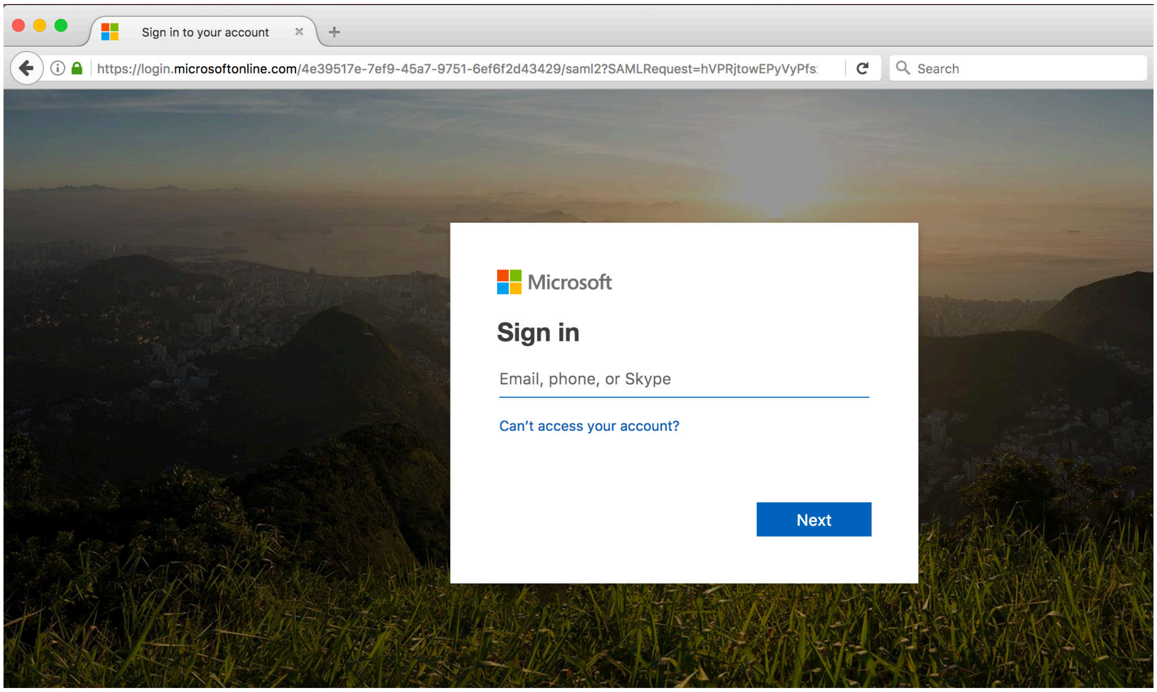
3. Verify the logged in username.


Access Panel Applications
Home
ebsasserter.eastus.cloudapp.azure.com:8000/OA_HTML/OA.jsp?OAFunc=OANEWHOMEPAGE#
Search
ORACLE E-Business Suite
Logged In As AZDEMOUSER1
Search Page
System Administration Functions
System Administrator, Vision Process (USA)
Add to Favorites

Verify SP-Initiated SSO

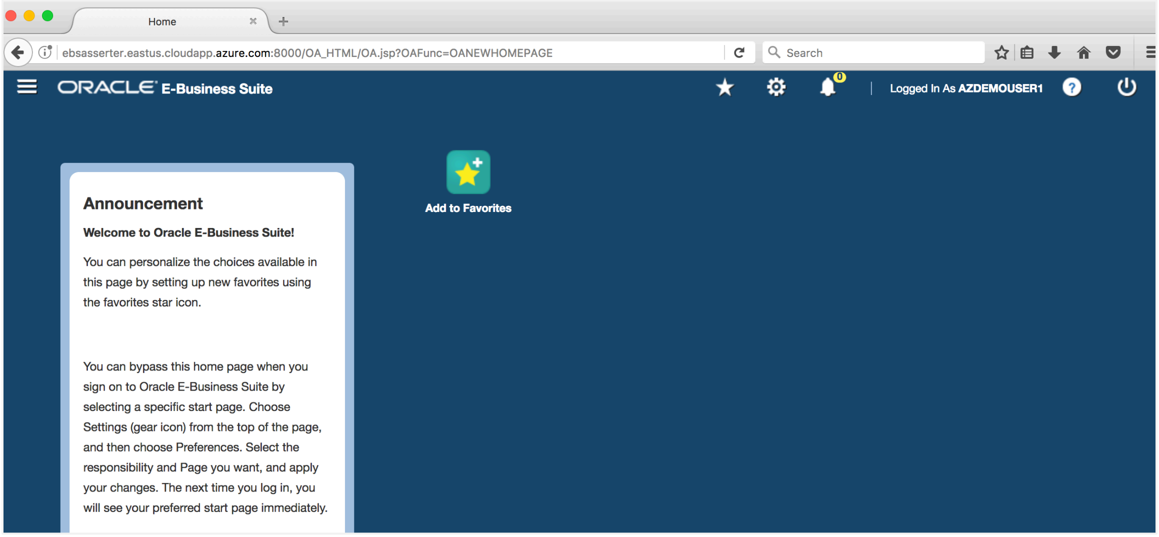
1. In a new browser window, enter the E-Business Suite AppsLogin URL.

   The Microsoft sign-in page appears.


Sign in to your account
https://login.microsoftonline.com/4e39517e-7ef9-45a7-9751-6ef6f2d43429/saml2?SAMLRequest=hVPRjtowEPyVyPfs
Search
Microsoft
Sign in
Email, phone, or Skype
Can't access your account?
Next

2. Enter your Microsoft Azure AD credentials.

   After you are authenticated, you should be redirected to E-Business Suite application.


Home
ebsasserter.eastus.cloudapp.azure.com:8000/OA_HTML/OA.jsp?OAFunc=OANEWHOMEPAGE
Search
ORACLE E-Business Suite
0
Logged In As AZDEMOUSER1
Add to Favorites

Announcement

Welcome to Oracle E-Business Suite!

You can personalize the choices available in this page by setting up new favorites using the favorites star icon.

You can bypass this home page when you sign on to Oracle E-Business Suite by selecting a specific start page. Choose Settings (gear icon) from the top of the page, and then choose Preferences. Select the responsibility and Page you want, and apply your changes. The next time you log in, you will see your preferred start page immediately.

Conclusion

Support for SSO protocols like SAML 2.0 makes interconnection between cross-cloud identity platforms secure and easier to set up. This white paper showcased how to configure SSO for the Oracle E-Business Suite application with Azure AD as the corporate identity provider.

ORACLE

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 Identity Cloud Service and Azure Active Directory
June 2019
Author: Manasi Vaishampayan (Oracle)
Contributing Author: Romit Girdhar (Microsoft)