



## North American Technology Division Solution Engineering Team

# 100 Oracle Public Cloud Workshop **Security: Identity Cloud Services Lab**

Update: March 5, 2018

## Introduction

This is the first of several labs that are part of the **Oracle Public Cloud Security and Management workshop**. This workshop will walk you through the various capabilities of **Oracle Identity Cloud Service**.

Although you will login as a single user, you will take on 2 personas during the workshop.

- The **LOB Administrator** persona will

Onboard users via CSV upload  
Setup and configure SSO Apps  
Configure external identity provider  
Configure MFA and policies

- The **End-User** persona will

Activate her account  
Setup and login using various MFA channels  
Request groups  
Verify SSO for apps from unified launchpad

## Objectives

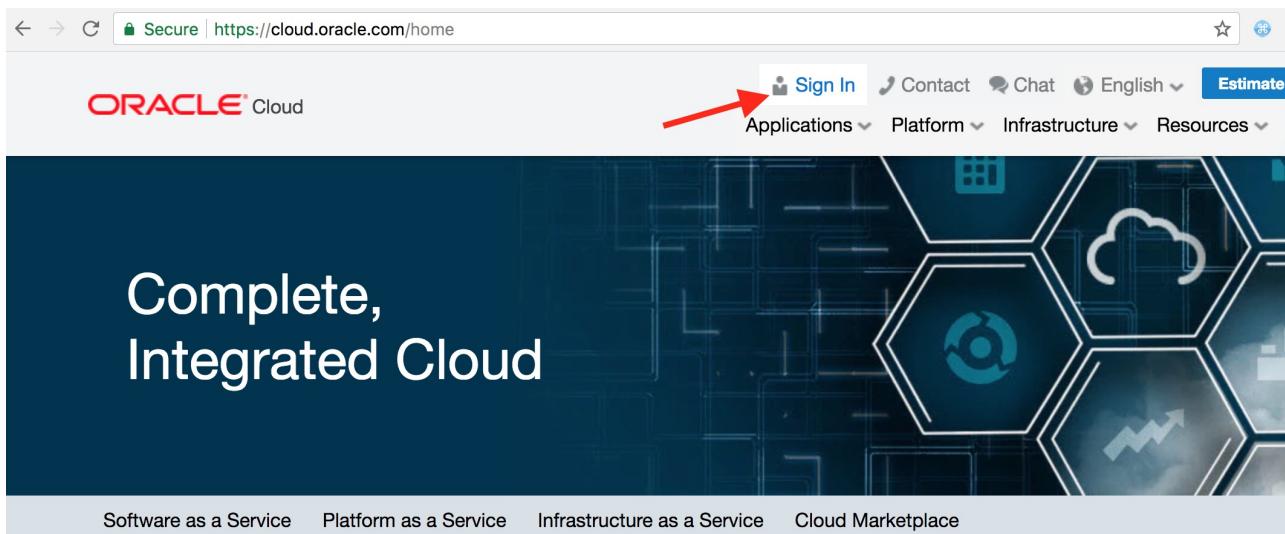
- In-built integration with Oracle cloud services <--Persona: Administrator
- Onboard users <--Persona: Administrator
- Configure SSO for an app <--Persona: Administrator
- Grant app to group <--Persona: Administrator
- Configure multi-factor authentication <--Persona: Administrator
- Activate account <--Persona: End-User
- Enroll in multi-factor authentication <--Persona: End-User
- Request group <--Persona: End-User
- Verify SSO <--Persona: End-User

## Pre-requisites

- The following lab requires an **Oracle Public Cloud** account trial subscription.

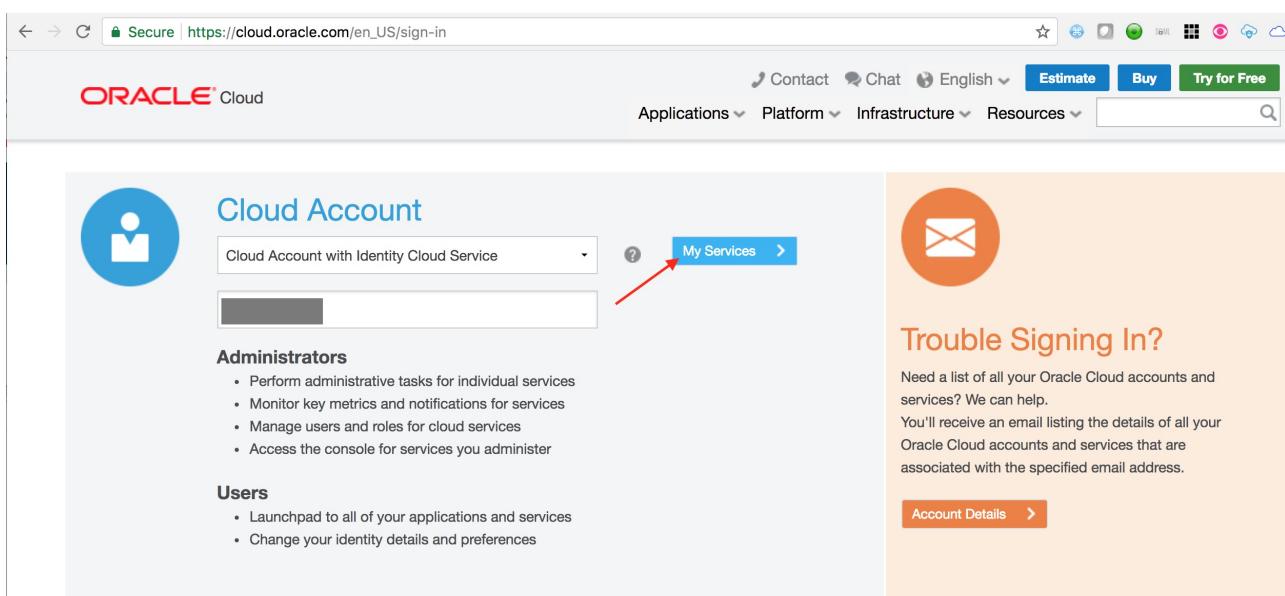
### STEP 0.1: Login to your Oracle Cloud Account

- From any browser, go to the URL:  
<https://cloud.oracle.com> (<https://cloud.oracle.com>)
- click **Sign In** in the upper right hand corner of the browser

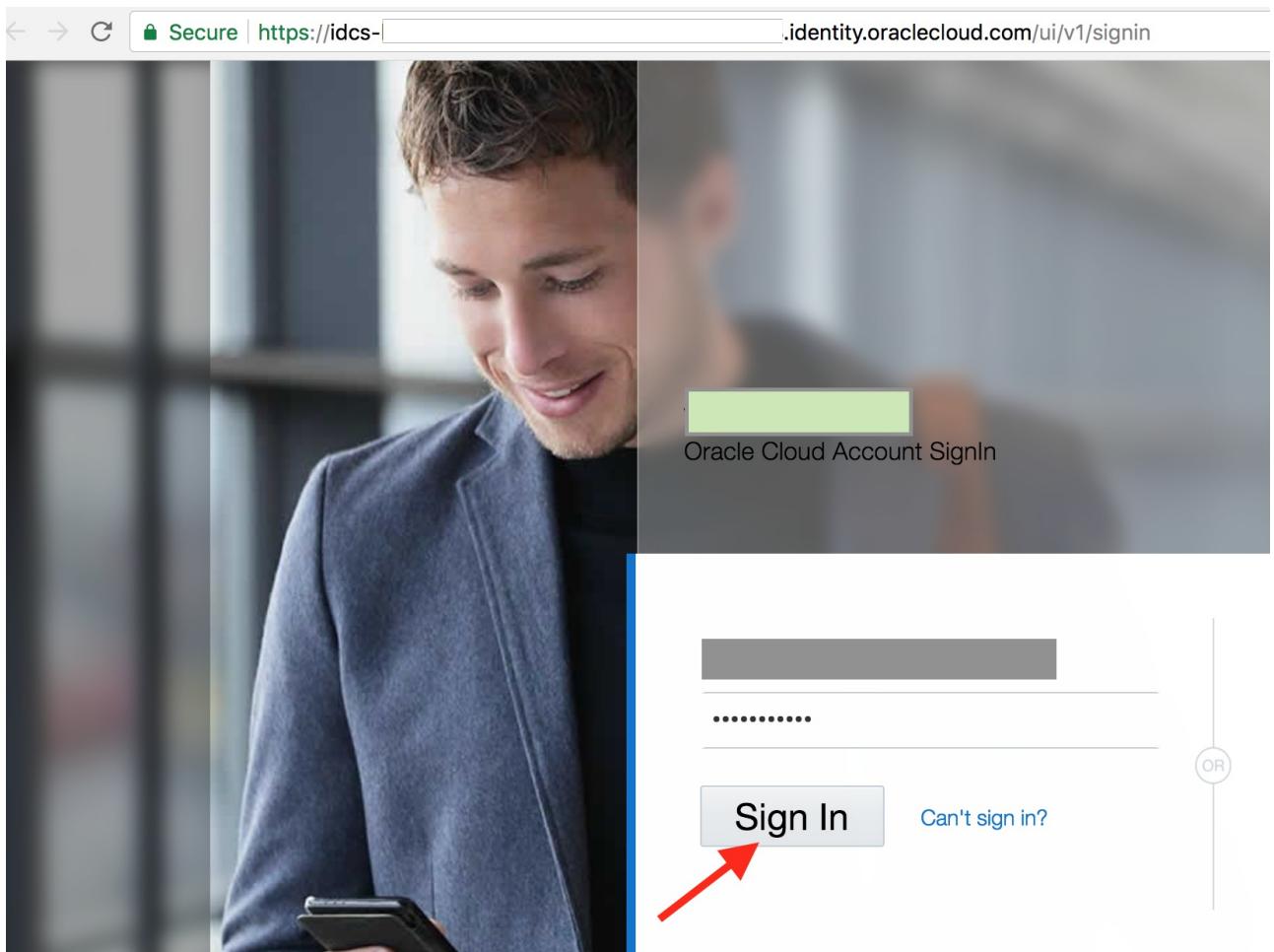


### Why Move to the Oracle Cloud

- Ensure **Cloud Account with Identity Cloud Service** is selected. Enter your cloud account name. Click on **My Services**



- On the login page, enter your user name and password and click **Sign In**



- You will be presented with a dashboard displaying the various cloud services available to this account.

A screenshot of the Oracle Cloud My Services dashboard. The URL in the address bar is https://myservices.console.oraclecloud.com/mycloud/cloudportal/dashboard. The dashboard has a blue header with the 'Dashboard' tab selected. It displays a summary section for 'Cloud Services' with a promotion for 'Upgrade to Paid' and '\$300 of \$300 Remaining'. Below this, there are two service cards: 'Oracle CASB' and 'Identity Cloud'. Both cards show a green checkmark icon and a 'Subscription ID' field. The 'Identity Cloud' card also shows an 'Instance' count of 1.

## STEP 0.2: Access IDCS Admin Console

- From the cloud **My Services** dashboard, click on **Users** in the upper right hand corner.

The screenshot shows the Oracle Cloud My Services dashboard. At the top right, there are several buttons: 'Dashboard', 'Users' (which has a red arrow pointing to it), 'Identity Domain', a bell icon, a question mark icon, and a user profile icon. Below the header, there's a 'Cloud Services' section with a 'Promotion' button labeled 'Upgrade to Paid', a notification count of '0 Important Notifications', and a budget status of '\$300 of \$300 USD Remaining'. At the bottom right of the dashboard area, there are buttons for 'Guided Journey', 'Account Management', 'Customize Dashboard', 'Create Instance', and a plus sign.

- Then click on **Identity Console** button located towards upper right hand corner again.

The screenshot shows the 'User Management' page under the 'Cloud My Services' menu. The title bar says 'User Management'. On the right side of the title bar, there is a 'Identity Console' button with a red arrow pointing to it. Below the title bar, there are tabs for 'Users' (which is selected) and 'My Profile'. There is a search bar, a sort dropdown set to 'Last Name (Ascending)', and a grid view button. The main content area displays a user profile for 'waymon whiting' with a blue circular icon containing 'WW'. Below the icon, the name 'waymon whiting' is displayed. Underneath the name, there is an 'Email:' field with a redacted email address. At the bottom left, there is a page navigation bar showing 'Page 1 of 1 (1 of 1 items)'.

- If you have logged in using your administrator Account, the users are shown up in IDCS admin console.

The screenshot shows the 'Users' list in the Oracle Identity Cloud Service (IDCS) Admin Console. The URL in the browser is <https://idcs-identity.oraclecloud.com/ui/v1/adminconsole/?root=users>. The page title is 'Identity Cloud Service - Users'. At the top, there are buttons for 'Select All', '+ Add', 'Import', 'Export', 'Activate', 'Deactivate', and 'More'. The main content area lists a single user entry: 'waymon whiting' with a blue circular icon containing 'WW'. To the right of the name is an 'Email' field with a redacted email address. There are also edit and delete icons next to the user entry.

### STEP 0.3: Access IDCS MyApp Console

- From the drop-down associated with the displayed logged-in user in the upper right hand corner of IDCS admin console, choose **My Apps**

The screenshot shows the Oracle Identity Cloud Service (IDCS) admin console. The top navigation bar includes the Oracle logo, the service name "Identity Cloud Service", and a search bar. Below the header, there are buttons for "Select All", "Add", "Import", "Export", "Activate", "Deactivate", and "More". The main content area is titled "Users" and displays a single user entry for "waymon whiting" with an email placeholder. In the top right corner, a user profile icon labeled "WW" has a dropdown menu with options: Help, My Apps (which is highlighted with a red arrow), My Home, About, and Sign Out.

The screenshot shows the Oracle My Apps dashboard. The top navigation bar includes the Oracle logo and a search bar. Below the header, there are buttons for "Favorites" and "Add". The main content area is titled "My Apps" and displays two application tiles: "Casb\_Sso-4c3876" and "OCI Integration". In the top right corner, a user profile icon labeled "WW" has a dropdown menu with options: Help, Catalog, My Profile, Admin Console, My Home, My Services (which is highlighted with a red arrow), About, and Sign Out.

## Scenario: Integration with Oracle cloud services

- From the drop-down associated with the displayed logged-in user in the upper right hand corner of IDCS admin console, choose **My Services** to come back to the cloud dashboard.

This screenshot is identical to the one above, showing the Oracle My Apps dashboard. The top navigation bar includes the Oracle logo and a search bar. Below the header, there are buttons for "Favorites" and "Add". The main content area is titled "My Apps" and displays two application tiles: "Casb\_Sso-4c3876" and "OCI Integration". In the top right corner, a user profile icon labeled "WW" has a dropdown menu with options: Help, Catalog, My Profile, Admin Console, My Home, My Services (which is highlighted with a red arrow), About, and Sign Out.

- Display the sidebar by clicking on the hamburger menu in the upper left hand corner. then expand **Services** to display available Oracle cloud services.

The screenshot shows the Oracle Cloud My Services dashboard. On the left, a sidebar menu is open under the 'Services' heading, with several service categories listed: Compute, Compute Classic, Storage Classic, Java, Database, Analytics, API Platform, Apairy, Application Container, Big Data - Compute Edit..., Container Classic, Data Hub Cloud Service, and Data Integration Platfor... A red arrow points from the text 'Click on the service Analytics.' to the 'Analytics' option in the sidebar.

- Click on the service **Analytics**.

The screenshot shows the Oracle Cloud My Services dashboard. The 'Analytics' service is now selected in the sidebar, indicated by a red arrow. The main content area displays various service cards, including 'Cloud Services' (with a promotion for \$300 USD), 'Oracle CASB' (Subscription ID: [redacted]), and 'Identity Cloud' (Subscription ID: [redacted], Instance 1). The 'Identity Cloud' card shows 'No data to display' for both 'Identity Cloud Service Basic - Enterprise' and 'IDCS Foundation (Unit Per)'.

- On the **Analytics** console, click on **Go to Console**

The screenshot shows the Oracle Analytics Cloud interface. At the top, there's a navigation bar with links for 'Instances' and 'Activity'. Below this is a large blue banner with the text 'Welcome to ORACLE ANALYTICS CLOUD!' and a sub-section titled 'GO FROM ZERO TO DEPLOYED APPLICATION TODAY'. It includes three buttons: 'Watch Video', 'Follow Tutorial', and a prominent yellow 'Go to Console' button. A red arrow points to the 'Go to Console' button.

- Observe that the logged in user has successfully single signed-on to the **Analytics** service console

The screenshot shows the 'Instances' page of the Oracle Analytics Cloud console. It features a header with 'Instances' and 'Activity' tabs. Below the header, it says 'As of Mar 3, 2018 5:15:18 PM UTC'. A 'Create Instance' button is visible. A red arrow points to this button. A blue curved arrow points from the 'Create Instance' button towards the text 'You don't have any instances. After meeting the [prerequisites](#), use this button to create an instance.'

## Scenario – Standard Employee Workflow

### Onboard Users – (Persona: Administrator)

IDCS supports user (also groups) on-boarding from on-premise **Active Directory**, using file upload, REST API, on-premise **Oracle Identity Management** solution, or manually from IDCS admin console.

For the exercise we will be using file upload option for users.

#### STEP 1: Obtain upload CSV file

- Download the CSV file for users from [here \(resources/Users.csv\)](#). Right-click on the link and save the file in your system. Inspect the content of the file from your favorite editor.

#### STEP 2: Import users in IDCS

- Click on the **Users** icon from top right corner assuming you are still on the **Analytics** console.

The screenshot shows the Oracle Analytics Cloud Instances page. At the top right, there is a user icon with a red arrow pointing to it. The page also features a blue header bar with the Oracle logo and the text "Oracle Analytics Cloud". Below the header, there are tabs for "Instances" and "Activity". A message in the center says "You don't have any instances. After meeting the [prerequisites](#), use this button to create an instance." A blue "Create Instance" button is located below the message.

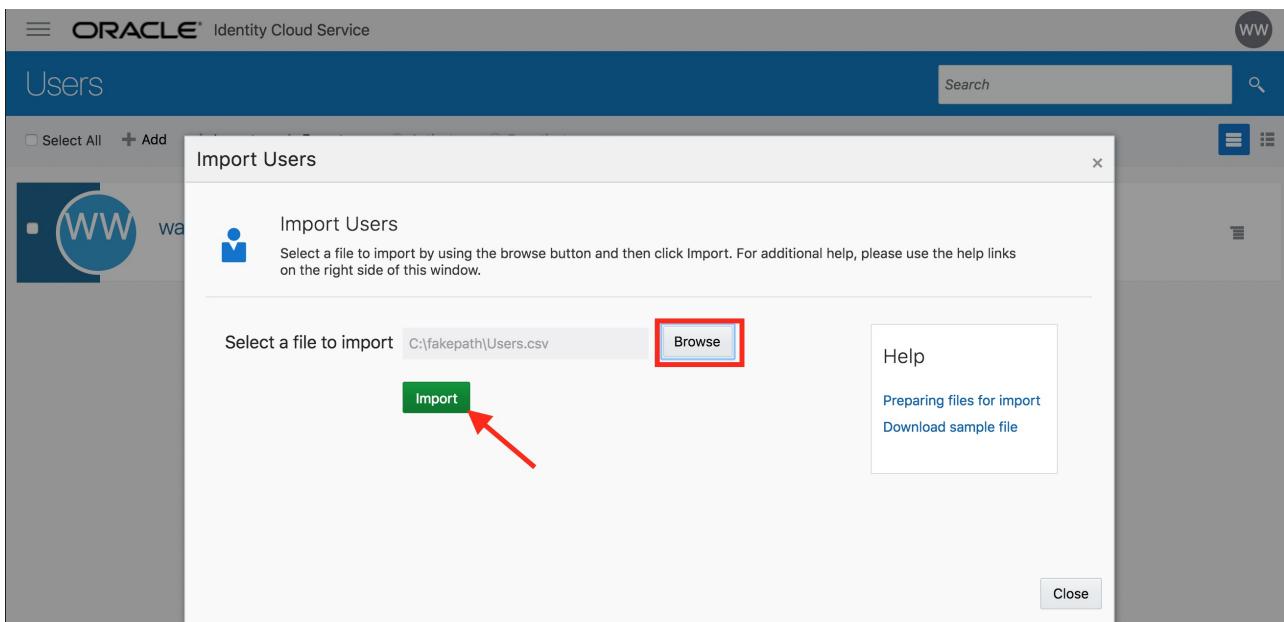
- Click on **Identity Console** from top right corner of the **User Management** page.

The screenshot shows the Oracle Cloud My Services User Management page. At the top right, there is a "Identity Console" button with a red arrow pointing to it. The page has a blue header bar with the Oracle logo and the text "User Management". Below the header, there are tabs for "Users" and "My Profile". A search bar and sorting options are also present. A user profile for "waymon whiting" is shown, featuring a blue circular icon with "WW" and the name "waymon whiting".

- On the **Users** page, click on the **Import** button.

The screenshot shows the Oracle Identity Cloud Service Users page. At the top left, there is an "Import" button with a red arrow pointing to it. The page has a blue header bar with the Oracle logo and the text "Users". Below the header, there are buttons for "Select All", "Add", "Import", "Export", "Activate", "Deactivate", and "More". A user profile for "waymon whiting" is shown, featuring a blue circular icon with "WW" and the name "waymon whiting".

- Select the **CSV** file that you saved locally. Click on **Import**



- Go to the **Jobs** tab in admin console. Verify that the import Job finished successfully. Click on **View Details** button.

Job ID 2de3d7c361ec4da59609849441f2efe2

<b>Status</b>	<b>User Import Job</b>	<b>Start Time</b>
Successful	Job Type	Mar 4, 2018 1:43:43 PM
100%		

- This will show the detailed information on the **Import** job. Inspect the details.

First Name	Last Name	Email	User Name	Status
Peter	Pan	demoidcs+user29@gmail.com	ppan	Creation Succeeded
Maria	Powell	demoidcs+user26@gmail.com	mpowell	Creation Succeeded
Chuck	Miller	demoidcs+user18@gmail.com	cmiller	Creation Succeeded
John	Hope	demoidcs+user15@gmail.com	jhope	Creation Succeeded
John	Schultz	demoidcs+user13@gmail.com	jschultz	Creation Succeeded

- Congratulations, you successfully imported users into IDCS.

## STEP 3: Verify user creation

- Go to the **Users** menu in admin console. Verify that the new users are visible on the console.

The screenshot shows two parts of the Oracle Identity Cloud Service Admin Console.

**Top Panel (Jobs Page):**

- Left sidebar: Dashboard, Users (highlighted with a red arrow), Groups, Applications, Jobs (selected), Reports, Settings, Security, My Services.
- Job ID: Job 2de3d7c361ec4da59609849441f2efe2 completed Successfully.
- Job Details:
 

Percent Complete	100 %	Total Users	32	Users imported	32	Users failed to import	0
Request Created on Date/Time	Mar 4, 2018 1:43:43 PM	Start Run Date/Time	Mar 4, 2018 1:43:43 PM	End Run Date/Time	Mar 4, 2018 1:43:46 PM		

**Bottom Panel (Users List):**

- Left sidebar: Dashboard, Users (highlighted with a red arrow), Groups, Applications, Jobs, Reports, Settings, Security, My Services.
- Users List:
 

User ID	User Name	Email	Mobile Number
AO	Amy Olsen Mrs	Email demoidcs+user12@gmail.com...	Mobile Number 9800000001
AY	Angus Young Mr	Email demoidcs+user28@gmail.com...	Mobile Number 9800000001
AT	Anna Torres Ms	Email demoidcs+user19@gmail.com...	Mobile Number 9800000001
BJ	Ben Jones Mr	Email demoidcs+user16@gmail.com...	Mobile Number 9800000001
BB	Beth Berg Ms	Email demoidcs+user21@gmail.com...	Mobile Number 9800000001
BR	Bill Ryan Mr	Email demoidcs+user31@gmail.com...	Mobile Number 9800000001
CP	Carol Pitt Mrs	Email demoidcs+user25@gmail.com...	Mobile Number 9800000001
CM	Chuck Miller Mrs	Email demoidcs+user18@gmail.com...	Mobile Number 9800000001
CB	Cora Burks Ms	Email demoidcs+user9@gmail.com...	Mobile Number 9800000001
DC	Danny Crane Mr	Email demoidcs+user1@gmail.com...	Mobile Number 9800000001
EL	Eric Lee Mr	Email demoidcs+user17@gmail.com...	Mobile Number 9800000001
EC	Ernie Chen Mr	Email demoidcs+user5@gmail.com...	Mobile Number 9800000001

- Click on your target end-user and verify user's detailed attribute information.

User assignments will be provided before the session.

## Configure SSO for an app – (Persona: Administrator)

Oracle Identity Cloud Service(IDCS) provides integration with any service that can be integrated via **SAML** (Security Access Markup Language) protocol. Administrations will be able to manage users into various applications via single control panel and end users will be able to get to applications via single click.

IDCS provides support for standard SAML 2.0 browser POST login & logout profiles.

In this hands-on exercise, we will setup integration with **Salesforce** using SAML. IDCS will act as **IdP** (Identity Provider) and Salesforce org as **SP** (Service Provider also known as a Relying Party)

- Download and save IDCS Metadata to a local XML file for your instance. Metadata is available from the following location –

<https://idcs-xxxxxx.identity.oraclecloud.com/fed/v1/metadata>  
where idcs-xxxxxx is your IDCS tenant name that you can grab from the browser URL of your IDCS console. Copy-paste the constructed URL on a new browser tab and save the XML file locally.

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```

<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:dsig="http://www.w3.org/2000/09/xmldsig#" xmlns:enc="http://www.w3.org/2001/04/xmlenc#"
  xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute" xmlns:query="urn:oasis:names:tc:SAML:metadata:ext:query" xmlns:saml="urn:oasis:names:tc:SAML:1.2:assertion"
  xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" ID="id-9pv6cRCDPeNsZohGyET-vxOCNWY-"
  cacheDuration="P3644DT0H0M0S" entityID="https://idcs-xxxxxx.identity.oraclecloud.com/fed" validUntil="2027-12-05T17:36:06Z">
  <dsig:Signature>
    <dsig:SignedInfo>
      <dsig:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      <dsig:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
    </dsig:SignedInfo>
    <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/2001/04/xmlenc#sha256" />
  </dsig:Signature>
</md:EntityDescriptor>

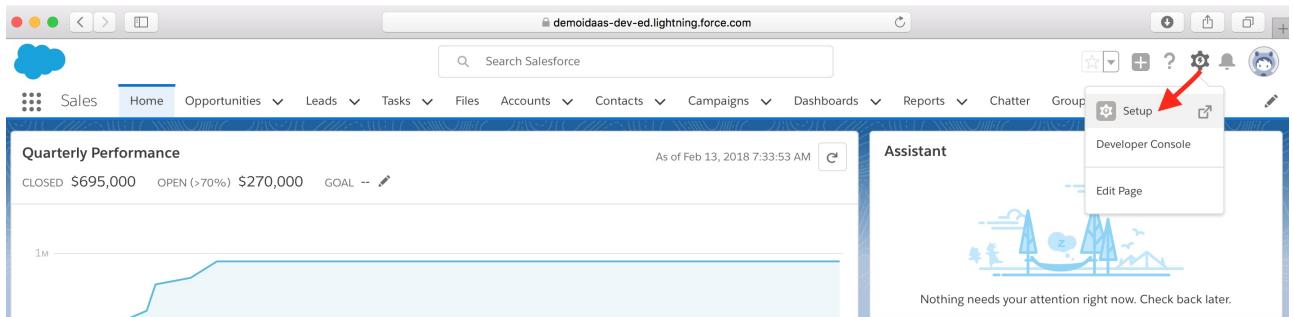
```

Following activities on Salesforce is optional. Email the metadata XML to your proctor.

- Login to the **Salesforce** developer account (<https://demoidaa-dev-ed.my.salesforce.com>)

Credentials will be provided during session.

- Bring up the **setup** page.



- From side menu bar, go to **Settings** -> **Identity** -> **Single Sign-On Settings**

A screenshot of the Salesforce Setup interface. On the left, there's a sidebar with a "Feature Settings" section containing "Objects and Fields", "Process Automation", "User Interface", "Custom Code", and "Environments". Below that is an "Integrations (BETA)" section with "SETTINGS" highlighted. Under "SETTINGS", there are sections for "Company Settings", "Identity" (which is expanded to show "Auth. Providers", "Identity Connect", "Identity Provider", "Identity Verification History", "Login Flows", "Login History", and "Single Sign-On Settings"), and "Security". A red arrow points to the "Single Sign-On Settings" link in the sidebar. The main content area shows the "Single Sign-On Settings" page with the title "Single Sign-On Settings". It includes a sub-section "Federated Single Sign-On Using SAML" with a "SAML Enabled" checkbox. Below that is a "SAML Single Sign-On Settings" section with buttons for "New", "New from Metadata File", and "New from Metadata URL". A red box highlights the "Edit" button in the "Federated Single Sign-On Using SAML" section. At the top of the page, there's a search bar labeled "Search Setup" and a "Help for this Page" link.

- Click on **Edit** and enable **Federated Single Sign-On Using SAML** option. Click on **Save**.

Single Sign-On Settings | Salesforce

Setup ▾ Home Object Manager ▾

Feature Settings

Objects and Fields

Process Automation

User Interface

Custom Code

Environments

Integrations (BETA)

SETTINGS

Company Settings

Identity

- Auth. Providers
- Identity Connect
- Identity Provider
- Identity Verification History
- Login Flows
- Login History

Single Sign-On Settings

SETUP Single Sign-On Settings

Single Sign-On Settings

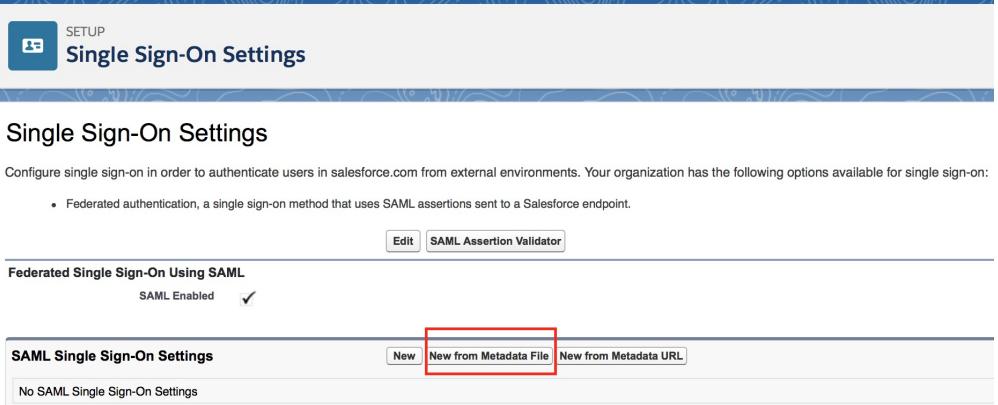
Federated Single Sign-On Using SAML

SAML Enabled

Save Cancel

- Click on **New from Metadata File** button to import IDCS metadata. Select the downloaded metadata XML file using **Choose File** button. Click on **Create**.

Single Sign-On Settings | Salesforce



Setup Home Object Manager

Feature Settings

Objects and Fields

Process Automation

User Interface

Custom Code

Environments

Integrations (BETA)

SETTINGS

Company Settings

Identity

Auth. Providers

Identity Connect

Identity Provider

Identity Verification History

Login Flows

Login History

Single Sign-On Settings

Single Sign-On Settings

Configure single sign-on in order to authenticate users in salesforce.com from external environments. Your organization has the following options available for single sign-on:

- Federated authentication, a single sign-on method that uses SAML assertions sent to a Salesforce endpoint.

Edit SAML Assertion Validator

Federated Single Sign-On Using SAML

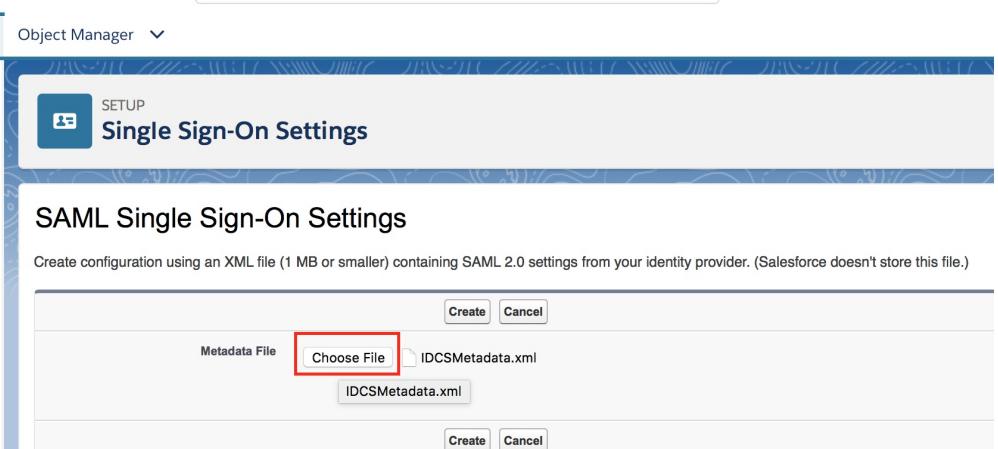
SAML Enabled ✓

SAML Single Sign-On Settings

New New from Metadata File New from Metadata URL

No SAML Single Sign-On Settings

Single Sign-On Settings | Salesforce



Setup Home Object Manager

Feature Settings

Objects and Fields

Process Automation

User Interface

Custom Code

Environments

Integrations (BETA)

SETTINGS

Company Settings

Identity

Auth. Providers

Identity Connect

Identity Provider

Identity Verification History

Login Flows

Login History

Single Sign-On Settings

SAML Single Sign-On Settings

Create configuration using an XML file (1 MB or smaller) containing SAML 2.0 settings from your identity provider. (Salesforce doesn't store this file.)

Metadata File Choose File IDCSSMetadata.xml

IDCSSMetadata.xml

Create Cancel

- Keep all the default information and click on **Save**

Salesforce Single Sign-On Settings

**SAML Single Sign-On Settings**

Name: idcs-  
SAML Version: 2.0  
Issuer: https://idcs-  
Identity Provider Certificate: Choose File, no file selected  
Request Signing Certificate: SelfSignedCert\_24Jan2018\_202257  
Request Signature Method: RSA-SHA256  
Assertion Decryption Certificate: Assertion not encrypted  
SAML Identity Type: Assertion contains the User's Salesforce username  
SAML Identity Location: Identity is in the NameIdentifier element of the Subject statement  
Service Provider Initiated Request Binding: HTTP POST  
Identity Provider Login URL: https://idcs-  
Custom Logout URL: identity.oraclecloud.com/fi  
Custom Error URL:  
Single Logout Enabled: checked  
Identity Provider Single Logout URL: https://idcs-  
Single Logout Request Binding: HTTP POST  
HTTP Redirect  
Just-in-time User Provisioning: User Provisioning Enabled: checked

API Name: idcs-  
Entity ID: https://demoidaas-dev-ed  
Current Certificate: CN=idcs-, CN=Cloud9, CN=sslDomains  
Expiration: 5 Dec 2027 17:36:06 GMT

Oracle Cloud Service Single Sign-On Settings

**SAML Single Sign-On Settings**

Name: idcs-  
SAML Version: 2.0  
Issuer: https://idcs-  
Identity Provider Certificate: CN=idcs-, CN=Cloud9, CN=sslDomains  
Request Signing Certificate: SelfSignedCert\_24Jan2018\_202257  
Request Signature Method: RSA-SHA256  
Assertion Decryption Certificate: Assertion not encrypted  
SAML Identity Type: Username  
SAML Identity Location: Subject  
Service Provider Initiated Request Binding: HTTP Redirect  
Identity Provider Login URL: https://idcs-  
Custom Logout URL:  
Custom Error URL:  
Single Logout Enabled: checked  
Identity Provider Single Logout URL: https://idcs-  
Single Logout Request Binding: HTTP Redirect

Just-in-time User Provisioning: User Provisioning Enabled: checked

Endpoints: View SAML endpoints for your organization, communities, or custom domains.  
Your Organization: Login URL: https://demoidaas-dev-ed.my.salesforce.com?so=00D1N000002M18V  
Logout URL: https://demoidaas-dev-ed.my.salesforce.com/services/auth/sp/saml2/logout  
OAuth 2.0 Token Endpoint: https://demoidaas-dev-ed.my.salesforce.com/services/oauth2/token?so=00D1N000002M18V

- Go to IDCS admin console -> Applications menu

ORACLE Identity Cloud Service

Status: Active

DC

Danny Crane  
Mr

Details Groups Access

Reset Password Deactivate Remove More

Update User

Account Information

- On the Applications page, click on Add and select App Catalog on the pop-up.

The screenshot shows the Oracle Identity Cloud Service interface. On the left, there's a sidebar with various navigation options like Dashboard, Users, Groups, Applications, Jobs, Reports, Settings, and Security. The 'Applications' option is selected. The main area is titled 'Applications' and shows a list of existing applications. A modal window titled 'Add Application' is open, listing four options: 'App Catalog', 'SAML Application', 'Mobile Application', and 'Trusted Application'. The 'App Catalog' option is highlighted with a red arrow.

- Search for **Salesforce** app and click on Add

The screenshot shows the 'App Catalog' search results for 'salesforce'. The search bar at the top has 'salesforce' entered. Below it, the results are displayed under the heading 'Search Results: 249'. There are two sections of results. The first section shows results from various categories, and the second section shows results specifically for 'Salesforce'.

Category	Application Name	Type	Add Button
&frankly	&frankly	SAML	Add
101domains.com	101domains.com	Form Fill	Add
15Five	15Five	SAML	Add
48HourPrint	48HourPrint	Form Fill	Add
7Geese	7Geese	SAML	Add

The screenshot shows the 'App Catalog' search results for 'salesforce'. The search bar at the top has 'salesforce' entered. Below it, the results are displayed under the heading 'Search Results: 1'. One result is shown for 'Salesforce'.

Category	Application Name	Type	Add Button
	Salesforce	Salesforce Application SAML	Add

- On the first page of configuration screen enter the **Organization ID** and **Domain Name** values as provided below. Then click on **Next**.

These values are exactly same as those found in the IDCS settings in Salesforce you just configured.

Domain Name : demoidaaas-dev-ed  
Organization ID : 00D1N000002M18V

The screenshot shows the Oracle Identity Cloud Service interface for adding a new application. The left sidebar is dark with white icons and text, showing 'Applications' as the active section. The main area has a light background. At the top, it says 'Add Salesforce'. Below that is a progress bar with 'Details' and 'SSO Configuration' steps. The 'Details' step is active. On the right, there's a 'Next >' button with a red arrow pointing to it. The 'App Details' section contains fields for 'Name' (Salesforce) and 'Description' (Salesforce Application). An 'Application Icon' is shown as a small blue cloud with the word 'salesforce'. Below this is a table of 'App Links' with three items: 'Salesforce Application', 'Salesforce Work.com', and 'Salesforce Chatter'. Underneath the table are two input fields: 'Domain Name' (demoidaaas-dev-ed) and 'Organization ID' (00D1N000002M18V), both of which are highlighted with a red box. There are also 'Custom Login URL' and 'Custom Logout URL' fields below. At the bottom of the page are 'Cancel' and 'Next >' buttons.

- Click on **Finish** button

This screenshot shows the 'SSO Configuration' step of the application setup. The left sidebar is identical to the previous screen. The main area has a light background. At the top, it says 'Add Salesforce'. Below that is a progress bar with 'Details' and 'SSO Configuration' steps. The 'SSO Configuration' step is active. On the right, there's a 'Back' button and a 'Finish' button with a red arrow pointing to it. There are also 'Download Signing Certificate' and 'Download Identity Provider Metadata' buttons. The 'General' section contains a note about defining SAML assertion attributes and uploading a signing certificate. It has a 'Signing Certificate' field with an 'Upload' button. Below that is an 'Advanced Settings' section with a plus sign icon. The 'Domain Name' and 'Organization ID' fields from the previous screen are still highlighted with a red box at the bottom of the page.

- Activate the application

The screenshot shows the Oracle Identity Cloud Service (IDCS) interface. On the left, there is a dark sidebar with various navigation options: Dashboard, Users, Groups, Applications (selected), Jobs, Reports, Settings, Security, and My Services. The main content area is titled "ORACLE Identity Cloud Service" and "Applications > Salesforce". It displays a "Salesforce" application card with a blue icon, labeled "Salesforce Application". Below the card, there are tabs for "Details", "SSO Configuration", "Users", and "Groups". The "Details" tab is selected. Under "App Details", there is a form with fields: "Name" (Salesforce) and "Description" (Salesforce Application). To the right of the form are "Save" and "Activate" buttons. A red arrow points to the "Activate" button.

This screenshot shows the same IDCS interface as the previous one, but with a modal dialog box centered over the application list. The dialog is titled "Activate Application?" and contains the message "Are you sure that you want to activate the application Salesforce?". It has two buttons: "Activate Application" (highlighted with a red arrow) and "Cancel". In the background, the application list table is visible, showing three entries: "Salesforce Work.com", "Salesforce Chatter", and "Salesforce Application".

This screenshot shows the IDCS interface after the activation process. The top status bar is green and displays the message "The Salesforce application has been activated." The main content area shows the "Salesforce" application card and its details. The "Activate" button is now grayed out and labeled "Deactivate". The "Save" button is present at the bottom right.

Congratulations, you successfully added and activated an application in IDCS.

## Grant app to group – (Persona: Administrator)

- Go to IDCS admin console -> **Groups** menu

The screenshot shows the Oracle Identity Cloud Service interface. On the left, a sidebar menu includes options like Dashboard, Users, Groups (which has a red arrow pointing to it), Applications, Jobs, Reports, Settings, Security, and My Services. The main content area is titled "ORACLE® Identity Cloud Service" and "Applications > Salesforce". It displays a "Salesforce" application card with a blue cloud icon. Below the card are tabs for Details, SSO Configuration, Users, and Groups. A green "Save" button is visible. The "App Details" section contains fields for Name (Salesforce) and Description (Salesforce Application).

- Add group **Employees**. Check the box User can request access. Click on **Finish**

The first part of the screenshot shows the "Groups" page with a red box around the "Groups" menu item in the sidebar. An arrow points to the "Add" button in the top navigation bar. The second part shows a modal window titled "Add Group" with a sub-section titled "Step 1: Groups Details". In this window, the "Name" field is set to "Employees" and the "User can request access" checkbox is checked (indicated by a red box). At the bottom right of the modal are "Next" and "Finish" buttons.

The screenshot shows the Oracle Identity Cloud Service interface. On the left, a dark sidebar menu includes options like Dashboard, Users, Groups (which is selected), Applications, Jobs, Reports, Settings, Security, and My Services. The main content area is titled "Groups > Employees". A success message at the top says "Group Employees has been successfully added." A red arrow points to the "Access" tab in the navigation bar below. The "Details" tab is currently selected. Below the tabs, there are fields for "Name" (Employees) and "Description" (Description). A checkbox for "User can request access" is checked. A green "Update" button is visible on the right.

- Go to the **Access** tab. Click on **Assign**.

This screenshot shows the "Assign Applications" dialog box overlaid on the Oracle Identity Cloud Service interface. The dialog has a header "Assign Applications" and a message "Please select up to 40 applications to assign.". It features a "Select All" checkbox and a search bar. Below is a list of applications: Casb\_Sso-4c3876, OCI Integration, and Salesforce. The checkbox next to Salesforce is checked. At the bottom, it says "Selected: 1" and "Clear Selection". A red arrow points to the "Assign" button in the top right of the dialog. The background shows the "Employees" group page with the "Access" tab selected. A green "Assign Applications" button is visible on the page.

- Select **Salesforce** and confirm

This screenshot shows the "Assign Applications" dialog box with the "Salesforce" application selected. The "Selected: 1" count is shown. A red arrow points to the "OK" button in the bottom right corner of the dialog. The background shows the "Employees" group page with the "Access" tab selected. A green "Assign Applications" button is visible on the page.

The screenshot shows the Oracle Identity Cloud Service (IDCS) interface. On the left sidebar, 'Groups' is selected. The main content area displays the 'Employees' group details. A success message 'The Salesforce application is assigned to Employees.' is shown in a green box with a checkmark. Below it, the 'Access' tab is selected. A search bar and a 'Select All' checkbox are present. An 'Assign' button is available to add more applications. The 'Salesforce' application is listed as assigned to the group.

- Congratulations, you successfully created a group and assigned it.

## Configure multi-factor authentication – (Persona: Administrator)

When a user signs in to an application, they are prompted for their user name and password, which is the first factor – something that they know. With **Multi Factor Authentication (MFA)** enabled in Oracle Identity Cloud Service, the user is then required to provide a second type of verification. This is called **2-Step Verification**.

The two factors work together to add an additional layer of security by using either additional information or a second device to verify the user's identity and complete the login process.

- From IDCS admin console, select **Security** → **MFA** from the sidebar to the left.

The screenshot shows the Oracle Identity Cloud Service interface. On the left, a dark sidebar lists various navigation items: Dashboard, Users, Groups (which is selected and highlighted in blue), Applications, Jobs, Reports, Settings, Security (expanded to show Administrators, Identity Providers, IDP Policies, Sign-On Policies, Network Perimeters, and MFA), and My Services. A red arrow points to the 'MFA' option under the Security section. The main content area is titled 'Groups > Employees' and shows the 'Employees' group details. It includes tabs for Details, Users (selected), and Access. Below these are search and filter controls, followed by a list item for 'Salesforce' with a checkbox, a 'Select All' button, an 'Assign' button with a plus sign, and a 'Revoke' button with a minus sign.

- Select all the options for **Select the factors that you want to enable**. Keep all other parameters to their default values. Click on **Save**.

Multi-Factor Authentication (MFA) Settings

Select the factors that you want to enable: ⓘ

<input checked="" type="checkbox"/> Security Questions	Configure
<input checked="" type="checkbox"/> Mobile App OTP	Configure
<input checked="" type="checkbox"/> Mobile App Notification	Configure
<input checked="" type="checkbox"/> Text Message (SMS)	Configure
<input checked="" type="checkbox"/> Email	Configure
<input checked="" type="checkbox"/> Bypass Code	Configure

Trusted Computer

Enable Trusted Computer

Number of days a computer can be trusted

Max number of trusted computers

Factors

Max number of enrolled factors

Login Rules

Max unsuccessful MFA attempts

**Save** **Cancel**

- Confirm new MFA settings.

Multi-Factor Authentication (MFA) Settings

Select the factors that you want to enable: ⓘ

<input checked="" type="checkbox"/> Security Questions	Configure
<input checked="" type="checkbox"/> Mobile App OTP	Configure
<input checked="" type="checkbox"/> Mobile App Notification	Configure
<input checked="" type="checkbox"/> Text Message (SMS)	Configure
<input checked="" type="checkbox"/> Email	Configure
<input checked="" type="checkbox"/> Bypass Code	Configure

Trusted Computer

Enable Trusted Computer

Number of days a computer can be b

Max number of trusted computers

Factors

Max number of enrolled factors

Login Rules

Max unsuccessful MFA attempts

**Save**

Confirmation

Are you sure that you want to update the settings?

**Yes** **No**

- Select **Security -> Sign-On Policies** from the sidebar to the left of admin console.

The screenshot shows the Oracle Identity Cloud Service interface. On the left, a dark sidebar lists various administrative options. The 'Sign-On Policies' item is highlighted with a red box and a red arrow pointing to it from the bottom-left.

The main content area is titled 'Multi-Factor Authentication (MFA) Settings'. It displays a list of factors to enable:

- Security Questions (Configure)
- Mobile App OTP (Configure)
- Mobile App Notification (Configure)
- Text Message (SMS) (Configure)
- Email (Configure)
- Bypass Code (Configure)

Below this, there are sections for 'Trusted Computer' and 'Factors'.

**Trusted Computer**:  
Enable Trusted Computer (checkbox checked)  
Number of days a computer can be trusted: 15  
Max number of trusted computers: 5

**Factors**:  
Max number of enrolled factors: 5

**Login Rules**:  
Max unsuccessful MFA attempts: 10

- Click on **Default Sign-On Policy**. This will open up the policy.

The screenshot shows the 'Sign-On Policies' list. The 'Default Sign-On Policy' row is selected and highlighted with a red box and a red arrow pointing to it from the bottom-left. Next to the policy name, there is a red arrow pointing to the text 'click here'.

- Go to the **Sign-On Rules** tab and then click on **Edit** against the **Default Sign-On Rule**.

The screenshot shows the Oracle Identity Cloud Service interface. On the left, a dark sidebar menu includes options like Dashboard, Users, Groups, Applications, Jobs, Reports, Settings, Security (with Administrators, Identity Providers, and IDP Policies), and Sign-On Policies. The Sign-On Policies option is selected, indicated by a blue border. The main content area is titled "Default Sign-On Policy" and shows the path "Sign-On Policies > Default Sign-On Policy". Below the title, there are three tabs: "Details", "Sign-On Rules", and "Assign Apps". A red arrow points from the left towards the "Sign-On Rules" tab, which is highlighted with a blue border. The "Details" tab is also outlined in blue. The "Sign-On Rules" section contains fields for "Policy Name" (set to "Default Sign-On Policy") and "Description" (set to "Default Sign on Policy for Tenant").

This screenshot shows the "Sign-On Rules" configuration page for the "Default Sign-On Policy". The "Sign-On Rules" tab is active and highlighted with a red border. The "Details" tab is also outlined in blue. The "Assign Apps" tab is visible but not active. The main area displays a table with one row, labeled "Default Sign-On Rule". To the right of the table is a green "Save" button. A red arrow points from the bottom right towards the "Edit" button, which is located at the far right of the table row. The sidebar on the left is identical to the one in the first screenshot.

- Check the box **Prompt for an additional factor**. Set the value of **Enrollment** to **Optional**. Click on **Save**.

The screenshot shows the Oracle Identity Cloud Service (IDCS) interface. The left sidebar has a dark theme with various navigation options like Dashboard, Users, Groups, Applications, Jobs, Reports, Settings, Security (Administrators, Identity Providers, IDP Policies), and Sign-On Policies. The 'Sign-On Policies' option is currently selected. The main content area is titled 'Default Sign-On Policy' and 'Edit Default Sign-On Rule'. It includes sections for 'Conditions' (user authentication, group membership, network perimeters) and 'Actions' (Access is Allowed, Prompt for reauthentication, Prompt for an additional factor, Enrollment is Optional). The 'Prompt for an additional factor' checkbox is checked and highlighted with a red box. A green arrow points to the 'Save' button at the bottom right.

The screenshot shows the Oracle Identity Cloud Service (IDCS) interface. The left sidebar has a dark theme with various navigation options like Dashboard, Users, Groups, Applications, Jobs, Reports, Settings, Security (Administrators, Identity Providers, IDP Policies), and Sign-On Policies. The 'Sign-On Policies' option is currently selected. The main content area is titled 'Default Sign-On Policy' and shows the 'Sign-On Rules' tab. It displays a table with one row: 'Default Sign-On Rule'. A success message at the top says 'The Default Sign-On Rule sign-on rule has been updated.' A green arrow points to the 'Save' button at the bottom right.

- Congratulations, you enabled and configured multi-factor authentication within IDCS.

## Activate account – (Persona: End-User)

For end-user flow, use either a separate browser or an incognito/ private browser session. This will ensure that administrator and user sessions are not mixed up.

- Login to gmail as [demoidcs@gmail.com](mailto:demoidcs@gmail.com). Go to the gmail label corresponding to your user. Verify that there is an activation email from IDCS.

Gmail password will be provided during session.

"User1" (1) - demoidcs@gmail.com - Gmail

Gmail ▾

**COMPOSE**

no-reply@oracle.com

Welcome to waymon, Danny Crane - Hello Danny Crane, Your waymon account is ready. To get started, activate your account. Activate Your Account

Jan 22

Inbox  
Starred  
Sent Mail  
Drafts  
**User1 (1)**  
User2 (1)  
User3 (1)  
User4 (1)  
More ▾

0 GB (0%) of 15 GB used  
Manage

Terms - Privacy

Last account activity: 16 hours ago  
Details

- Open and review the email. Click on the **Activate Your Account** button.

Google

label:user1

Gmail ▾

**COMPOSE**

Welcome to waymon, Danny Crane User1 x

no-reply@oracle.com <no-reply@oracle.com> to me 5:56 PM (16 hours ago)

Activate Your Account click here

Details

If the [activate your account](#) link doesn't work, please copy and paste the following URL into the address bar of your browser:  
<https://idcs-2B8Q1tDVJzkbSyph%2BioY0l7sRArPEAIAPHhQ%3D>

**Important:** This link will expire on Tuesday, January 23, 2018 5:56:13 PM CST.

If you don't recognize this message, contact your system administrator at [REDACTED] @gmail.com.

- IDCS change password page will open up. Provide a suitable password that passes the listed **Password Criteria**. The criterion/rule verification is indicated with a green check mark against each of the rule. Click on **Submit**.

Welcome to waymon, Danny Crane - demoidcs@gmail.com - Gmail

Identity Cloud Service | Change Password

Set a new password for your user account

\* User Name dcrane

\* New Password [REDACTED]

\* Confirm New Password [REDACTED]

**Submit**

**Password Criteria:**

- ✓ The password must have at least 8 characters.
- ✓ The password cannot exceed 40 characters.
- ✓ The password cannot contain the First Name of the user.
- ✓ The password cannot contain the Last Name of the user.
- ✓ The password cannot contain the user name.
- ✓ The password must have at least 1 lowercase characters.
- ✓ The password must have at least 1 uppercase characters.
- ✓ The password must have at least 1 numeric characters.
- ✓ Cannot repeat the Current Password
- ✓ The password cannot contain the whitespaces.

- Verify that you are redirected to the MFA enrollment page.

Secure | https://idcs-identity.oraclecloud.com/ui/v1/signin

**ORACLE** Enable 2-Step Verification

dcrane

2-Step Verification adds an additional layer of security to your account by using a second device or security questions to verify your identity. Once set up, other users cannot access your account even if they guess your password.

Diagram: Password + Proof = Secure Access

The process guides you through the steps to enable 2-Step Verification for your account.

What is 2-Step Verification? **Enable >** Skip

## Enroll in multi-factor authentication – (Persona: End-User)

- On the **Enable 2-Step Verification** page, click on **Enable**.

Secure | https://idcs-identity.oraclecloud.com/ui/v1/signin

**ORACLE** Enable 2-Step Verification

dcrane

2-Step Verification adds an additional layer of security to your account by using a second device or security questions to verify your identity. Once set up, other users cannot access your account even if they guess your password.

Diagram: Password + Proof = Secure Access

The process guides you through the steps to enable 2-Step Verification for your account.

What is 2-Step Verification? **Enable >** Skip

- Select the method **Email**.

# ORACLE® Enable 2-Step Verification

dcrane

## 1 Select a Method

What are the differences?

Mobile App

Mobile Number

Security Questions

Email

## 2 Enter the One-Time Passcode

An email that contains a passcode has been sent to [demoidcs+user1@gmail.com](mailto:demoidcs+user1@gmail.com).

Passcode

Verify

- Access your email to obtain the one-time passcode .

The screenshot shows a Gmail inbox with the search bar set to "label:user1". A message from "no-reply@oracle.com" is selected, with the subject "Your waymon One-Time Passcode". The message body contains:

ORACLE®

Hello Danny Crane,

878685 is the one-time passcode for your waymon account dcrXXX. This passcode is valid for 10 minutes.

**Details**

Use this one-time passcode to complete 2-Step Verification.  
If you don't recognize this message, contact your system administrator at [waymonw@gmail.com](mailto:waymonw@gmail.com).

- Provide the 6-digit code on the enrollment page and click on **Verify**.

# ORACLE® Enable 2-Step Verification

dcrane

## 1 Select a Method

What are the differences?

Mobile App

Mobile Number

Security Questions

Email

## 2 Enter the One-Time Passcode

An email that contains a passcode has been sent to **demoidcs+user1@gmail.com**.

Passcode

878685

Verify

click here

Didn't get the email? [Resend Email](#)

- Ensure that the success enrollment message is displayed. Click on **Done**.

# ORACLE® Enable 2-Step Verification

dcrane

## Successfully Enrolled

Your email address, **demoidcs+user1@gmail.com**, has been set as your 2-Step Verification method.



Done

It is recommended that you set up an additional method. This ensures that you have a backup.

Mobile App

Install the Mobile Authenticator App on your device, and then use the passcode that is generated by the App or approve requests through push notifications.

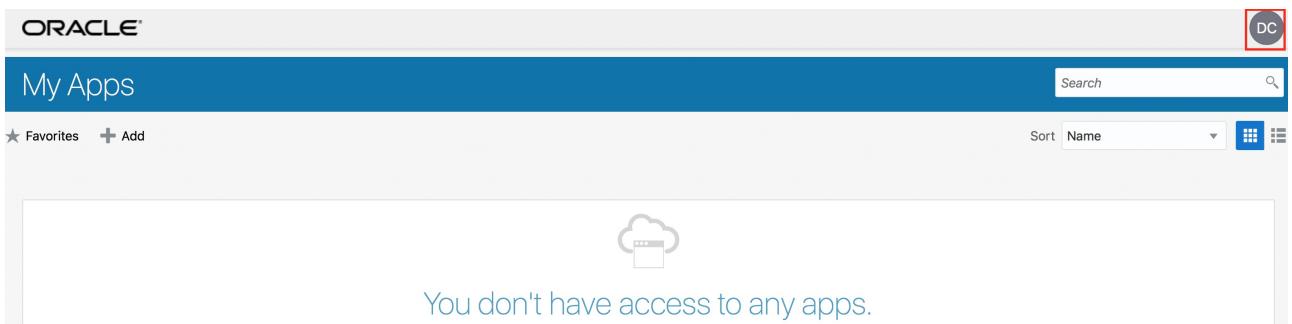
Mobile Number

Receive an SMS, which contains a passcode. Use the passcode to verify your device.

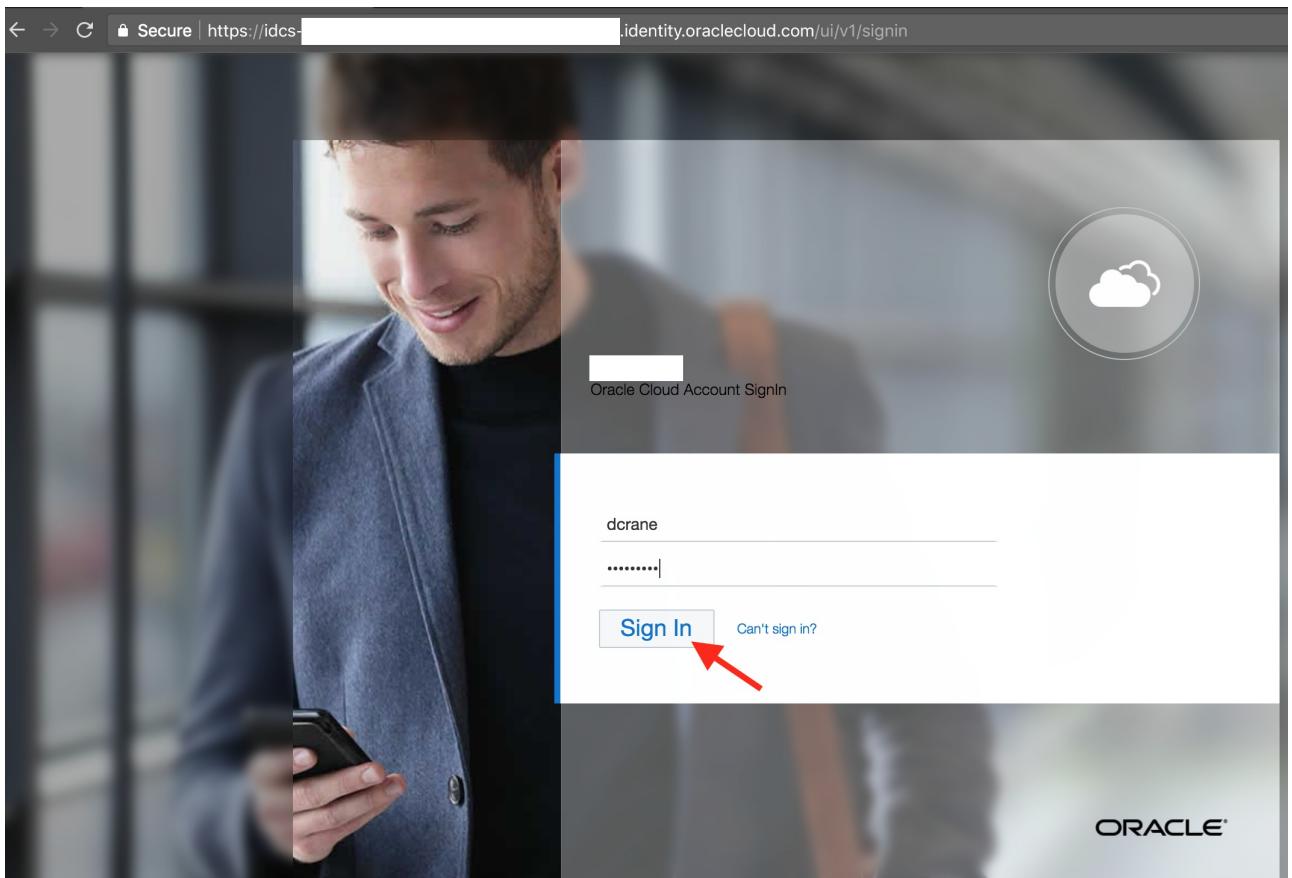
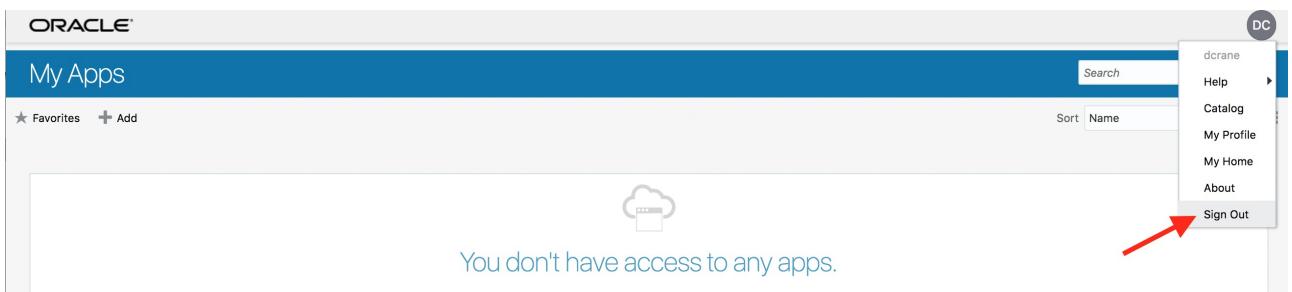
Security Questions

Provide answers to pre-registered questions to verify your identity.

- Verify that you are redirected to the empty **My Apps** page.



- Sign out from IDCS and re-login with your credentials.



- Ensure that you are challenged by 2-Factor authentication and have received a new email containing a new 6-digit one time code.

## ORACLE® 2-Step Verification

dcrane

 An email that contains a passcode has been sent to **demoidcs+user1@gmail.com**.

Passcode

Verify

Trust this computer for 15 day(s)

Unable to receive an email? [Use backup verification method](#)



no-reply@oracle.com <no-reply@oracle.com>

to me ▾

9:56 AM (

**ORACLE®**

Hello Danny Crane,

250223 is the one-time passcode for your whitingw account dcrXXX. This passcode is valid for 10 minutes.

**Details**

Use this one-time passcode to complete 2-Step Verification.

If you don't recognize this message, contact your system administrator at [REDACTED]

- Provide the new 6-digit code on the challenge screen for verification.

## ORACLE® 2-Step Verification

dcrane

 An email that contains a passcode has been sent to **demoidcs+user1@gmail.com**.

Passcode

Verify

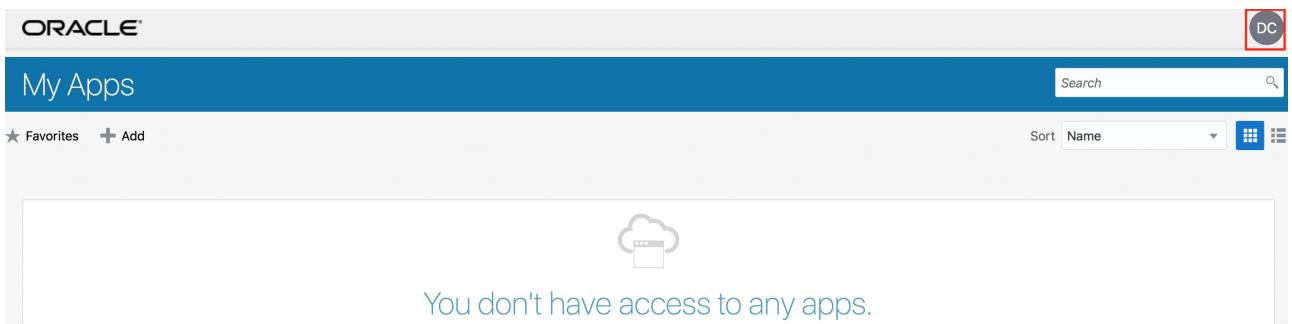
Didn't get the email? [Resend Email](#)



Trust this computer for 15 day(s)

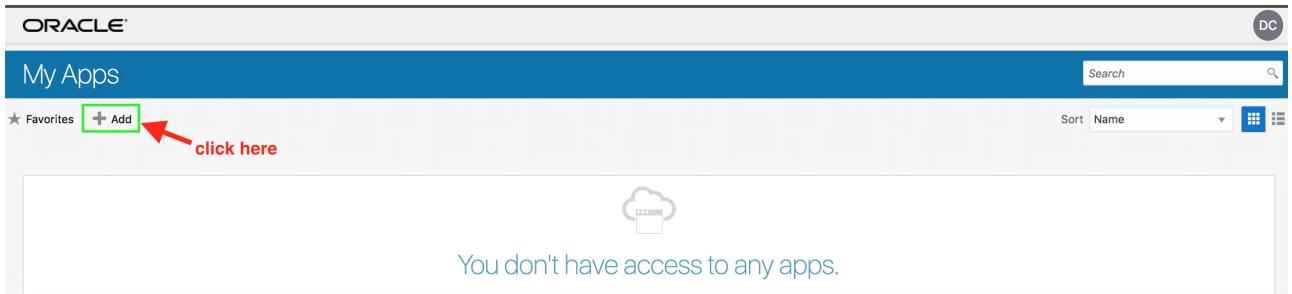
Unable to receive an email? [Use backup verification method](#)

- On successful verification, ensure that you are logged in to the **My Apps** page.



## Request group – (Persona: End-User)

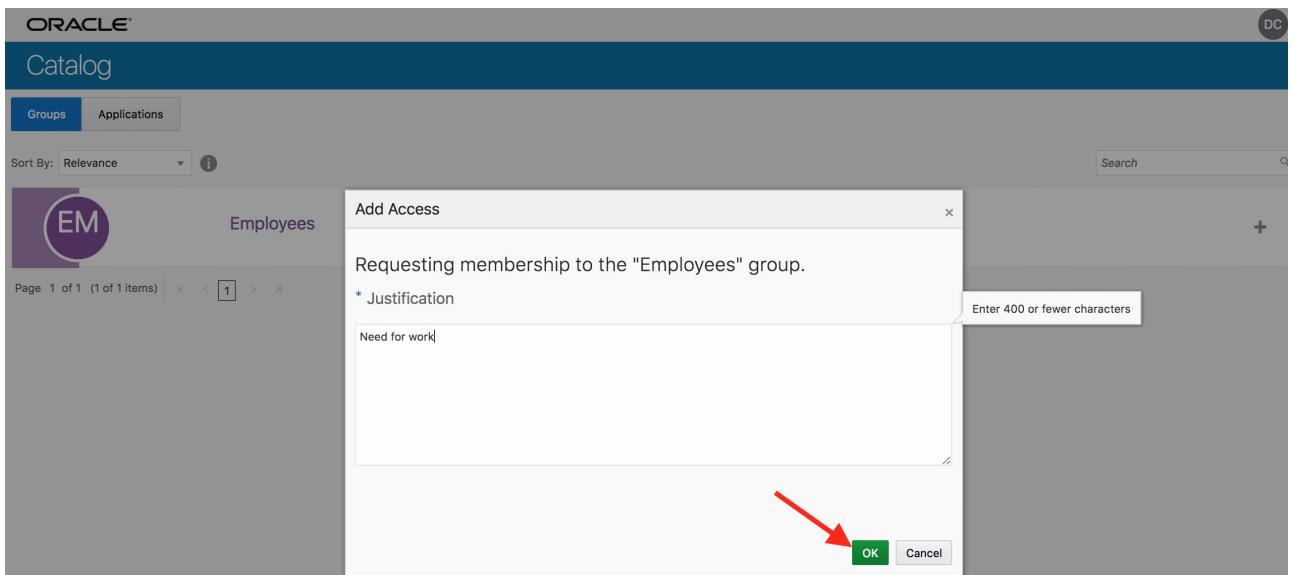
- From MyApps page click on **Add** access request button.



- Verify that **Employees** group is available on the **Groups** tab. Click on + sign to request access to the group.



- Provide justification on the resulting popup page. Click on **OK**.



- Go to **My Profile** section from menu located top-right.

The screenshot shows the Oracle Catalog interface. At the top right, there is a user profile menu with options: dcrane, Help, My Apps, My Profile (highlighted with a green box and a red arrow pointing to it), My Home, About, and Sign Out. Below the menu, the user's name 'dcrane' and email 'demoldcs+user1@gmail.com' are displayed.

- Ensure that Employee group is visible under My Access tab.

The screenshot shows the Oracle Catalog interface with the 'My Access' tab selected (highlighted with a red box). Under the 'Groups' tab, the 'Employee' group is visible. The user's name 'Danny Crane' and title 'Mr' are displayed at the top. The navigation bar includes links for My Profile Details, Change My Password, Set Email Options, Social Accounts, 2-Step Verification, My Access (selected), and My Requests.

- Go to My Apps section from menu located top-right.

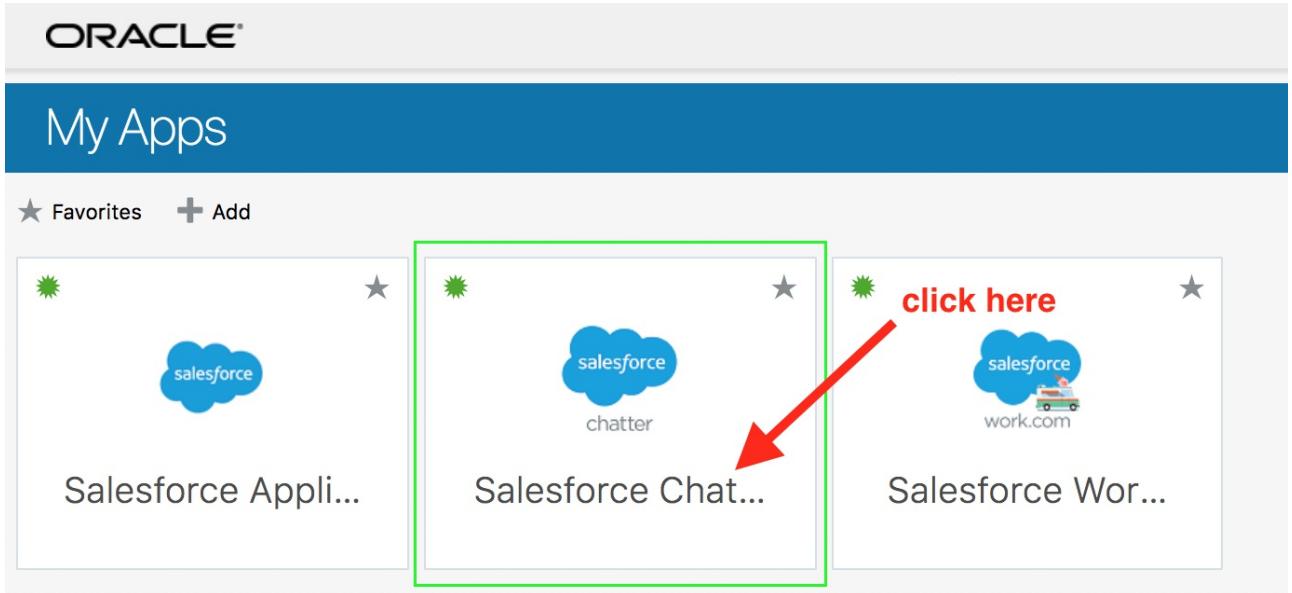
The screenshot shows the Oracle Catalog interface with the 'My Apps' section selected (highlighted with a green box and a red arrow pointing to it). The user's name 'Danny Crane' and title 'Mr' are displayed at the top. The navigation bar includes links for My Profile Details, Change My Password, Set Email Options, Social Accounts, 2-Step Verification, My Access, and My Requests. The 'My Apps' section displays three Salesforce applications: 'Salesforce Application', 'Salesforce Chatter', and 'Salesforce Work.com'. The 'Salesforce Application' card is highlighted with a red box.

- Ensure that Salesforce applications are visible now on the My Apps page.

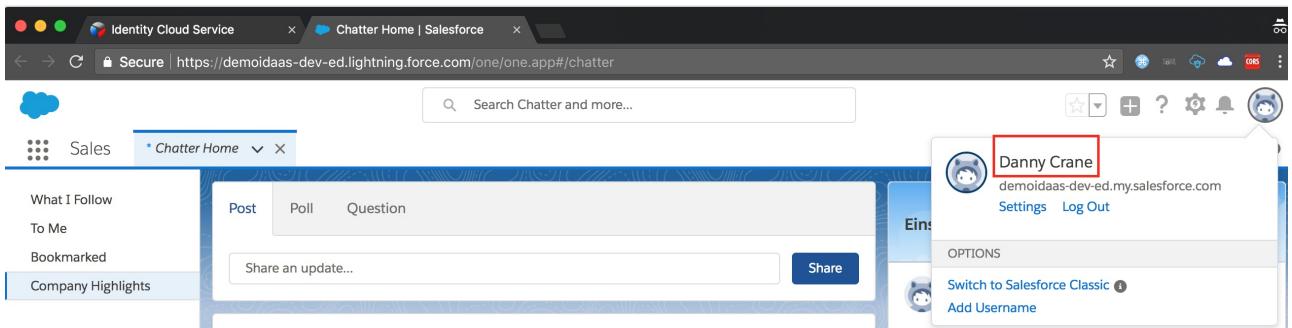
The screenshot shows the Oracle Catalog interface with the 'My Apps' page selected. The user's name 'Danny Crane' and title 'Mr' are displayed at the top. The navigation bar includes links for My Profile Details, Change My Password, Set Email Options, Social Accounts, 2-Step Verification, My Access, and My Requests. The 'My Apps' page displays three Salesforce applications: 'Salesforce Application', 'Salesforce Chatter', and 'Salesforce Work.com'. The 'Salesforce Application' card is highlighted with a red box.

## Verify SSO – (Persona: End-User)

- Click on the **Salesforce Chatter** app.



- Ensure that user is automatically logged-in to Salesforce Chatter (SSO)



- Congratulations, you completed the IDCS Hands-on lab.