

# DUMPS ARENA

## Salesforce Certified Identity and Access Management Designer

Salesforce Identity-and-Access-Management-Designer

Version Demo

Total Demo Questions: 10

Total Premium Questions: 128

Buy Premium PDF

<https://dumpsarena.co>

[sales@dumpsarena.co](mailto:sales@dumpsarena.co)

sales@dumpsarena.co  
dumpsarena.co

**QUESTION NO: 1**

Universal Containers (UC) wants to build a custom mobile app for their field reps to create orders in salesforce. After the first time the users log in, they must be able to access salesforce upon opening the mobile app without being prompted to log in again. What Oauth flows should be considered to support this requirement?

- A. Web Server flow with a Refresh Token.
- B. Mobile Agent flow with a Bearer Token.
- C. User Agent flow with a Refresh Token.
- D. SAML Assertion flow with a Bearer Token.

**ANSWER: C****QUESTION NO: 2**

Universal containers (UC) would like to enable SSO between their existing Active Directory infrastructure and salesforce. The it team prefers to manage all users in Active Directory and would like to avoid doing any initial setup of users in salesforce directly, including the correct assignment of profiles, roles and groups.

Which two optimal solutions should UC use to provision users in salesforce? Choose 2 answers

- A. Use the salesforce REST API to sync users from active directory to salesforce
- B. Use an app exchange product to sync users from Active Directory to salesforce.
- C. Use Active Directory Federation Services to sync users from active directory to salesforce.
- D. Use Identity connect to sync users from Active Directory to salesforce

**ANSWER: B D****QUESTION NO: 3**

Universal containers (UC) has a custom, internal-only, mobile billing application for users who are commonly out of the office. The app is configured as a connected App in salesforce. Due to the nature of this app, UC would like to take the appropriate measures to properly secure access to the app. Which two are recommendations to make the UC? Choose 2 answers

- A. Disallow the use of single Sign-on for any users of the mobile app.
- B. Require high assurance sessions in order to use the connected App

- C. Use Google Authenticator as an additional part of the logical processes.
- D. Set login IP ranges to the internal network for all of the app users profiles.

**ANSWER: B C**

#### **QUESTION NO: 4**

Universal Containers (UC) has decided to use Salesforce as an Identity Provider for multiple external applications. UC wants to use the salesforce App Launcher to control the Apps that are available to individual users. Which three steps are required to make this happen?

- A. Add each connected App to the App Launcher with a Start URL.
- B. Set up an Auth Provider for each External Application.
- C. Set up Salesforce as a SAML Idp with My Domain.
- D. Set up Identity Connect to Synchronize user data.
- E. Create a Connected App for each external application.

**ANSWER: A C E**

#### **QUESTION NO: 5**

Universal Containers (UC) would like its community users to be able to register and log in with LinkedIn or Facebook Credentials. UC wants users to clearly see Facebook & LinkedIn Icons when they register and login. What are the two recommended actions UC can take to achieve this Functionality? Choose 2 answers

- A. Enable Facebook and LinkedIn as Login options in the login section of the Community configuration.
- B. Create custom Registration Handlers to link LinkedIn and facebook accounts to user records.
- C. Store the LinkedIn or Facebook user IDs in the Federation ID field on the Salesforce User record.
- D. Create custom buttons for Facebook and LinkedIn using JAVAscript/CSS on a custom Visualforce page.

**ANSWER: A B**

#### **QUESTION NO: 6**

Universal Containers (UC) employees have Salesforce access from restricted IP ranges only, to protect against

unauthorised access. UC wants to roll out the Salesforce1 mobile app and make it accessible from any location. Which two options should an Architect recommend? Choose 2 answers

- A. Relax the IP restriction with a second factor in the Connect App settings for Salesforce1 mobile app.
- B. Remove existing restrictions on IP ranges for all types of user access.
- C. Relax the IP restrictions in the Connect App settings for the Salesforce1 mobile app.
- D. Use Login Flow to bypass IP range restriction for the mobile app.

**ANSWER: A C**

#### QUESTION NO: 7

Universal Containers (UC) is planning to deploy a custom mobile app that will allow users to get e-signatures from its customers on their mobile devices. The mobile app connects to Salesforce to upload the e-signature as a file attachment and uses OAuth protocol for both authentication and authorization. What is the most recommended and secure OAuth scope setting that an Architect should recommend?

- A. Id
- B. Web
- C. Api
- D. Custom\_permissions

**ANSWER: D**

#### QUESTION NO: 8

Universal containers (UC) has a classified information system that it's call centre team uses only when they are working on a case with a record type of "classified". They are only allowed to access the system when they own an open "classified" case, and their access to the system is removed at all other times. They would like to implement SAML SSO with salesforce as the IDP, and automatically allow or deny the staff's access to the classified information system based on whether they currently own an open "classified" case record when they try to access the system using SSO. What is the recommended solution for automatically allowing or denying access to the classified information system based on the open "classified" case record criteria?

- A. Use a custom connected App handler using apex to dynamically allow access to the system based on whether the staff owns any open "classified" cases.
- B. Use apex trigger on case to dynamically assign permission sets that grant access when a user is assigned with an open "classified" case, and remove it when the case is closed.
- C. Use custom SAML jit provisioning to dynamically query the user's open "classified" cases when attempting to access the classified information system

D. Use salesforce reports to identify users that currently owns open "classified" cases and should be granted access to the classified information system.

**ANSWER: A**

**QUESTION NO: 9**

Universal Containers (UC) has built a custom token-based Two-factor authentication (2FA) system for their existing on-premise applications. They are now implementing Salesforce and would like to enable a

Two-factor login process for it, as well. What is the recommended solution as Architect should consider?

- A. Use the custom 2FA system for on-premise applications and native 2FA for Salesforce.
- B. Replace the custom 2FA system with an AppExchange App that supports on premise application and salesforce.
- C. Use Custom Login Flows to connect to the existing custom 2FA system for use in Salesforce.
- D. Replace the custom 2FA system with Salesforce 2FA for on-premise applications and Salesforce.

**ANSWER: D**

**QUESTION NO: 10**

Universal Containers (UC) is building a customer community and will allow customers to authenticate using Facebook credentials. The First time the user authenticating using facebook, UC would like a customer account created automatically in their Accounting system. The accounting system has a web service accessible

to Salesforce for the creation of accounts. How can the Architect meet these requirements?

- A. Create a custom application on Heroku that manages the sign-on process from Facebook.
- B. Use JIT Provisioning to automatically create the account in the accounting system.
- C. Add an Apex callout in the registration handler of the authorization provider.
- D. Use OAuth JWT flow to pass the data from Salesforce to the Accounting System.

**ANSWER: C**