



IDENTITY-AND-ACCESS- MANAGEMENT-ARCHITECT^{Q&As}

Salesforce Certified Identity and Access Management Architect

**Pass Salesforce IDENTITY-AND-ACCESS-
MANAGEMENT-ARCHITECT Exam with 100%
Guarantee**

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.passapply.com/identity-and-access-management-architect.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Salesforce
Official Exam Center



VCE & PDF

PassApply.com

<https://www.passapply.com/identity-and-access-management-architect.html>

2024 Latest passapply IDENTITY-AND-ACCESS-MANAGEMENT-ARCHITECT

PDF and VCE dumps Download

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





QUESTION 1

Universal containers (UC) has a mobile application that it wants to deploy to all of its salesforce users, including customer Community users. UC would like to minimize the administration overhead, which two items should an architect recommend? Choose 2 answers

- A. Enable the "Refresh Tokens is valid until revoked" setting in the Connected App.
- B. Enable the "Enforce Ip restrictions" settings in the connected App.
- C. Enable the "All users may self-authorize" setting in the Connected App.
- D. Enable the "High Assurance session required" setting in the Connected App.

Correct Answer: AC

QUESTION 2

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.

Correct Answer: A

QUESTION 3

A global fitness equipment manufacturer is planning to sell fitness tracking devices and has the following requirements:

- 1) Customer purchases the device.
- 2) Customer registers the device using their mobile app.
- 3) A case should automatically be created in Salesforce and associated with the customers account in cases where the device registers issues with tracking.



Which OAuth flow should be used to meet these requirements?

- A. OAuth 2.0 Asset Token Flow
- B. OAuth 2.0 Username-Password Flow
- C. OAuth 2.0 User-Agent Flow
- D. OAuth 2.0 SAML Bearer Assertion Flow

Correct Answer: A

QUESTION 4

Northern Trail Outfitters (NTO) has an off-boarding process where a terminated employee is first disabled in the Lightweight Directory Act Protocol (LDAP) directory, then requests are sent to the various application support teams to finish user deactivations. A terminated employee recently was able to login to NTO's Salesforce instance 24 hours after termination, even though the user was disabled in the corporate LDAP directory.

What should an identity architect recommend to prevent this from happening in the future?

- A. Create a Just-in-Time provisioning registration handler to ensure users are deactivated in Salesforce as they are disabled in LDAP.
- B. Configure an authentication provider to delegate authentication to the LDAP directory.
- C. use a login flow to make a callout to the LDAP directory before authenticating the user to Salesforce.
- D. Setup an identity provider (IdP) to authenticate users using LDAP, set up single sign-on to Salesforce and disable Login Form authentication.

Correct Answer: B

QUESTION 5

Northern Trail Outfitters (NTO) has an existing custom business-to-consumer (B2C) website that does NOT support single sign-on standards, such as Security Assertion Markup Language (SAML) or OAuth. NTO wants to use Salesforce

Identity to register and authenticate new customers on the website.

Which two Salesforce features should an identity architect use in order to provide username/password authentication for the website?

Choose 2 answers

- A. Identity Connect
- B. Delegated Authentication
- C. Connected Apps
- D. Embedded Login



Correct Answer: BD

[Latest IDENTITY-AND-ACCESS-MANAGEMENT-ARCHITECT Dumps](#)

[IDENTITY-AND-ACCESS-MANAGEMENT-ARCHITECT PDF Dumps](#)

[IDENTITY-AND-ACCESS-MANAGEMENT-ARCHITECT VCE Dumps](#)