PassQueen
a.k.a dumpsqueen.com

Okta Certified Professional Exam

Okta Okta-Certified-Professional

Version Demo

Total Demo Questions: 11

Total Premium Questions: 118

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, User and Group Management	25
Topic 2, Application Management	23
Topic 3, Directory Integration	14
Topic 4, Authentication and Security	42
Topic 5, Mix Questions	14
Total	118

QUESTION NO: 1

Is this an expected behavior when an incremental import is performed from Active Directory?

Solution: Only the groups are imported

A. Yes

B. No

ANSWER: B

Explanation:

No is correct. An incremental Active Directory import is intended to identify and import directory changes that have occurred since the prior import, rather than limiting the import to group objects alone. Okta uses the Active Directory agent and Active Directory change-tracking information to detect relevant changes efficiently. As a result, the scope of an incremental import can include changed user records as well as changed group records and associated membership information when applicable. The precise objects processed depend on what has changed in the directory and on the import configuration, but "only the groups are imported" is not the expected general behavior of an incremental import.

Okta's Active Directory integration documentation distinguishes full imports from incremental imports: a full import reads all relevant users and groups, while an incremental import processes changes since the last successful import. This incremental mechanism reduces processing while keeping Okta synchronized with Active Directory updates. Therefore, seeing an import that is restricted solely to groups should not be treated as the normal expected outcome of choosing an incremental import; it warrants checking whether user objects actually changed, whether the import scope or filters exclude users, and whether the prior import completed successfully. See Okta's Import users from Active Directory and Active Directory integration documentation.

QUESTION NO: 2

Is this an Okta setting an end user can change?

Solution: Color

A. Yes

B. No

ANSWER: B

Explanation:

No is correct. Color is an organization-level branding and theme setting, rather than a preference that an individual end user controls from their Okta dashboard. Okta administrators configure the visual appearance presented to users, including brand elements and color choices, through the Admin Console's branding and customization capabilities. This ensures that the organization can maintain a consistent identity and user experience across its Okta sign-in and dashboard-related experiences. End users may manage the personal information, authentication factors, and application-dashboard preferences that their organization permits, but they do not have authority to alter the organization's configured color branding. The exact branding controls available can vary by Okta engine and enabled features, but their administration remains an administrative responsibility. Okta documents branding as a configuration performed in the Admin Console, where administrators can customize the look and feel of the sign-in experience and manage themes. See Okta's Branding documentation and its Settings documentation for administrator-managed configuration guidance.

QUESTION NO: 3

An Okta Administrator configured the factor enrollment policy to require Okta Verify as a factor and Google Authenticator and Voice Call Authentication as optional factors

Is this what happens when an end user authenticates with Okta?

Solution: The end user must enroll in all three factors and use all three factors when authenticating.

A. Yes

B. No

ANSWER: B

Explanation:

No is correct. A factor enrollment policy controls which authenticators a user must enroll in and which additional authenticators the user may choose to enroll in. With Okta Verify configured as required, the user must enroll in Okta Verify when the policy applies. Google Authenticator and Voice Call Authentication, when configured as optional, are available for enrollment but do not create an obligation for the user to enroll in them. Therefore, the user is not required to enroll in all three authenticators.

Enrollment requirements are distinct from authentication requirements. The policy that protects an application or Okta resource determines whether, and under what conditions, the user must provide an additional authenticator during sign-in. A user who has enrolled only in the required authenticator can satisfy an authentication challenge using that enrolled method when it meets the applicable assurance requirements. Okta does not require a user to present every authenticator they have enrolled during a single authentication transaction; the applicable authentication policy prompts for the required assurance level. Okta documents this separation between authenticator enrollment policy rules and authentication policy rules in its authenticator policy documentation and policy overview.

QUESTION NO: 4

Is this a protocol that uses ID tokens?

Solution: SAML

A. Yes

B. No

ANSWER: B

Explanation:

“No” is correct because SAML does not use OpenID Connect ID tokens. In a SAML single sign-on flow, the identity provider communicates authentication and user-attribute information to the service provider in a SAML assertion. The assertion is an XML-based security token and commonly contains an authentication statement, attribute statements, and conditions that specify details such as the intended audience and validity period. The service provider validates that SAML assertion to establish the user’s session.

An ID token is specifically an OpenID Connect artifact. It represents the result of authentication and contains claims about the authenticated end user; it is typically encoded as a JSON Web Token (JWT). Okta’s OpenID Connect documentation describes ID tokens as tokens returned by the authorization server that include identity claims, while its SAML documentation describes SAML integrations as relying on assertions exchanged between the identity provider and service provider. Although both protocols can convey identity information for federation and SSO, their token formats and protocol terminology are distinct. Therefore, SAML should be identified as using SAML assertions, not ID tokens.

References: Okta: Validate ID tokens; Okta: SAML concepts.

QUESTION NO: 5

Is this an advantage of deploying the Okta LDAP Agent to integrate Okta with an LDAP directory service?

Solution: End users are stored locally in LDAP but are NOT imported to Okta.

A. Yes

B. No

ANSWER: B

Explanation:

No is correct. Deploying the Okta LDAP Agent does allow an organization to retain its LDAP directory as the source of truth for user identities and credentials, but the agent's LDAP import capability brings selected LDAP users and groups into the Okta Universal Directory. Okta creates corresponding user records in Okta so that those users can be assigned applications, governed by Okta policies, included in groups, and authenticated through Okta-managed integrations.

The import does not require moving or deleting the original LDAP entries. The users remain stored in the on-premises LDAP directory, and the LDAP Agent can support delegated authentication, allowing password validation to continue against LDAP when configured. However, retaining users exclusively in LDAP with no corresponding imported Okta user records is not the standard LDAP Agent integration model and would prevent Okta from managing those identities for access to assigned cloud applications. Imports may be scoped and scheduled, but the core integration synchronizes imported directory identities into Okta. See Okta's directory integration documentation and LDAP Agent documentation.

QUESTION NO: 6

Is this what an end user needs to do in order to switch between Okta accounts from within the same browser? Solution: Set up Okta as a trusted site.

A. Yes

B. No

ANSWER: B

Explanation:

No is correct. Switching between Okta accounts in one browser is an Okta end-user account/session function, not a browser trusted-sites configuration task. An end user switches accounts from the Okta End-User Dashboard account menu, where available, by selecting another remembered account or adding/signing in to a different account. Okta manages the resulting authenticated browser sessions through its session and cookie mechanisms. The precise account-switching experience can vary by Okta Identity Engine configuration, browser behavior, and an organization's sign-on policies, but browser trusted-site lists do not provide the account-switching capability. Administrators should ensure that users can access the Okta dashboard and follow the organization's intended sign-in and account-selection flow. They should also consider their session policies and browser cookie requirements when troubleshooting sign-in behavior. Okta's End-User Dashboard documentation describes the dashboard experience and user menu functionality, while Okta's session-cookie guide explains how browser sessions are established and maintained. See Okta End-User Dashboard documentation and Okta session cookie guide.

QUESTION NO: 7

Can an Okta Administrator enable multifactor authentication (MFA) at this level?

Solution: Application

A. Yes

B. No

ANSWER: A

Explanation:

Yes is correct. An Okta Administrator can require multifactor authentication for access to an individual application by configuring that application's sign-on policy. In Okta Identity Engine, an application can use an authentication policy and app sign-in policy rules that require users to satisfy an additional factor before access is granted. This allows administrators to

apply stronger authentication requirements to sensitive applications without necessarily applying the same requirement to every application in the tenant.

For example, a rule can evaluate the user, group membership, network context, device context, or other configured conditions, then require multifactor authentication when the user attempts to launch the application. The user must have an appropriate authenticator enrolled and complete the required challenge to meet the policy requirement. Application-level requirements are therefore an important part of implementing risk-appropriate access controls: an organization may permit lower-friction access to less sensitive resources while requiring MFA for applications containing confidential data or administrative capabilities.

Okta documents application access requirements through app sign-in policies and their rules, including rules that require multifactor authentication. See Okta app sign-in policies and Okta authentication policies.

QUESTION NO: 8

Is this intimation available from the Okta Trust web page?

Solution: OKta service level agreement (SLA)

A. Yes

B. No

ANSWER: B

Explanation:

No is correct. Okta's Trust site is intended to provide transparency into the operational status, availability history, security posture, compliance resources, and incident-related communications for Okta services. It is a useful destination for customers who need current service-health information or trust and assurance materials.

An Okta Service Level Agreement, however, is a contractual document that defines Okta's service-availability commitment, how availability is measured, applicable exclusions, and the process for requesting service credits when the agreement's conditions are met. Okta publishes this material through its legal agreements resources rather than treating it as status or operational information on the Trust site. A customer evaluating contractual commitments should therefore consult the official Okta agreements page and the agreement incorporated into their applicable order or subscription documentation.

For the authoritative SLA terms, see Okta Agreements. For service-status and trust-related operational information, see the Okta Trust Center.

QUESTION NO: 9

Is this one of the default base attributes in the Okta user profile that can be marked as required or optional for Okta mastered users?

Solution: firstName

A. Yes

B. No

ANSWER: A

Explanation:

Yes is correct. `firstName` is the First Name base attribute in the Okta user profile. Okta supplies a standard set of base attributes for every user profile, and these attributes generally have fixed definitions. First Name and Last Name are important exceptions because Okta allows an administrator to configure whether each is required or optional for users mastered by Okta. This setting is useful when an organization's identity and account-creation processes do not always have a legal or preferred given name available at the time a user record is created. The requiredness setting affects validation of

the user profile for the applicable mastering scenario, while the attribute remains part of the standard Okta user profile schema. Okta's documentation specifically identifies First Name and Last Name as attributes whose required status can be changed for Okta- and Active Directory-mastered users. Therefore, the proposed attribute name `firstName`, which is the API/profile variable for First Name, satisfies the condition in the question. See Okta's First and last name attributes documentation and its User profile API reference for the standard profile attribute naming.

QUESTION NO: 10

Is this an example of an Okta P1 level support ticket Issue?

Solution: An individual end user CANNOT access a business application

A. Yes

B. No

ANSWER: B

Explanation:

No is correct. Okta's highest-priority support classification is reserved for a service failure or severe service degradation that creates a critical, broad business impact. The defining condition is not merely that a person cannot sign in to or launch an application; it is the scope and severity of the resulting business disruption. For example, a highest-priority incident can apply when the customer cannot access business resources generally, or when users cannot access an application that is critical to business operations.

The stated situation identifies a single individual who cannot access a business application, without establishing that the application is business-critical or that the issue prevents a broader user population from working. That information does not meet the documented threshold for the highest-priority classification. Support severity should be selected according to the operational impact, affected population, and urgency, then updated if evidence shows that the impact is more extensive than initially understood. Okta documents its severity and priority definitions, including the criteria for a highest-priority ticket, in its Customer Support Ticket Severity and Priority Definition. For escalation and support-case handling context, see the Okta Customer Support Help Center.

QUESTION NO: 11

An Okta Administrator ran a full import from Active Directory An expected group was NOT imported into OKta. Is this a reason why the group was NOT imported into Okta?

Solution: The organizational unit (OU) containing the group was NOT selected for Import

A. Yes

B. No

ANSWER: A

Explanation:

Yes is correct. In the Okta Active Directory integration, the organizational units selected in the integration configuration define the directory scope that Okta searches during an import. A full import retrieves users and groups only from the selected organizational units and, where applicable, their included child organizational units. Therefore, if the organizational unit that contains the expected Active Directory group was not selected for import, that group is outside Okta's configured import scope and will not be brought into Okta during the full import.

An administrator should review the Active Directory integration settings in the Okta Admin Console, locate the organizational-unit selection for the import configuration, and ensure that the organizational unit containing the group is included. After updating the scope, running another import allows Okta to discover the group, subject to the normal import settings and connectivity of the Active Directory agent. Okta's documentation describes selecting the organizational units from which Okta

imports directory objects, including groups. See Okta Active Directory agent documentation and Okta Active Directory integration documentation.