PassQueen
a.k.a dumpsqueen.com

Okta Certified Administrator Exam

Okta Okta-Certified-Administrator

Version Demo

Total Demo Questions: 15

Total Premium Questions: 157

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, User and Group Management	21
Topic 2, Authentication and Authorization	38
Topic 3, Application Management	38
Topic 4, Directory Integration	41
Topic 5, Security and Compliance	11
Topic 6, Troubleshooting	5
Topic 7, Mix Questions	3
Total	157

QUESTION NO: 1

Which of the following is / are Okta required attributes?

Solution: None of the above

A. Yes

B. No

C. None of the above

ANSWER: C

Explanation:

None of the above is correct because the supplied responses, “Yes” and “No,” do not identify any Okta user-profile attributes. They are answers to a yes/no question rather than attribute names, so neither can validly answer a question asking which attributes are required. Okta’s default user profile does include standard attributes that are required when creating a user, including `firstName`, `lastName`, `login`, and `email`. The login value is the user’s unique sign-in identifier, while the other values support the core Okta user profile. Because none of those attributes, or any actual attribute name, appears among the original choices, “None of the above” is the only accurate selection for this item. Administrators can extend the Okta user profile with custom attributes and can manage profile mappings, but those additions do not make “Yes” or “No” into required-attribute answers. See Okta’s Create User API documentation for the required default-profile properties and the Okta profile documentation for profile concepts.

QUESTION NO: 2

On a Windows machine, which is the right behavior if you try to sign into your Okta org and agentless DSSO is properly configured for it?

Solution: You will be automatically redirected to The Okta Sign In page for your organization, where you need to fill in with your AD credentials

A. Yes

B. No

ANSWER: B

Explanation:

No is correct. With agentless Desktop Single Sign-on (DSSO) properly configured, a user on a managed Windows device should be authenticated transparently using Integrated Windows Authentication (IWA), rather than being sent to an Okta sign-in page to manually enter Active Directory credentials. When the user accesses the Okta org, the browser can negotiate authentication with the configured IWA Web agent endpoint using the user’s existing Windows session. Okta then receives the authentication result and establishes the Okta session, providing a seamless sign-in experience. This behavior depends on the device, browser, network, and IWA configuration meeting the applicable requirements, including access to the IWA Web agent and appropriate browser integrated-authentication settings. The defining expected behavior in a correctly configured agentless DSSO deployment is therefore automatic authentication based on the signed-in Windows identity, not a manual AD credential prompt. Okta documents that Desktop SSO enables users to sign in to Okta automatically when they are signed in to their Windows devices. See Okta agentless Desktop SSO documentation and agentless DSSO prerequisites.

QUESTION NO: 3

Can you include / exclude users from specific Network Zones defined in Okta from both Sign On and Password policies?

Solution: You can do this with both policy types mentioned

A. Yes

B. No

ANSWER: A

Explanation:

Yes is correct. Okta Network Zones define sets of network locations, such as IP address ranges, IP address gateways, or dynamically maintained zones, that can be used as conditions in security policy rules. Administrators can create named zones and then apply those zones when configuring access requirements for sign-on and password-related controls. This allows policy behavior to be tailored to a user's connection location—for example, applying a rule when a request originates from an approved corporate network or when it originates outside a designated trusted zone.

In Okta sign-on policy rules, network location is an available condition for determining whether and how a user can establish a session. Password policy rules can likewise use network-zone conditions to scope password requirements and password-management behavior based on the network from which the user is connecting. The policy rule configuration supports selecting applicable zones and defining whether the rule applies to connections in, or outside of, those zones. Consequently, the same Okta-defined Network Zone concept can be used for inclusion or exclusion logic in both policy types, as stated in the solution. See Okta's Network Zones documentation and Password policy documentation.

QUESTION NO: 4

In an SP-initiated SAML 2.0 flow, the SP will never redirect to Okta if the session is already active

Solution: It might be seamless for the user, but the redirect is happening

A. Yes

B. No

ANSWER: A

Explanation:

Yes is correct. In a service-provider-initiated SAML flow, the user begins at the service provider, which creates a SAML authentication request and redirects the browser to Okta, the identity provider. This redirect remains part of the protocol flow even when the user already has an active Okta session. The active session changes the user experience at Okta: Okta can recognize the existing session and satisfy the authentication request without displaying a sign-in prompt or requesting credentials again. Okta then produces a SAML assertion and redirects the browser back to the service provider's assertion consumer service. As a result, the transaction can appear seamless to the user, while browser redirects to and from Okta still occur in the background. This distinction matters when troubleshooting SAML integrations, browser behavior, session policies, and redirect URIs: absence of a visible login page does not mean that the identity-provider leg of an SP-initiated SAML transaction was skipped. Okta's documentation describes SP-initiated SAML as a flow in which the application sends an authentication request to Okta, and the SAML specification defines the request and response exchange between the service provider and identity provider. See Okta SAML concepts and OASIS SAML 2.0 Core specification.

QUESTION NO: 5

Okta AD Agents can be successfully and completely configured by:

Solution: Super administrators

A. Yes

B. No

ANSWER: A

Explanation:

Yes is correct. Super administrators have the broad administrative privileges required to fully configure and manage an Okta Active Directory agent integration. This includes adding and configuring an AD domain, setting up delegated authentication or directory import as appropriate, managing the agent connection, and configuring the assignments, imports, and provisioning behavior associated with the directory integration. The AD agent itself is installed on a Windows server that can reach the Active Directory domain controllers, then registered with the Okta tenant using an administrative account with sufficient Okta permissions. A super administrator can perform the entire Okta-side configuration because this role has full access across the Okta Admin Console, including directory integrations, security settings, applications, and lifecycle-management configuration. Okta documents that the Super Admin role has all permissions and should be assigned only where full administrative access is necessary. For the directory agent workflow and its administrative requirements, see Okta Active Directory agent documentation. For details about the Super Admin role and its permissions, see Administrators and permissions in Okta.

QUESTION NO: 6

Which is a / are best-practice(s) in a SAML 2.0 situation?

Solution: To not link your admin user from the SP via SAML with a user from Okta, if the app (SP) does not provide a SAML bypass URL

A. Yes

B. No

ANSWER: A

Explanation:

Yes is correct. It is a sound SAML administration best practice to retain an administrative access path that does not depend on the same SAML single sign-on integration being administered. If an application service provider does not offer a SAML bypass URL or another documented method for local administrator sign-in, federating the sole or primary SP administrator through Okta can create a lockout risk. For example, an Okta configuration issue, an assignment change, an IdP outage, a certificate problem, or an accidental change to the SAML application could prevent that administrator from reaching the SP's own administration console. Maintaining a separate, securely protected local SP administrator account provides a recovery path for correcting the SAML configuration and restoring normal federated access. This approach follows the broader security principle of preserving emergency or break-glass administrative access that is independent from the normal federation flow. The local account should use a strong unique password, appropriate multifactor authentication where supported, restricted access, and documented recovery procedures. Okta's SAML guidance explains the SAML trust relationship and the importance of correctly configuring the IdP and service provider, while NIST discusses the value of secure contingency and recovery capabilities for authentication systems. See Okta SAML app integration documentation and NIST SP 800-63B.

QUESTION NO: 7

With Okta you federate the 'Office 365 tenant name' (which is the default Microsoft domain you have) or the 'Office 365 domain'?

Solution: You federate with Okta both the 'Office 365 tenant name' and the 'Office 365 domain'

A. Yes

B. No

ANSWER: B

Explanation:

No is correct because federation for Microsoft 365 is configured on one or more verified Microsoft Entra ID domains, not on the tenant name as a separate federation target. A tenant has an initial Microsoft-provided `.onmicrosoft.com` domain,

while organizations commonly add and verify their own domains for user sign-in, such as `example.com`. When Okta is used as the identity provider, the relevant user sign-in domain is converted to a federated domain and its federation settings identify Okta as the authentication service. Users whose user principal names use that federated domain are then redirected to Okta when they authenticate.

The tenant remains the Microsoft Entra ID organizational container that owns domains, users, applications, and subscriptions; it is not an additional domain that must also be federated. Therefore, the statement that both the tenant name and the Office 365 domain are federated is not accurate. Administrators should verify the intended custom domain in Microsoft Entra ID and configure federation for that domain in accordance with their Okta Microsoft 365 deployment configuration. Microsoft's domain-management guidance is available in Manage custom domain names in Microsoft Entra ID, and its federation guidance is available in Manage federated domains in Microsoft Entra ID.

QUESTION NO: 8

An administrator needs to investigate why a user was denied access to an application yesterday. Which Okta feature provides event details such as the affected user, policy evaluation, outcome, and timestamp?

A. System Log

B. Profile Editor

C. Applications dashboard

D. Directory integration import preview

ANSWER: A

Explanation:

The Okta System Log provides event records for sign-ins, policy decisions, application access, administrative actions, provisioning events, and other organization activity. An administrator can search the System Log using event details, actors, targets, outcomes, and time ranges to identify why a particular access attempt was denied.

The System Log is intended for operational troubleshooting and security investigation. Organizations that require long-term retention or correlation with other security data should export or stream events to an external logging platform. See Okta System Log documentation and Okta System Log API reference.

QUESTION NO: 9

Which is a / are best-practice(s) in a SAML 2.0 situation?

Solution: To never enable SAML for all your end-users

A. Yes

B. No

ANSWER: B

Explanation:

"No" is correct because an absolute rule to never enable a SAML application for all end users is not an Okta best practice. Okta supports assigning an application to everyone, as well as to specific groups or individual users. The appropriate assignment scope is determined by the application's intended audience, licensing, access-policy requirements, and the organization's security and operational needs. For an application genuinely required by the entire workforce, assignment to all users can be appropriate and simplifies lifecycle management because eligible users receive access automatically. Before a broad production rollout, administrators should validate the SAML integration with a limited test population, confirm attribute and group mappings, verify sign-on policy behavior, and ensure the service provider accepts the assertions as expected. After validation, access should be managed according to least-privilege principles and reviewed as business requirements change. Okta's application-assignment documentation describes assignments to users and groups, including

broad assignments, while its SAML integration guidance covers configuring and testing SAML single sign-on. See Okta: Assign applications to users and groups and Okta Developer: Build a SAML SSO integration.

QUESTION NO: 10

The SCIM protocol is for provisioning and managing identity data on the web.

Solution: An application-level REST protocol

A. Yes

B. No

ANSWER: A

Explanation:

Yes is correct. SCIM, short for System for Cross-domain Identity Management, is an application-level protocol designed to automate the exchange and lifecycle management of identity information between an identity provider and cloud applications or services. It uses a RESTful architecture and standard HTTP methods, such as GET, POST, PUT, PATCH, and DELETE, to perform operations on resources including Users and Groups. Its standardized JSON schemas and endpoints enable an organization to provision accounts, update profile attributes, assign or remove group membership, and deprovision accounts consistently across integrated applications.

In Okta, SCIM integrations allow Universal Directory identities and group assignments to drive downstream account lifecycle actions automatically. For example, assigning a person to an application can create the corresponding account in the target service, while changes to attributes or group membership can be pushed through SCIM according to the application configuration. This makes SCIM a core standards-based mechanism for automated provisioning and identity-data management on the web. The SCIM specification describes it as an HTTP-based protocol for managing identities, and Okta documents SCIM as its standard protocol for provisioning integrations. See RFC 7644: SCIM Protocol and Okta SCIM overview.

QUESTION NO: 11

When does Okta bring LDAP groups into Okta? Solution: Only during LDAP JIT

A. Yes

B. No

ANSWER: B

Explanation:

No is correct because LDAP Just-In-Time provisioning is not the only mechanism through which LDAP group information can be brought into Okta. An LDAP integration can run an import, either manually or according to its configured import schedule, to retrieve users and groups from the LDAP directory. During this import process, Okta can create or update the corresponding Okta groups and evaluate LDAP group membership so that imported users can be assigned to the appropriate groups. Administrators configure which LDAP organizational units and group objects are in scope and can use the import workflow to review or automatically confirm imported changes. LDAP JIT provisioning has a different primary role: it creates or updates an Okta user when that person authenticates through delegated LDAP authentication, helping ensure access for a user who has not yet been imported. JIT can also evaluate configured group membership at authentication time, but it does not make LDAP JIT the sole path for bringing LDAP groups into Okta. Therefore, the statement that this occurs only during LDAP JIT is inaccurate. Okta's LDAP integration documentation describes the LDAP agent, imports, and directory synchronization behavior, while its JIT documentation describes the authentication-time provisioning flow. See Okta LDAP agent documentation and Okta LDAP JIT provisioning documentation.

QUESTION NO: 12

As an Okta admin, when you implement IWA, you have to know how to successfully test it to see if it's working. For this you:

Solution: Restart AD Domain Controller and go into IIS and see if you have IWA references in there

A. Yes

B. No

ANSWER: B

Explanation:

No is correct because restarting an Active Directory domain controller and merely checking IIS for Integrated Windows Authentication references is not the prescribed way to validate an Okta Integrated Windows Authentication deployment. Successful validation must confirm the end-to-end user authentication experience: a domain-joined workstation, a browser configured to permit integrated authentication to the relevant Okta/IWA endpoint, and a signed-in Windows user whose identity can be transparently authenticated by the IWA Web Agent. The meaningful result is that the user is recognized and directed into Okta without being prompted to enter Okta credentials when the applicable IWA routing rule and sign-on policy apply.

The IWA Web Agent is installed on a Windows server running IIS, but the presence of IIS configuration entries does not by itself demonstrate that the agent can communicate with Okta, validate the logged-in user, locate that user in Active Directory, and satisfy the configured Okta policy. Testing should therefore use Okta's documented IWA test process and verify the resulting authentication behavior from an appropriate client machine. Review Okta's Test the IWA Web Agent guidance and its IWA Web Agent installation documentation for the required environment and validation steps.

QUESTION NO: 13

An administrator wants an application to receive a user's department value only when the user is provisioned or updated in that application. Where should the administrator configure this attribute flow?

A. In the Okta user to application user profile mapping

B. In the application to Okta user profile mapping

C. In the application's sign-on policy

D. In the authenticator enrollment policy

ANSWER: A

Explanation:

In the Okta user to application user profile mapping is correct. This mapping uses the Okta user profile as the source and the target application user profile as the destination. It controls how values, including department and custom attributes, are transformed and sent to the application during supported provisioning operations.

An Active Directory to Okta mapping controls how directory data enters the Okta user profile, while an application to Okta mapping is used for imports from an application. The target application must support provisioning and expose a compatible writable attribute for Okta to send the value. See Okta attribute mapping documentation.

QUESTION NO: 14

Whenever you make an API call, you will then get back:

Solution: Response headers

A. Yes

B. No

ANSWER: A

Explanation:

Yes is correct. An HTTP API call results in an HTTP response, and that response includes response headers along with a status code and, when applicable, a response body. Okta's APIs follow this HTTP model. Response headers communicate important metadata about the result, such as the content type, request identifiers used for troubleshooting, pagination links for list responses, and rate-limit information. In particular, Okta exposes rate-limit values in headers including `X-Rate-Limit-Limit`, `X-Rate-Limit-Remaining`, and `X-Rate-Limit-Reset`, allowing API clients to monitor available request capacity and respond appropriately before limits are exceeded. Headers remain part of the response even when a request does not return a substantive JSON body, such as many successful delete operations or responses whose status indicates no content. API integrations should therefore inspect response headers as well as the HTTP status and body, particularly for correlation, paging, and rate-limit handling. Okta documents the structure and use of response headers in its API guidance and details the rate-limit headers separately. See Okta API overview and Okta rate-limit best practices.

QUESTION NO: 15

An administrator wants users from a partner organization to authenticate through an external Identity Provider, while employees authenticate directly through Okta. Which configuration is used to make this routing decision before authentication?

A. An Identity Provider routing rule

B. An app sign-in policy rule

C. A group rule

D. An application provisioning rule

ANSWER: A

Explanation:

An Identity Provider routing rule is used to determine which identity provider handles an authentication request. Routing rules can evaluate conditions such as the user's login domain, network zone, device platform, or application context, and then route the user either to Okta or to a configured external identity provider.

For this scenario, a rule can match the partner email domain and route those users to the external Identity Provider, while other users follow the default Okta authentication path. An app sign-in policy controls authentication requirements for an application after the appropriate authentication path is selected; it does not replace IdP routing rules for this purpose. See Okta Identity Provider routing rules documentation.