# OKTA ADMINISTRATOR CERTIFICATION PRACTICE EXAM (SAMPLE)

## STUDY GUIDE


## SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

**VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE**

https://oktaadmin.examzify.com

# Table of Contents

# Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn't just about memorization, it's about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you're preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You'll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it's correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It's ideal for learners who want to:

- Practice answering questions under realistic conditions,
- Improve accuracy and speed,
- Review explanations to strengthen weak areas, and
- Approach the exam with greater confidence.

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn't about getting every question right the first time, it's about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let's begin.

# How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here's how to get the most out of your Examzify study guide:

### 1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Your goal is to identify knowledge gaps early.

### 2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations.

### 3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

### 4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

### 5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

### 6. Repeat and Review

Don't just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning. Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There's no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly, adapt the tips above to fit your pace and learning style. You've got this!

# Questions

1. **Can a Human Resources Source application be used to deactivate users in Okta?**

   A. Yes

   B. No

   C. Only for certain user groups

   D. Only for inactive users

2. **Which password policy feature should an Okta Administrator use to prevent users from changing their new password for at least five days?**

   A. Session Lifetime

   B. Password complexity

   C. Minimum password age

   D. Password expiration

3. **Does Okta recommend ensuring that password settings match the Active Directory password policy?**

   A. Yes

   B. No

   C. Occasionally

   D. Only for custom applications

4. **Is the URL https://org.okta.com/login/sso_iwa? valid for bypassing Desktop SSO login mode?**

   A. Yes

   B. No

   C. Only for certain users

   D. Only in specific zones

5. **What does enabling Just-in-time provisioning do when an Active Directory user signs into Okta?**

   A. Creates new user accounts manually

   B. Transfers user data directly from Okta

   C. Automatically provisions user accounts based on AD attributes

   D. Deletes unused user accounts from Okta

**6. Must the Okta username format be an email address for a company using Desktop SSO to sync passwords to SWA applications?**

A. Yes

B. No

C. Only for certain user roles

D. Only for users with secondary authentication

**7. What is the expected behavior when an application is enabled as a source?**

A. Okta provisions users to the application

B. The application provisions users to Okta

C. Okta syncs with external directories

D. Users manage their own credentials

**8. Can an Okta Administrator override the attribute mapping from external sources?**

A. Yes, it can be overridden anytime

B. No, once set, it cannot be changed

C. Only under exceptional cases

D. This requires direct API access

**9. What condition can be configured to prompt users for Multifactor Authentication in a global session policy rule?**

A. At every sign in

B. Only for first-time logins

C. After every password change

D. When accessing sensitive data

**10. An Okta admin is evaluating capabilities of authorization servers. Which ability is supported only by the organization's authorization server?**

A. Integrate with third-party applications

B. Utilize custom branding

C. Manage API scopes through Okta

D. Enforce password policies

# Answers

1. A
2. C
3. A
4. B
5. C
6. B
7. B
8. A
9. A
10. C

# Explanations

## 1. Can a Human Resources Source application be used to deactivate users in Okta?

A. Yes

B. No

C. Only for certain user groups

D. Only for inactive users

*A Human Resources Source application can indeed be used to deactivate users in Okta. This functionality is particularly effective because HR systems typically manage the lifecycle of employee records, including the processes related to hiring, offboarding, and changes in employment status. In Okta, when integrated with an HR Source application that supports deactivation, user accounts can automatically be marked as inactive or deactivated based on their employment status in the HR system. This can help streamline user management and ensure that users who are no longer employees do not retain access to organizational resources. The integration allows for real-time updates to user information and status, enhancing security and compliance within the organization. Utilizing HR systems for user deactivation also promotes efficiency and accuracy in user lifecycle management, reducing the administrative burden on IT departments and ensuring that user access aligns with current employee statuses.*

## 2. Which password policy feature should an Okta Administrator use to prevent users from changing their new password for at least five days?

A. Session Lifetime

B. Password complexity

C. Minimum password age

D. Password expiration

*To prevent users from changing their new password for at least five days, the appropriate feature to utilize is the minimum password age. This policy setting is designed specifically to ensure that once a user sets their new password, they must retain that password for a defined period — in this case, five days — before being allowed to change it again. This helps maintain security by reducing the chances of users quickly cycling through passwords, which can lead to weaker security practices. Minimum password age policies are essential in environments where password security is a priority, as they encourage users to think carefully about their password choices, rather than routinely changing them without due consideration. This feature also assists in compliance with organizational security standards that require stable password usage over a specific timeframe. Other features listed, while related to password management, serve different purposes. Session lifetime governs how long a user session remains active before re-authentication is required. Password complexity pertains to the rules around the construction of the password itself, ensuring it meets certain criteria (like length or character diversity) to enhance security. Password expiration, on the other hand, dictates when a password must be changed, but does not restrict how soon a user can change it after setting a new password. Thus, minimum password age is the most relevant feature*

## 3. Does Okta recommend ensuring that password settings match the Active Directory password policy?

A. Yes

B. No

C. Occasionally

D. Only for custom applications

*Yes, Okta recommends ensuring that password settings match the Active Directory (AD) password policy. This alignment is crucial for maintaining a consistent user experience across the organization, especially when integrating Okta with Active Directory for user authentication and provisioning. When password policies are harmonized, users are less likely to face confusion or errors during the login process, as they will encounter familiar rules and requirements. Additionally, having matching policies supports security best practices by reducing vulnerabilities that could arise from discrepancies in password requirements between Okta and AD. This approach also simplifies management for IT administrators since they only need to enforce one set of policies. Matching the policies ensures that any changes made to the password settings in AD are reflected uniformly in Okta, further preventing any potential conflicts and enhancing the overall security posture of the organization. This consistency is especially important for companies relying on Single Sign-On (SSO) and seamless user experiences across various applications and services.*

## 4. Is the URL https://org.okta.com/login/sso_iwa? valid for bypassing Desktop SSO login mode?

A. Yes

B. No

C. Only for certain users

D. Only in specific zones

*The URL https://org.okta.com/login/sso_iwa? is not valid for bypassing Desktop SSO (Single Sign-On) login mode. In this scenario, the inherent purpose of the URL link is tied to SSO integration within certain environments and does not facilitate bypassing the established SSO protocol across the board. Desktop SSO is designed to provide a seamless authentication experience for users by leveraging cached credentials on their devices. Thus, bypassing this login mode through a specific URL would compromise the intended security and efficiency of SSO. Essentially, the Desktop SSO feature is built to streamline user login experiences, and circumventing this would go against its fundamental design. The other options imply varying degrees of exceptions or allowances which are not applicable without proper context or configurations being met. Thus, it upholds the principle that bypassing a secure login method cannot be done simply through the provided URL.*

**5. What does enabling Just-in-time provisioning do when an Active Directory user signs into Okta?**

A. Creates new user accounts manually

B. Transfers user data directly from Okta

C. Automatically provisions user accounts based on AD attributes

D. Deletes unused user accounts from Okta

*Enabling Just-in-time provisioning (JIT) allows for the automatic creation of user accounts in Okta when an Active Directory user logs in for the first time. This process utilizes the attributes from the user's Active Directory account to provision a new Okta account seamlessly and without requiring any manual intervention. When a user authenticates via SAML, for example, JIT provisioning can take action using the user's details passed during the login process, such as their name, email address, and group memberships. This convenience reduces administrative overhead by eliminating the need for manual account creation, allowing users to gain instant access to Okta and its integrations with the necessary permissions aligned with their AD attributes. The other options do not accurately reflect the primary function of JIT provisioning. Manual account creation is not part of JIT as it specifically automates this process. Transferring user data directly from Okta does not accurately describe how JIT interacts with Active Directory for user creation. Additionally, deleting unused accounts is not a feature of JIT provisioning; rather, it relates to lifecycle management, which is a different process altogether.*

**6. Must the Okta username format be an email address for a company using Desktop SSO to sync passwords to SWA applications?**

A. Yes

B. No

C. Only for certain user roles

D. Only for users with secondary authentication

*The correct answer is that the Okta username format does not have to be an email address for a company using Desktop SSO to sync passwords to SWA (Secure Web Authentication) applications. In the context of Okta and Desktop SSO, username formats can be flexible. While many organizations choose to use email addresses as usernames for consistency and ease of user management, Okta allows for different formats. This flexibility means that usernames can be simple alphanumeric strings or any custom format that meets the organization's needs. Using an email address as a username is common because it is easily recognizable and typically unique. However, opting for a different format can also work effectively, especially in cases where an organization may want to eliminate the dependency on email addresses for user identification — for instance, in systems where usernames are tied to internal IDs or employee numbers. This understanding is crucial for administrators because it allows them to define a username policy that aligns with their organization's preferences and operational requirements, rather than being restricted to using email addresses exclusively.*

## 7. What is the expected behavior when an application is enabled as a source?

A. Okta provisions users to the application

B. The application provisions users to Okta

C. Okta syncs with external directories

D. Users manage their own credentials

*When an application is enabled as a source in Okta, it indicates that the application will be responsible for provisioning users into Okta. In this setup, Okta acts as a consumer of identity information provided by the application. This means that the application has the authority and mechanism to create, update, or deactivate user accounts directly in Okta based on its own user management processes. Enabling an application as a source allows organizations to streamline user management by having the application push identity details into Okta, reducing the need for manual entry and ensuring alignment between user data in the application and in Okta. This is especially useful in environments where user permissions and attributes may be dynamically adjusted within the application itself, further enhancing security and efficiency in user lifecycle management. The implications of this setup can be significant, especially for organizations using multiple applications as their source of truth. Instead of relying on Okta to provision users, the application takes the lead, facilitating greater integration and automation of identity processes.*

## 8. Can an Okta Administrator override the attribute mapping from external sources?

A. Yes, it can be overridden anytime

B. No, once set, it cannot be changed

C. Only under exceptional cases

D. This requires direct API access

*An Okta Administrator can indeed override the attribute mapping from external sources at any time. This flexibility is integral to managing and adjusting integration settings based on the evolving needs of an organization. In practice, administrators may encounter different scenarios where changes to attribute mapping are necessary, such as updates in the data structure from an external application, changes in business processes, or the need to address specific user attributes more accurately. This capability allows for efficient management of user data and ensures that the information pulled from external sources aligns perfectly with an organization's requirements. This feature is designed to be user-friendly, enabling administrators to make such changes without needing specialized technical skills or direct API access. Consequently, the ability to modify these mappings enhances an organization's adaptability and control over its identity management processes.*

**9. What condition can be configured to prompt users for Multifactor Authentication in a global session policy rule?**

A. At every sign in

B. Only for first-time logins

C. After every password change

D. When accessing sensitive data

*Configuring a global session policy rule to prompt users for Multifactor Authentication (MFA) at every sign-in is an effective strategy for ensuring ongoing security. This condition means that each time a user attempts to sign in, they will have to complete an MFA challenge, which adds another layer of verification beyond just their username and password. Doing so helps protect against unauthorized access, especially in environments where the risk is high or compliance needs require stringent security measures. While prompting MFA only for first-time logins could limit security by not addressing subsequent access attempts, and requiring it after every password change might not effectively secure ongoing sessions, prioritizing MFA at each sign-in addresses potential threats continuously. Accessing sensitive data can also be crucial for triggering MFA; however, many security policies advocate for universal prompts to avoid gaps in security based on user behavior or specific actions taken.*

**10. An Okta admin is evaluating capabilities of authorization servers. Which ability is supported only by the organization's authorization server?**

A. Integrate with third-party applications

B. Utilize custom branding

C. Manage API scopes through Okta

D. Enforce password policies

*The ability to manage API scopes through Okta is a specific feature supported by an organization's authorization server. Authorization servers in Okta are designed to handle access and permissions for APIs, and one of their core functions is to define and manage API scopes. Scopes determine the level of access that clients (like applications) can request when attempting to gain authorization to access a resource. With this specific feature, administrators can create, modify, or delete custom scopes as needed, allowing them to tailor the authorization process based on the organization's unique requirements. This includes fine-tuning what resources can be accessed and under what conditions, enhancing security, and ensuring that applications only have the access they absolutely need. In contrast, the other options are features that may not be unique to an organization's authorization server. For instance, integrating with third-party applications can occur through various methods and is not solely governed by the capabilities of the authorization server. Utilizing custom branding is often a feature of Okta's user interface and can apply to multiple services outside of just the authorization server, similarly enforcing password policies is typically managed through general security settings rather than being an exclusive feature of the authorization server itself.*

# Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we'd love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://oktaadmin.examzify.com

We wish you the very best on your exam journey. You've got this!