

New 2019 Okta Certified Consultant Maintenance Exam

The Okta Certified Consultant Maintenance Exam is an on-demand, unproctored, open book exam. This exam is intended for individuals who hold the Okta Certified Consultant certification and need to ensure their certification remains current.

- **Number of Questions:** This exam consists of 36 questions covering a list of topics outlined below.
- **Time Limit:** The total amount of time allotted to complete this exam is 75 minutes.
- **Passing Score:** Okta does not provide passing scores; however, at the completion of the exam, a Pass/Fail decision will be provided.
- **Retake Policy:** The normal Okta certification retake policy outlined in the [Certification Program Handbook](#) does **NOT** apply to this maintenance exam. In addition, for this maintenance exam, in particular, exam takers will have a second shot. What this means is that you will be allowed to sit the exam twice for a one-time fee of 100 USD. If you pass the exam, you will not be allowed to retake it. However, if you fail the exam, you can request a voucher at certification@okta.com to re-sit the exam. If you fail for a second time, you will need to pay 100 USD to retake the exam for the third time.

Topics Covered on the Exam

Section	Objective	Task(s)	Link(s) to Related Documentation
User Lifecycle Management - Level I	Access Request Workflow for App Self-Service	<ul style="list-style-type: none"> ● Demonstrate understanding of how Access Request Workflow for App Self-Service works 	<ul style="list-style-type: none"> ● Access Request Workflow
	Configuring App Approval Workflow	<ul style="list-style-type: none"> ● Demonstrate knowledge of the App Approval Workflow 	<ul style="list-style-type: none"> ● Configure App Approval Workflow
	Admin Role Behavior Changes	<ul style="list-style-type: none"> ● Demonstrate understanding of admin role behavioral changes 	<ul style="list-style-type: none"> ● The Super Admin Role
Security - Level I	Multifactor Authentication	<ul style="list-style-type: none"> ● Demonstrate knowledge of the benefits of U2F as a multi-factor authentication factor 	<ul style="list-style-type: none"> ● Web Authentication (FIDO2)
	Group Membership Rules Limit Increase	<ul style="list-style-type: none"> ● Demonstrate knowledge of the benefits of the increase in the limit of Group Membership Rule 	<ul style="list-style-type: none"> ● Create Group Rules
	Voice Call as an MFA Factor	<ul style="list-style-type: none"> ● Demonstrate knowledge of the process to configure Voice Call as a factor 	<ul style="list-style-type: none"> ● Multifactor Authentication

	Passing Username to Target Orgs	<ul style="list-style-type: none"> • Demonstrate understanding of the identity provider discovery flow 	<ul style="list-style-type: none"> • Identity Provider Discovery
	Location-based network zones	<ul style="list-style-type: none"> • Demonstrate knowledge of the use of location-based network zones 	<ul style="list-style-type: none"> • Define Geolocation for a Dynamic Zone
Identity and Access Management - Level II	Push Notification for Okta RADIUS Agent	<ul style="list-style-type: none"> • Demonstrate knowledge of the process to configure Autopush for RADIUS 	<ul style="list-style-type: none"> • Autopush for RADIUS
	Social Identity Providers	<ul style="list-style-type: none"> • Demonstrate knowledge of the process to add social identity providers in Okta 	<ul style="list-style-type: none"> • Identity Providers
User Lifecycle Management - Level II	Attribute Mapping Overrides	<ul style="list-style-type: none"> • Demonstrate understanding of how attribute mapping overrides work 	<ul style="list-style-type: none"> • Application-Based Mapping
	Configuring App Approval Workflow	<ul style="list-style-type: none"> • Demonstrate understanding of the process to configure the App Approval Workflow 	<ul style="list-style-type: none"> • Configure App Approval Workflow
	Assigning Users to Multiple Groups in One Group Rule	<ul style="list-style-type: none"> • Demonstrate understanding of group rules 	<ul style="list-style-type: none"> • Group Rules
Security - Level II	Extended Client Access Policy Capability for Apps	<ul style="list-style-type: none"> • Determine when to add an app-based sign-on policy to allow or restrict access to an application 	<ul style="list-style-type: none"> • Add Sign-on policies for applications
	Establish Device Trust for macOS	<ul style="list-style-type: none"> • Demonstrate knowledge of the process to enable device trust for macOS 	<ul style="list-style-type: none"> • Add Sign On policies for applications • Enforce Okta Device Trust for Jamf Pro-managed macOS devices
Identity and Access Management - Level III	Push Notifications for Okta RADIUS Agent	<ul style="list-style-type: none"> • Determine when to enable Autopush for RADIUS 	<ul style="list-style-type: none"> • Autopush for RADIUS
	SCIM App Wizard	<ul style="list-style-type: none"> • Demonstrate understanding of the SCIM App Wizard 	<ul style="list-style-type: none"> • Using the App Integration Wizard
	Social Identity Providers	<ul style="list-style-type: none"> • Demonstrate in-depth knowledge of social identity providers and social authentication 	<ul style="list-style-type: none"> • Using Facebook for Login
	CSV Directory Integration	<ul style="list-style-type: none"> • Demonstrate understanding of CSV directory integration 	<ul style="list-style-type: none"> • CSV Directory Integration
Customizations	Custom Email Domain	<ul style="list-style-type: none"> • Demonstrate knowledge of the process to configure custom email domains 	<ul style="list-style-type: none"> • Configure a Custom Email Domain
	Custom URL Domain	<ul style="list-style-type: none"> • Demonstrate knowledge of the process to configure custom URL domains 	<ul style="list-style-type: none"> • Customize Your Okta Org • Configure a Custom URL Domain
Security - Level III	Establish Device Trust for macOS	<ul style="list-style-type: none"> • Demonstrate understanding of how device trust works for macOS 	<ul style="list-style-type: none"> • Enforce Okta Device Trust for Jamf Pro-managed macOS devices

User Lifecycle Management - Level III	Assigning Users to Multiple Groups in One Group Rule	<ul style="list-style-type: none">• Determine when to assign users to multiple groups in one group policy	<ul style="list-style-type: none">• Group Rules
---------------------------------------	--	---	---

Register for your exam with [Examity](#) now!

Troubleshooting Your Unproctored Certification Maintenance Exam

In the very rare event that your exam freezes or stops loading, kindly **Refresh** your **Browser Window** to correct the problem and resume your exam. Please note, refreshing your exam browser window will take you back to the **Introductions Screen** of the exam. However, all of your answers are retained, so once you click the **Take Exam** button again, your exam will resume where you left off. You will not lose any of your previous responses.