Prep Content for Okta Certified Professional - Hands-on Configuration Exam
Congratulations on taking this step toward earning your first Okta Certification--the Okta Certified Professional!

This guide is designed to help you prepare for the Okta Certified Professional Hands-on Configuration Exam. It covers the topics on the exam and it includes links to demo videos showing the configuration of the features associated with those core topics.

Anyone who passes this hands-on configuration exam will be awarded the Okta Certified Professional certification.

The Okta Certified Professional certification is a prerequisite for the Okta Certified Administrator and Okta Certified Consultant certifications.
How to use this prep guide

Review the use cases and tasks listed on page 5.

Do you have experience administering those use cases and performing most of those tasks?

YES

Go to page 9, watch the demos of any tasks that you have not performed, and practice those tasks

NO

Review the entire guide, but focus on those topics and tasks that are unfamiliar to you
## Exam Format

<table>
<thead>
<tr>
<th>Item Type</th>
<th>This hands-on configuration exam consists of four use cases. Each use case requires the completion of several configuration tasks. Participants will complete tasks in pre-assigned Okta Preview Orgs.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Allotted</td>
<td>2 hours</td>
</tr>
<tr>
<td>Availability</td>
<td>24x7 Proctored by Examity</td>
</tr>
<tr>
<td>Scoring</td>
<td>Automated (Candidates will receive official Pass/Fail decision within 72 hours)</td>
</tr>
</tbody>
</table>
Use Cases and Tasks Covered on the Exam

Onboarding
- Create users
- Assign admin roles
- Update user profiles
- Create groups
- Assign users to groups
- Create group rules

Application Setup
- Add an app integration
- Set up inbound saml
- Set up lifecycle management for the application
- Assign a group to the application

Security Enforcement
- MFA factor configuration
- Set up MFA enrollment for users in a group
- Create a sign-on policy
- Create a network zone

Attribute Mapping and Offboarding
- Define attribute mappings for an application
- Deactivate a user
- Create custom attributes
Prerequisites

Individuals who are interested in taking this hands-on configuration exam should have experience performing the following tasks in Okta:

- Defining Users in Okta
- Configuring Groups
- Configuring SSO with SAML
- Configuring Okta Lifecycle Management (App Provisioning)
- Configuring Universal Directory
- Implementing the Okta Policy Framework

We highly recommend that individuals who do not have hands-on experience with Okta attend Okta Essentials prior to attempting this exam.
Document Map

1. Define Your Users in Okta
2. Manage Users using Groups
3. Configure SSO & Provisioning
4. Manage User Profiles in UD
5. Implement the Okta Policy Framework
# Table of Contents

<table>
<thead>
<tr>
<th>Module</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define Your Users in Okta</td>
<td>11</td>
</tr>
<tr>
<td>Manage Users using Groups</td>
<td>25</td>
</tr>
<tr>
<td>Configure SSO and Provisioning</td>
<td>33</td>
</tr>
<tr>
<td>Manage User Profiles in Universal Directory</td>
<td>58</td>
</tr>
<tr>
<td>Implement the Okta Policy Framework</td>
<td>70</td>
</tr>
<tr>
<td>Offboarding</td>
<td>93</td>
</tr>
</tbody>
</table>
# Demo Videos

<table>
<thead>
<tr>
<th>Hyperlinks to Demo Videos</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="#">Create and Activate Okta-Sourced Users</a></td>
</tr>
<tr>
<td><a href="#">Assign Administrative Roles</a></td>
</tr>
<tr>
<td><a href="#">Create Groups</a></td>
</tr>
<tr>
<td><a href="#">Configure IdP-initiated SAML SSO for Org2Org</a></td>
</tr>
<tr>
<td><a href="#">Configure Lifecycle Management between Okta orgs</a></td>
</tr>
<tr>
<td><a href="#">Manage Profile Attributes</a></td>
</tr>
<tr>
<td><a href="#">Set Up Zones</a></td>
</tr>
<tr>
<td><a href="#">Set Up Multifactor Enrollment</a></td>
</tr>
<tr>
<td><a href="#">Set Up an Okta Sign-On Policy</a></td>
</tr>
<tr>
<td><a href="#">Offboarding</a></td>
</tr>
</tbody>
</table>
Where Are We?

- Define Your Users in Okta
  - Manage Users using Groups
  - Configure SSO & Provisioning
  - Manage User Profiles in Universal Directory
  - Implement the Okta Policy Framework
  - Offboarding
Define Your Users in Okta
Module Story
Define Your Users in Okta

Why?
As the first step toward adopting Okta Identity cloud, how to get your user information into Okta so that you can manage from one place?

Does your organization have the issue of proliferation of privileged users, and how to limit the access of these users?

Objectives
• Create and manage user accounts in Okta
• Set administrative permissions for user accounts
# Three Types of People in Okta

<table>
<thead>
<tr>
<th>Okta-sourced</th>
<th>Directory-sourced</th>
<th>Application-sourced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile managed by</td>
<td>Okta</td>
<td>Directory</td>
</tr>
<tr>
<td>Authenticated by</td>
<td>Okta</td>
<td>Directory / Delegated Authentication</td>
</tr>
<tr>
<td>Credential store</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Okta User Profile Attributes

• Base Attributes
  – 31 default base attributes for all users in an org

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Required</th>
<th>Optional</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username &amp; Primary email</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>First name &amp; Last name</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Other attributes</td>
<td></td>
<td>Y</td>
</tr>
</tbody>
</table>

• Custom Attributes: Define additional attributes that are not available in the base attributes.
User Statuses

Initial States (On-boarding)

- **Staged**: The (new) user account has been created, but the activation process has not been initiated.
- **Pending User Action**: The user account has been added and the activation has been initiated, but the user has not yet set a password.

Blocked States

- **Password Reset**: The user is allowed to resolve forgotten password issue by resetting the password without relying on the service desk.
- **Password Expired**: The account password has expired and needs to be changed.
- **Locked Out**: The account has been locked due to a consecutive number of incorrect passwords used.

Termination State

- **Deactivated**: The user account is inactive and admin can’t assign any applications to the user.
- **Suspended**: The user cannot log in due to an action taken by an administrator.
Create Accounts
Creating Individual Okta-sourced Users

- **Required Attributes**
  - First name
  - Last name
  - Username
  - Primary email

- **Configuration** determines user status
  - Password: Set by user
  - Send user activation email now
## Account Initial States

<table>
<thead>
<tr>
<th>Configuration in UI</th>
<th>Status</th>
<th>What does it mean?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Staged</td>
<td>Account has been created but is in dormant state.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>Pending user</td>
<td>Account has been created and activation has been initiated, but the user has</td>
</tr>
<tr>
<td></td>
<td>action</td>
<td>not yet set a password.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>Active</td>
<td>Account is active and can be assigned to applications or services.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Create and Activate Okta-Sourced Users

Click here to watch the Demo Video.

This demo covers the following topics:

- Sign into Okta Org
- Review User and Admin Dashboard
- Create and Activate account; user defines password
- Create and Activate account; admin defines password
- Review User Account (Apps, Groups & Profile)
- Update Profile data
- Review User Statuses and Lifecycle Operations
Manage Privileged Account
Assign Administrator Permissions

Role based assignment:

• Can be assigned to any user
• Enables you to segment administrators based on job functions and roles
## Administrator Role Comparisons

<table>
<thead>
<tr>
<th>Role</th>
<th>Super</th>
<th>Organization</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Has full access to perform all administrative tasks and permission</td>
<td>• Can perform most org-wide settings</td>
<td>• Can manage profile information</td>
</tr>
<tr>
<td></td>
<td>sets in Okta</td>
<td>• Can perform all management tasks for users and groups.</td>
<td>• Can view users and groups, but not modify either</td>
</tr>
<tr>
<td></td>
<td>• Only role that can assign admin privileges</td>
<td>• Cannot perform any application management tasks</td>
<td>• Can manage information on applications to which they are assigned access</td>
</tr>
<tr>
<td>Group</td>
<td>• Can create users, deactivate users, reset passwords</td>
<td>• Can view and run reports</td>
<td>• Can View users</td>
</tr>
<tr>
<td></td>
<td>• Can also be used restrict these tasks to a select group or groups of Okta users.</td>
<td>• Can view users, groups, and applications, but cannot modify any settings</td>
<td>• Can reset password and MFA</td>
</tr>
<tr>
<td></td>
<td>• Cannot perform group creation and any application management tasks</td>
<td>• Can view, but not modify organizational settings</td>
<td>• Can clear user session</td>
</tr>
<tr>
<td>Read Only</td>
<td>• Can view and run reports</td>
<td>• Can view, but not modify organizational settings</td>
<td>• Can unlock users</td>
</tr>
<tr>
<td>Help Desk</td>
<td>• Can View users</td>
<td>• Can view, but not modify organizational settings</td>
<td>• Can unlock users</td>
</tr>
</tbody>
</table>
Assign Administrative Roles

Click here to watch the Demo Video.

This demo covers the following topic:

- Assign Okta Administrative Roles Based on Job Role
Where Are We?

- Define Your Users in Okta

**Manage Users using Groups**
- Configure SSO & Provisioning
- Manage User Profiles in Universal Directory
- Implement the Okta Policy Framework
- Offboarding
Manage Users using Groups
Module Story
Manage Users using Groups

Why?
Do you need to easily identify people in similar job functions, requiring similar application access using similar access policies?

Objectives
• Describe Okta group types
• Create groups
• Populate group members with group rules
<table>
<thead>
<tr>
<th>Okta</th>
<th>Directory</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Okta groups are created and membership is managed in Okta.</td>
<td>• Directory groups are created and membership is managed in the external directory service.</td>
<td>• Application groups are created and membership is managed in the application.</td>
</tr>
<tr>
<td>• Only Okta groups can contain Okta, directory and application sourced users.</td>
<td>• Only directory-sourced users can be members of directory groups; this is established in the external directory service.</td>
<td>• Members of application groups are pulled into Okta during application creation.</td>
</tr>
<tr>
<td></td>
<td>• Directory groups are copied into Okta.</td>
<td>• Application groups are copied into Okta.</td>
</tr>
<tr>
<td></td>
<td>• If the external directory instance is deactivated or deleted, the associated groups no longer appear in Okta.</td>
<td>• If the application connector is deactivated or deleted, the group no longer appears in Okta.</td>
</tr>
</tbody>
</table>
Groups in Okta

- **Create an Okta Group**
- **Okta Group**
- **Active Directory Group**
- **Application Groups**
Supported Features

- Easily add group members and assign app(s) to a group
- Use group rules for automating group membership
Group Rules

• Can be configured based on any user attribute or group membership

• Are written as expressions using:
  – Expression Builder
  – Expression Editor

• User profile update will trigger rule evaluation
Create Groups

Click [here](#) to watch the Demo Video.

This demo covers the following topics:

- Create Help Desk Group
- Add User Manually to Help Desk Group
- Create Sales Group
- Configure Group Rule to Add User Dynamically to Sales Group
Where Are We?

- Define Your Users in Okta
- Manage Users using Groups
- **Configure SSO & Provisioning**
  - Manage User Profiles in Universal Directory
  - Implement the Okta Policy Framework
  - Offboarding
Configure SSO & Provisioning
Module Story

Configure SSO & Provisioning

Why?

• Does your organization have an enterprise fragmentation problem – employees have to log into and switch between multiple apps and websites to complete their work?
• Does your organization use separate systems that govern the identity lifecycle of a user?

Objectives

• Given an application, select the appropriate authentication method for SSO access
• Configure application SSO access following company’s policies
• Automate user account management with application provisioning/deprovisioning
Cloud SSO and Provisioning with the Okta Integration Network (OIN)

7,000+

1330+ SAML
150+ Mobile
290+ Provisioning

Connect to your favorite cloud applications in minutes.
Okta Integration Network (OIN)

Search the OIN for application connectors

Configured company applications

Publicly available applications on the OIN
Single Sign-On

- SWA
- SAML
- WS-Fed
- OIDC
Primary vs. Federated Authentication

**Primary authentication**: the process of proving the identity of a person or system.

**Federated authentication**: the process by which an app or site requests proof of authentication from a trusted source.
General Configurations
Application Configurations

Every application has different configurations varying by SSO integration method and features supported.
General Settings

• General Settings include:
  – App Settings
  – VPN Notification
  – App Embed Link

• The contents of the General Settings vary for each application.
Sign On

The Sign On tab contains application connection options where you can configure settings for:

- Sign-on methods
- Credentials details (Application username format; Password reveal)
- Sign-on policies
Assignments

• Any user or group can be assigned to an application.
• Users who are members of groups are automatically assigned the application if the group is assigned to the application.
Configure SAML SSO
The Three Roles in SAML

- **Identity Provider**
- **End User**
- **Service Provider**

- Authenticate
- Assert
- Provide
The Three Roles in SAML – Communication

Identity Provider

Assertion request

SAML Assertion
Information a SP needs about the person accessing the SP site.

Service Provider

Assertion consumer endpoint (Assertion Consumer Service)

IdP endpoint (SSO service)

Browser

Assertion request

ACS URL
IdP-Initiated SSO with SAML

Browser

Access Okta login page
Return login form
Submit user credentials
Return end user dashboard
Request to access app
Redirect to app
Forward SAML response to ACS URL
Return app landing page

App

Authenticate user
Establish session

Okta

Construct SAML assertion

ACS = Assertion Consumer Service
SP-Initiated SSO with SAML

Browser

Access app page
Redirect
Request SAML authentication
Return login form
Submit user credentials
Redirect
Forward SAML response to ACS URL
Return app page

App

No valid session detected

Okta

No valid session detected
Authenticate user and generate SAML assertion

ACS = Assertion Consumer Service
The Essential Settings

To establish trust relationship between two Okta orgs (aka Org2Org), you need to configure the following essential settings:

- **Identity Provider Certificate**: A self-signed X.509 certificate issued by IdP to sign or encrypt messages.
- **Issuer**: The unique ID of IdP that issues SAML assertion.
- **Entity ID**: The unique URL that identifies SP.
Configure IdP-initiated SAML SSO for Org2Org

Click here to watch the Demo Video.

- This demo covers configuring trust relationship between two Okta orgs
Provision Users to Applications
Streamline Joiner-Mover-Leaver Process with Okta

**Source Identity:**
- HR Systems
- Directories
- Self Service Registration

**Joiner**
- Immediate
- Scheduled

**Assign Resources**
- Birthright access
- Self Service Request

**Mover**
- Job Changes
- Promotions
- Marriage
- Leave of Absence

**Leaver**
- Immediate
- Scheduled
Configure Application Provisioning – API Integration

Some apps require a token to authenticate against their API.
Account Provisioning

Source of account: On-prem Directory, HR/CRM App

Import:
- AD/LDAP

Push:
- Salesforce
- Office 365
- Google
- Box

Application
Configure Provisioning – Downstream Application

Provisioning to App

Create Users

Creates or links a user in Okta Org2Org when assigning the app to a user in Okta.

The default username used to create accounts is set to Okta username.

Update User Attributes

Okta updates a user's attributes in Okta Org2Org when the app is assigned. Future attribute changes made to the Okta user profile will automatically overwrite the corresponding attribute value in Okta Org2Org.

Deactivate Users

Deactivates a user's Okta Org2Org account when it is unassigned in Okta or their Okta account is deactivated. Accounts can be reactivated if the app is reassigned to a user in Okta.

Sync Password

Creates a Okta Org2Org password for each assigned user and pushes it to Okta Org2Org.
Configure Lifecycle Management between Okta orgs

Click here to watch the Demo Video.

This demo covers the following topics:

• Review Active Org1 Users
• Configure Provisioning in Okta (To App)
• Assign Users to Application and Verify Provisioning
• Test IdP-initiated SSO Flow (Validate Previous SAML Configuration)
Where Are We?

- Define Your Users in Okta
- Manage Users using Groups
- Configure SSO & Provisioning
- Manage User Profiles in Universal Directory
  - Implement the Okta Policy Framework
  - Offboarding
Manage User Profiles in Universal Directory
Module Story
Universal Directory

Why?
Do you want your user profile information to match across all applications and directories?
Do you want to take attribute data coming in from a source and transform it so that it is represented correctly in Okta?

Objectives
• Describe how Okta maintain a single source of truth using profile sourcing
• Manage user profile in Universal Directory
• Transform and map user profile attributes
Centralized User Management with Universal Directory

- Universal Directory
  - Provide foundation
  - Sync information
  - Unify policy management
- Single Sign-On
- Lifecycle Management
- MFA
About User Profiles

User profile is a record of information stored in Okta Universal Directory that contains specific user attributes.
User Profile Attributes

- User profiles for applications and directories consist of both base attributes and custom attributes.
- **Okta user profile** – The Okta user profile can be extended with rich custom attributes.
- **Application user profile** – Each app/directory controls the attributes that Okta can import from or push to the app/directory.
Adding Custom Attributes

Data Types
- String
- Number
- Boolean
- Integer
- Array of strings
- Array of numbers
- Array of integers
- Linked object

Attribute Options
- Enumerated values
- Required/optional
- Data quality constraints
Within Okta, a schema is a container to manage object classes and attributes. The object class is a container to manage the attributes, which holds the data.
Profile Editor

- Add and remove attributes from the profile
- Customize attribute mappings
- Perform data transformations within inbound/outbound flows
About Profile Sources

• The Okta user profile is associated with a single source of truth

• Profile Source priority determines the source of truth when a user is assigned to multiple sourcing entities

<table>
<thead>
<tr>
<th>Profile Source</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP DC=oktaice,DC=local</td>
<td>1</td>
</tr>
<tr>
<td>Active Directory oktaice.local</td>
<td>2</td>
</tr>
<tr>
<td>BambooHR</td>
<td>3</td>
</tr>
</tbody>
</table>
Sync Attributes

Profile & Lifecycle Sourcing

- Allow Active Directory to source Okta users

Enabling this setting allows Active Directory to control the profiles of assigned users and makes these profiles read only in Okta. Profiles are managed based on profile source priority.

Update User Attributes

Okta updates a user's attributes in Salesforce.com when the app is assigned. Future attribute changes made to the Okta user profile will automatically overwrite the corresponding attribute value in Salesforce.com.
Manage Profile Attributes

*Click here to watch the Demo Video.*

This demo covers the following topics:

- Review Profile Editor
- Map Okta Attributes from Org1 or Org2
- Verify Updated Attributes in Org2
Where Are We?

- Define Your Users in Okta
- Manage Users using Groups
- Configure SSO & Provisioning
- Manage User Profiles in Universal Directory
- **Implement the Okta Policy Framework**
- Offboarding
Implement the Okta Policy Framework
Module Story
Implement the Okta Policy Framework

Why?

Does your organization need stronger authentication beyond passwords?

Is there a way to step up authentication based on security risk without imposing additional authentication burdens to users?

Objectives

• Explain how security policies are enforced in Okta

• Given security requirements, create and apply the appropriate security policy in your environment

• Configure MFA to implement adaptive and stronger authentication
About Policies

• Policies help you manage access to your applications and APIs.
• Policies are evaluated when an access request is made.
• A policy contains a set of rules which define permissions that determine whether the request is allowed or denied.
• Policies are group-scoped and rules are context-scoped.
• Different policy types share a common framework but have different policy settings and rule data.
## Policy Types

<table>
<thead>
<tr>
<th>Type</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Governs password complexity and age, account lockout, and self-service recovery options.</td>
</tr>
<tr>
<td>Multifactor</td>
<td>Controls when, where and which factors may be used for enrollment.</td>
</tr>
<tr>
<td>Okta Sign-On</td>
<td>Determines who can sign in and how a user is allowed to sign into Okta, including control of MFA enforcement.</td>
</tr>
<tr>
<td>Application Sign-On</td>
<td>Determines the extra levels of authentication that you can add before an application can be accessed, also includes control of MFA enforcement.</td>
</tr>
</tbody>
</table>
How Are Policies Evaluated?

• Policies are evaluated top down
  – The first policy to have its criteria met is the one applied
  – Subsequent policies are ignored

• Primarily based on group membership
  – A policy can be associated with one or multiple groups.

• In general, the most restrictive policy should be ordered to evaluate first.
Policy Application – Single Group

1. Finance
2. HR
3. Sales
4. Everyone Group

Sales
Policy Application – Single Group

1. Finance (Not Applied)
2. HR (Not Applied)
3. Sales (Executed)
4. Everyone Group (Not Evaluated)
Policy Application – Multiple Groups

1. Finance
2. HR
3. Sales
4. Everyone Group
Policy Application – Multiple Groups

1. Finance (Executed)
2. HR (Not Evaluated)
3. Sales (Not Evaluated)
4. Everyone Group (Not Evaluated)
Policy Rules

• Like policies, rules are evaluated top down

• Based on context, primarily client IP address
  – Can be in or not in a zone

• In general, the rules with the narrowest criteria should be ordered to evaluate first.

• A policy with no rules cannot be applied.
About Network Zones

Network Zones define security perimeters that help safeguard your private network.

**IP Zones:** Typically define corporate network boundaries

**Dynamic Zones:** Define one or many countries and/or regions within

110.68.45.67 – 110.68.45.77
Set Up Zones

Click here to watch the Demo Video.

This demo covers the following topic:

• Define IP Zone
Set Up MFA Enrollment Policies
Multifactor Authentication: An Overview
Multifactor Enrollment Setup

1. Select the factors
2. Factor enrollment
Selecting Factor Types

Soft-Based Token

Third-party Vendor

Phone-Based Token

Question and Email
Creating Enrollment Policies

Set conditions that determine when/where to enroll the factors

Assign to groups

Select how the factors are to be applied

Note: To configure multifactor policies, you must first enable at least one MFA factor.
Set Up Multifactor Enrollment

*Click here to watch the Demo Video.*

This demo covers the following topics:

- Select Enrollment Factors
- Create an MFA Enrollment Policy
- Enroll the Factors
How Does Okta Evaluate an Okta Sign-on Policy?

1. User enter credentials
2. Verify username first
3. Check group membership
4. Evaluate contextual conditions
5. Prompt MFA?
   - Y: Accepted?
     - Y: Okta Org (session)
     - N: Denied
   - N: Denied
6. Validate password
   - Denied
   - Allowed
The Default Policy defines everyone can access Okta from anywhere without MFA.
Set Up an Okta Sign-On Policy

*Click [here](#) to watch the Demo Video.*

This demo covers the following topics:

- Create an Okta Sign-on Policy
- Sign in Okta with MFA
Where Are We?

• Define Your Users in Okta
• Manage Users using Groups
• Configure SSO & Provisioning
• Manage User Profiles in Universal Directory
• Implement the Okta Policy Framework
• Offboarding
Offboarding
Deprovisioning

Ensure that people who are no longer with your organization do not have access to sensitive or licensed applications.
Offboarding

Click here to watch the Demo Video.

This demo covers the following topics:

• Deactivate User

• Verify Deprovisioning in Service Provider
You should now be able to:

• Log into the Okta org as an Okta administrator
• Create and manage user accounts in Okta
• Create groups and populate members with group rules
• Configure SAML authentication for application SSO
• Provision users to integrated applications
• Create, sync and map user profile attributes using Universal Directory
• Implement MFA to improve your organization's security posture
• Deactivate/deprovision identities in Okta