Identity & Access Management (IAM) Project Report 1

Sep 2023 – Aug 2025

Prepared by: Vinay Kumar

# Table of Contents

1. Introduction

2. Skills Demonstrated

3. Project Reports

3.1 SSO Setup (SAML/OIDC)

3.2 MFA Configuration

3.3 Access Policies

3.4 App Integration

4. Project Timeline

5. Conclusion

# 1. Introduction

This report documents Identity & Access Management (IAM) projects completed between September 2023 and August 2025. The work demonstrates expertise in Okta Workforce Identity, Microsoft Active Directory integration, Single Sign-On (SSO), Multi-Factor Authentication (MFA), Lifecycle Management, and automation using Okta APIs.

# 2. Skills Demonstrated

- Okta Workforce Identity & Universal Directory

- Single Sign-On (SSO) with SAML/OIDC

- Multi-Factor Authentication (MFA) configuration

- Role-based access and conditional policies

- Security best practices in IAM

# 3. Project Reports

## SSO Setup (SAML/OIDC)

Objective: Configure Okta as Identity Provider (IdP) and enable SAML/OIDC based authentication.

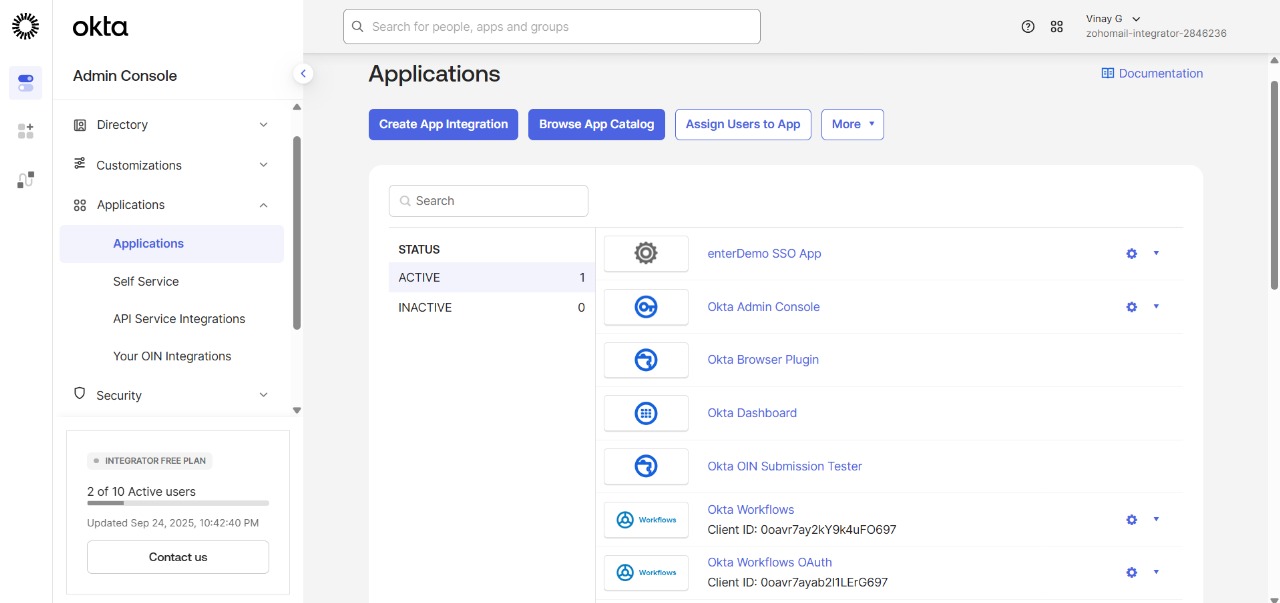
Steps Implemented:

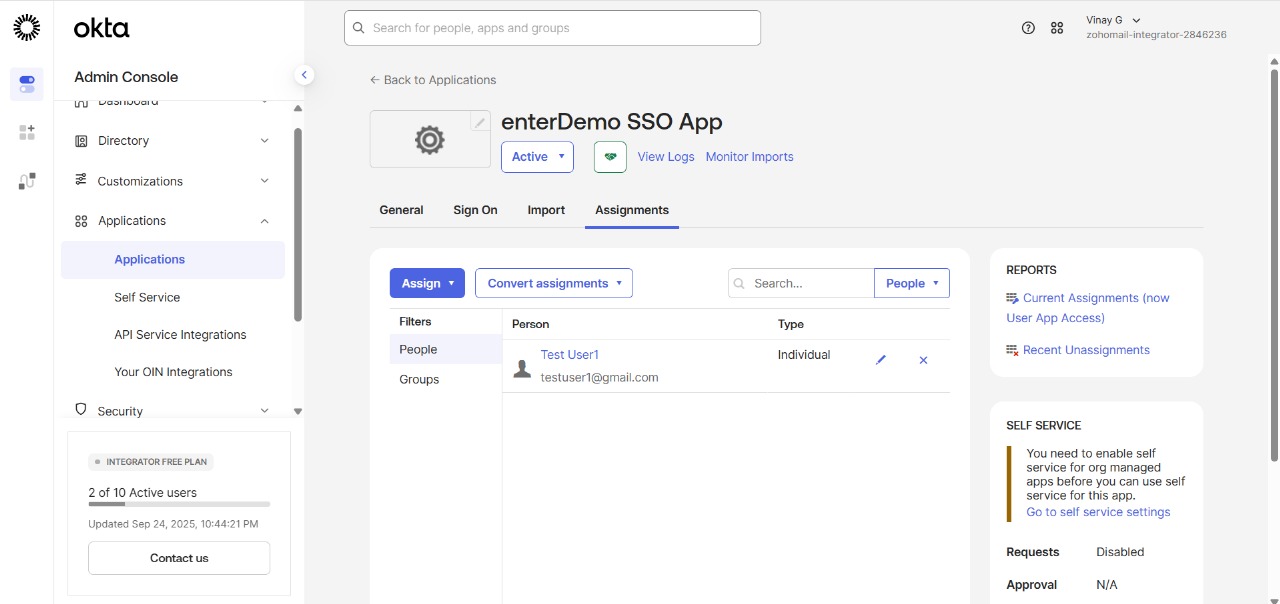
- Configured test application with SAML integration.

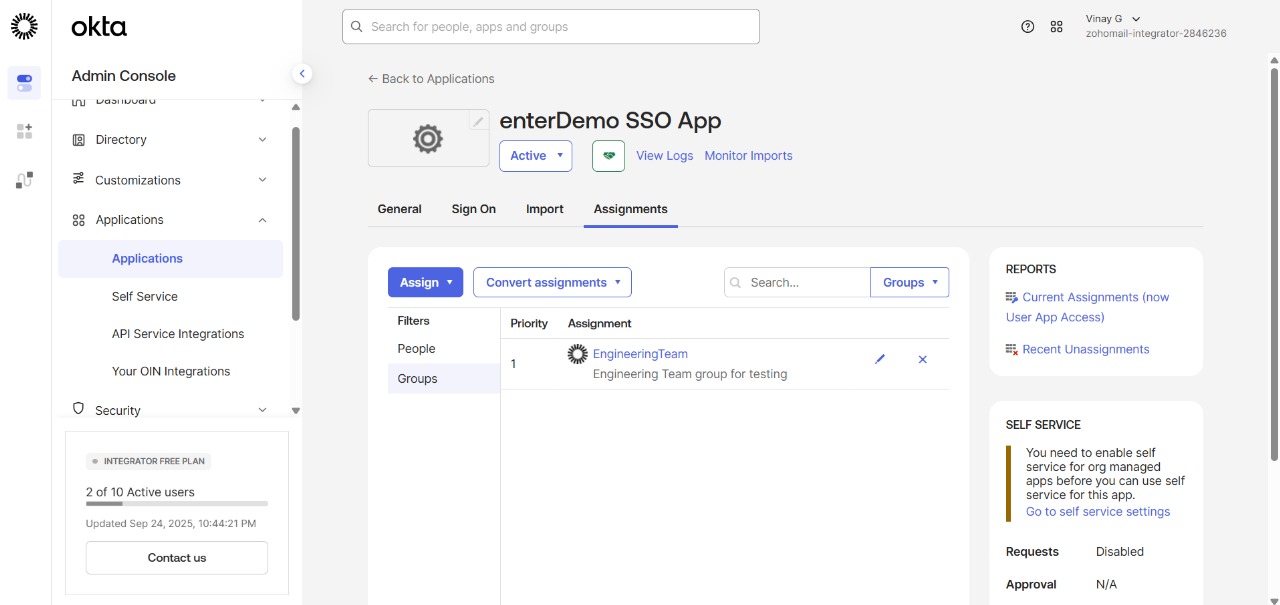
- Verified IdP-initiated and SP-initiated login flows.

- Tested session handling and logout flows.

Outcome: Successful login/logout with secure session management.







## MFA Configuration

Objective: Enhance authentication with multi-factor security.

Steps Implemented:

- Enabled MFA using Okta Verify, SMS, and Email factors.

- Applied adaptive policies based on risk context.

- Enforced MFA during high-risk logins.

Outcome: Improved security through multiple authentication layers.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

## Access Policies

Objective: Implement contextual and role-based access policies.

Steps Implemented:

- Defined conditional access rules based on device and location.

- Applied role-based session policies.

Outcome: Controlled access and reduced unauthorized logins.

## App Integration

Objective: Integrate enterprise applications using SAML and OIDC.

Steps Implemented:

- Configured enterprise SaaS apps with Okta as IdP.

- Verified OIDC flows with sample applications.

Outcome: Simplified secure access to enterprise apps.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.



# 4. Project Timeline

**Project Timeline (Report 1: SSO, MFA, Access Policies, App Integration)**

* **Sep 2023 – Dec 2023**
  + Setup Okta environment and initial configurations.
  + Implemented **SSO (SAML/OIDC)** with test applications.
  + Validated login/logout flows.
* **Jan 2024 – Jun 2024**
  + Rolled out **MFA configuration** (Okta Verify, SMS, Email).
  + Enforced adaptive MFA policies for critical apps.
* **Jul 2024 – Dec 2024**
  + Designed and applied **Access Policies** (conditional, per-app).
  + Tested with different user groups and network zones.
* **Jan 2025 – Apr 2025**
  + Integrated **enterprise SaaS apps** (SAML/OIDC).
  + Verified provisioning flows (manual).
* **May 2025 – Aug 2025**
  + Completed **App Integration enhancements**.
  + Optimized session policies, signing certificates, and MFA rules.

# 5. Conclusion

This two-year project portfolio demonstrates end-to-end experience in Identity & Access Management using Okta Workforce Identity and Microsoft Active Directory. The hands-on work spans SSO, MFA, Lifecycle Management, App Integration, and API automation, preparing for enterprise-level IAM roles.