Rahul Thakur

2702930765
rahulsthakur55@gmail.com

Summary

- Over 5 years of IT experience in Identity Access Management (IAM, OKTA Administrator and Business Analyst.
- Having 3+ years of experience in **Identity and Access Management implementation**, **Administration & Support**.
- Proficient in **IDAM** tool **OKTA**.
- Have an extensive experience in **SSO** using **OKTA**.
- Experience on setting up **SAML** applications in **OKTA** Installing AD on member domains, validating **Single sign-on** user provisioning and troubleshooting **password synchronization** across multiple OKTA platforms.
- Proficient in provisioning and de-provisioning users to various applications in OKTA.
- Experienced in integrating **OKTA** with **Active Directory** using **OKTA AD Agent.**
- Expertise in **User life cycle management** and implementation of various workflows design with different Application Resources.
- Experienced in provisioning users using **OKTA CSV Import.**
- Hands on experience on making changes to user profile in AD and OKTA.
- Experience in building custom **Rules, Policies, Provisioning** in IAM.
- Proficient on mastering and syncing users and groups from **Active Directory**, **LDAP**, **Salesforce**.
- Experience in using **SAML**, **WS-Fed** to implement **SSO** to external **web applications** in OKTA.
- Have a good understanding of Federation protocols like **SAML, WS-FED.**
- Good understanding on **OAuth 0** and **OpenID Connect**.
- Implemented the **Single Sign On**, **Identity and Access Management** solution **OKTA** – Salesforce, Facebook, Zendesk, Office 365, Zoom, Box, Workday, Concur, Tableau, and JIRA.
- Implementing self-service password capabilities enterprise wide in **OKTA Multi-factor Authentication**.
- Experience with API, setting up OKTA API tokens using POSTMAN application.
- Experienced in day-to-day operational support in adding and deleting accounts, applying policies, synchronizing failed accounts, Password rotations.
- Experience in Configuring **Multi-Factor Authentication**.
- Configuration of **SSO** for **SaaS** and **on premise** applications using **OKTA cloud.**
- Configure external **Directories, Groups, and Rules**.
- Configure Users to admin Specific Roles.
- Configure custom Application integration for SSO.
- Configure authentication, authorization and password policies.
- Monitor User, Application, Active Directory Logs in OKTA.
- Life cycle management of User’s Profile after creation.
- Configure incremental scheduler for auto import and synchronize user’s profile by running full and incremental scheduler.
- Managing Access control of user’s profile on OKTA Integrated Application.
- MFA enablement and configuration for All/customized user list.
- Network IP Subnet white listing/blocking to access OKTA integrated application.
- Troubleshooting with users for access related issues like not being able to login in OKTA, User’s profile integration in OKTA, password policies, MFA policies, Allow/Deny access on application policies.
- Coordinate with HRMS team on the User profile issues.
- Good understanding on SOX, SOC2 Compliance.

- Elegant Communication, Documentation, Strong organizational and multi-tasking skills.
- Self-motivated, innovative, Dedication, and ability to adapt and learn new concepts and technologies.

Skills

IDAM Tools - OKTA
Identity and Access Management - MFA configuration, RBAC, Integration of SAML, OAuth, OpenID based application in OKTA, Network IP whitelisting/blocking in OKTA, Strong Auth
Directory Services - LDAP, Active Directory, Oracle Unified Directory
IDE - Eclipse
Database - MySql, Oracle
MS Office Tools - MS Word, Excel, PowerPoint, Visio, SharePoint

Professional Details

VENNBIO
OKTA Administrator, Aug'21 to present

- Integrate applications to OKTA using SAML 2.0 & OAuth.
- Configured SAML 0 connectors for various applications to enable SSO.
- Enabled OKTA Single sign-on (SSO for user authentication and authorization that permits a user to use one set of login credentials (name and password) to access multiple applications.
- Implemented Adaptive multi factor authentication security for all the applications adaptive MFA is the easy way to secure the users data.
- Integrated OKTA SSO to 20+ applications along with enabling MFA at OKTA tenant & application level.
- Worked on Authentication API to provide services like multi-factor enrollment and verification, recover forgotten passwords, and unlock accounts, verify the username and password credentials.
- Used JIT Provisioning and hourly synch process import to OKTA from Active Directory and LDAP One place to manage all the users, groups and devices, mastered in OKTA or from any number of sources.
- Implemented OKTA Group rules and birthright provisioning of users into downstream applications.
- Install and upgrade OKTA agents in production and lower environments.
- Integrated OKTA with the company's AD domain to import, confirm and activate users.
- Involved in creating, updating, adding resources and lock, unlock, enable, disable, and delete the user accounts.
- Managing user provisioning to Microsoft Active directory.
- Password synchronization between OKTA and AD.
- Configuring and managing provisioning to multiple domains in Active Directory.
- Implemented Custom Workflows as per client requirement.
- Designing of Role based provisioning policies as per Role/Access matrix of the organization.
- Generating New Users using OKTA CSV Import feature for Provisioning of new users.
- Monitored application usage and analyzed authentication errors using system logs and reports.
- Supporting implementation for cloud applications such as Office 365, Tableau, JIRA, Facebook, Tableau, Workday, G suite, Salesforce, Zendesk, Box,Dropbox.
- Worked with firewall team to configure IP zones for internal & external networks.
- Implemented various forms of MFA.
- Troubleshoot SSO issues using Fiddler and SAML Tracer Chrome Panel.
- Create technical documentation for users and L2 support team.
- Maintaining Active Directory groups and users, configure push groups from OKTA to Active Directory.

SIGNIFY HEALTH

IAM Business Analyst, May'19 to Jul'21

- Gather business and technical requirements from stakeholders.
- Develop and document policies, procedures, standards, and guidelines related to identity and access management.
- Experience in SSO, multi-factor authentication, SAML.
- Experience in enterprise directory services integrations (Active Directory, LDAP, WS-Federation, SAML).
- Perform detailed business analysis across multiple platforms and applications.
- Experience in IAM services and concepts (authentication, authorization, provisioning, identity lifecycle management, etc).
- Assisted business users regarding OKTA product and integration with 3rd party apps.
- Created knowledge-based articles, sub-task stories, business requirement and standard operating procedure documents using Confluence, Word, Jira and Service Now applications.
- Experience with IAM, directory services, Active Directory, LDAP, Role-based access, and user permissions.
- Provided assistance with continuous documentation improvement.
- Assisted customers and performed assessments in defining more streamlined process for existing IAM solutions.
- Ensure that only authorized users have access to critical IT resources.
- Interface with business clients, integration, operations teams to define requirements, deliverables, and provide the necessary expertise and support to ensure delivery.
- Manage schedules and plans to ensure timely completion of project deadlines and actively participate in decision making and other project management activities.
- Provided necessary training to team members on IAM related tools and processes Continuously expand knowledge of security related tools, processes and procedures.

APP DYNAMICS
IAM Business Analyst, Jun'17 to May'19

- Implemented Single Sign On (SSO) that uses Service Provider initiated and Identity Provider initiated SSO.
- Web Gates protect resources on Oracle HTTP Server (OHS) and authentication was provided by OAM.
- Installed and configured Access Manager Policy agents and crafted policy rules to govern service access Policy Agent deployment.
- Contributed to implementation, deployment and administration of Identity and Access Management (IAM) solutions, including user provisioning, role-based access control, authentication, and authorization.
- Coordinated with Business Partners and Information Technology Application Groups to define Business Roles and Technical Roles and assisted in integrating these requirements into IAM solution.
- Performed analysis of application data from HR systems, Active Directory domains and SOX applications to be integrated with IAM tool to identify required manipulation of use data into IAM solution.
- Provided Data Modification support to the implementation team during and post Go Live of each project phase.
- Collaborated with the QA team to create Use Cases and Test Cases for User Acceptance testing.
- Collaborated with the Project Manager and Communication Analyst to create Training Plans and Materials.