[English Only] SSO Authentication Engineer (Single Sign-On)

WFH Available, Good Work-Life balance

Job Information

Recruiter
Skillhouse Staffing Solutions K.K.

Job ID
1564054

Industry
Insurance

Company Type
Large Company (more than 300 employees) - International Company

Non-Japanese Ratio
About half Japanese

Job Type
Permanent Full-time

Location
Tokyo - 23 Wards

Salary
Negotiable, based on experience ~ 11 million yen

Work Hours
9:00 - 18:00 (Mon-Fri)

Holidays
Saturday, Sunday, National Holidays, Paid Holidays

Refreshed
November 18th, 2025 11:02

General Requirements

Minimum Experience Level
Over 3 years

Career Level
Mid Career

Minimum English Level
Business Level

Minimum Japanese Level
None

Minimum Education Level
High-School

Visa Status
Permission to work in Japan required

Job Description

A global and one of the world's largest Insurance Service provide is looking for a Sing-Sign-On (SSO) Engineer.

Responsibilities:

- Implement and support enterprise access management solutions, including authentication, authorization, and single sign-on (SSO) mechanisms.
- Collaborate with cross-functional teams to design and implement solutions with existing systems and applications, ensuring seamless access for users while maintaining security controls.
- Conduct regular security assessments and audits of services to identify and remediate vulnerabilities, ensuring data confidentiality, integrity, and availability.
- Stay updated on emerging technologies and industry trends in identity management, evaluating their potential impact and relevance to the organization.
- Provide technical guidance and support to teams on issues, troubleshooting and resolving complex problems as needed.
- Participate in incident response and Security incident management activities, assisting in the investigation and driving resolution and root cause.
- Create and maintain configurations, processes, and procedures to effectively transfer and maintain knowledge within the organization and supporting solutions throughout their lifecycle.
- Provide quality customer service through excellent communication, feedback, and follow-through.
- Drives resolution of complex problems and recommends capacity, performance improvements and cost savings where feasible.
- Facilitates understanding and agreements among multiple stakeholders to resolve system and applications interfaces and interoperability concerns
- Serves as an escalation point as needed during critical and/or high impact issues

Why should you apply:
- Long term work opportunity, plus WFH available
- Great team dynamics and learning opportunity
- Opportunities to learn/brush-up English/Japanese language

Company Details:
A US based world's leading insurance providers, offering a broad range of life, health, and retirement solutions to individuals, families, and businesses. The company is heavily invested in digital transformation, utilizing advanced technologies like cloud computing, data analytics, AI, and cybersecurity to enhance customer experience and streamline operations. As part of its values, it has a strong focus on creating a diverse environment, and in particular on the appointment of women in high-level position.

Services/Benefits: Transportation expenses up to 20,000 yen per month, plus Paid leave, plus social insurance (health insurance, welfare pension, and work-related accident insurance), Periodic health examination, and Employment insurance

Required Skills

- Bachelor's degree in Computer Science, Software Engineering, Computer Engineering, or equivalent experience
- Proficiency in protocols like JSON web token, SAML, OIDC (OpenID Connect) and others
- 3+ years of experience in implementing and supporting authentication and authorization processes using a variety of technologies such as Ping Identity PingFederate, PingID, PingOne Protect, Microsoft Active Directory, - and Azure Active Directory/Entra ID
- Extensive knowledge of authentication, authorization, and related protocols such as SAML 2.0, OAuth 2.0, OpenID Connect, LDAP (Lightweight Directory Access Protocol), Kerberos, RADIUS (Remote Authentication Dial-In User Service), SCIM (System for Cross-domain Identity Management), FIDO2
- Working knowledge of directory services products such as Microsoft Active Directory, Azure Active Directory/Entra ID, Google Workspace Directory, Amazon Cognito
- Familiarity with scripting languages such as Python, PowerShell, etc. and Infrastructure as Code frameworks such as Terraform and CloudFormation

Company Description