Okta ICAM Engineer

Concept Plus is a mission-focused technology solutions provider that transforms IT concepts into impactful solutions for federal agencies. Headquartered in Fairfax, VA, we bring the agility, responsiveness, and customer intimacy of a small business combined with the quality and infrastructure of a larger firm.

Recognized as an award-winning Oracle partner, we have delivered innovative solutions across Defense, Intelligence, Civilian, Health IT, and Tribal sectors. Our highly certified experts build systems that drive efficiency, accelerate modernization, and ensure mission outcomes with certainty.

We offer competitive pay, comprehensive health, dental, and vision insurance, paid life insurance, paid time off, 11 paid holidays, performance bonuses, tuition reimbursement, unlimited training, and the opportunity to thrive in a collaborative, flexible, and innovative environment.

For more information, visit www.conceptplus.com.

About the role

Concept Plus is seeking an Okta ICAM Engineer to support client ICAM modernization initiatives. This role focuses on integrating and optimizing identity solutions within environments that utilize client credentials, federation services, and Zero Trust architecture aligned with federal standards, including NIST SP 800 63, OMB ICAM guidelines, and client identity directives.

What you'll do

- Design, implement, and maintain ICAM solutions using Okta Identity Cloud in support of federal identity requirements, including Workforce Identity, SSO, MFA, and adaptive authentication.
- Integrate Okta with client credential systems, including certificate-based authentication, PKI validation, and federation with government identity providers.
- Configure and support identity federation using SAML, OIDC, and OAuth across government applications, platforms, and on-prem enterprise systems.
- Develop and manage identity lifecycle processes aligned with federal access control policies, RBAC/ABAC models, and authoritative identity sources.
- Implement Zero Trust identity pillars, including strong authentication, device trust, continuous validation, and least-privilege access principles.
- Build automation and identity workflows using Okta Workflows, APIs, and scripting tools to support compliance and operational efficiency.
- Troubleshoot identity-related issues across client authentication flows, PKI chains, SSO integrations, and SCIM provisioning.
- Ensure compliance with NIST 800 63, FICAM architecture standards, DoW IdAM policies, and FedRAMP security controls where required.
- Collaborate closely with cybersecurity, cloud engineering, and system owners to support secure identity integration for mission systems.

- Contribute to ICAM modernization roadmaps, ATO support documentation, and continuous improvements in identity posture..

Required Qualifications

- US Citizen
- 5–8+ years of experience in ICAM/IAM engineering within federal or government environments.
- 3–5+ years of hands-on experience with Okta Identity Cloud (administration, integration, federation).
- Practical experience supporting PIV/CAC-based authentication, PKI trust chains, certificate mapping, and federation with federal IdPs.
- Strong understanding of authentication protocols (SAML, OIDC, OAuth), SCIM provisioning, and directory services (Active Directory, Azure AD).
- Experience with identity policy, RBAC/ABAC, account lifecycle management, and enterprise identity governance.
- Hands-on experience with automation (PowerShell, Python, or Bash).
- Familiarity with Zero Trust identity architecture, especially in federal or DoW environments.
- Excellent documentation, communication, and collaboration skills.

Preferred Qualifications

- Experience supporting ICAM modernization initiatives in federal agencies or DoW environments.
- Okta Professional or Consultant Certification.
- Familiarity with NIST SP 800 63, NIST CSF, OMB ICAM guidance, DoW Zero Trust Strategy, and FedRAMP controls.
- Experience integrating identity services with Azure Government, or on-prem mission systems.

Concept Plus is an Equal Opportunity Employer. As such, we will give your application full consideration without regard to your race, color, religion, sex, age, national origin, disability, veteran status, sexual orientation, gender identity, or any other classification protected by federal, state, or local law.