

# Case Study

Streamlining IT Operations and Security with Okta

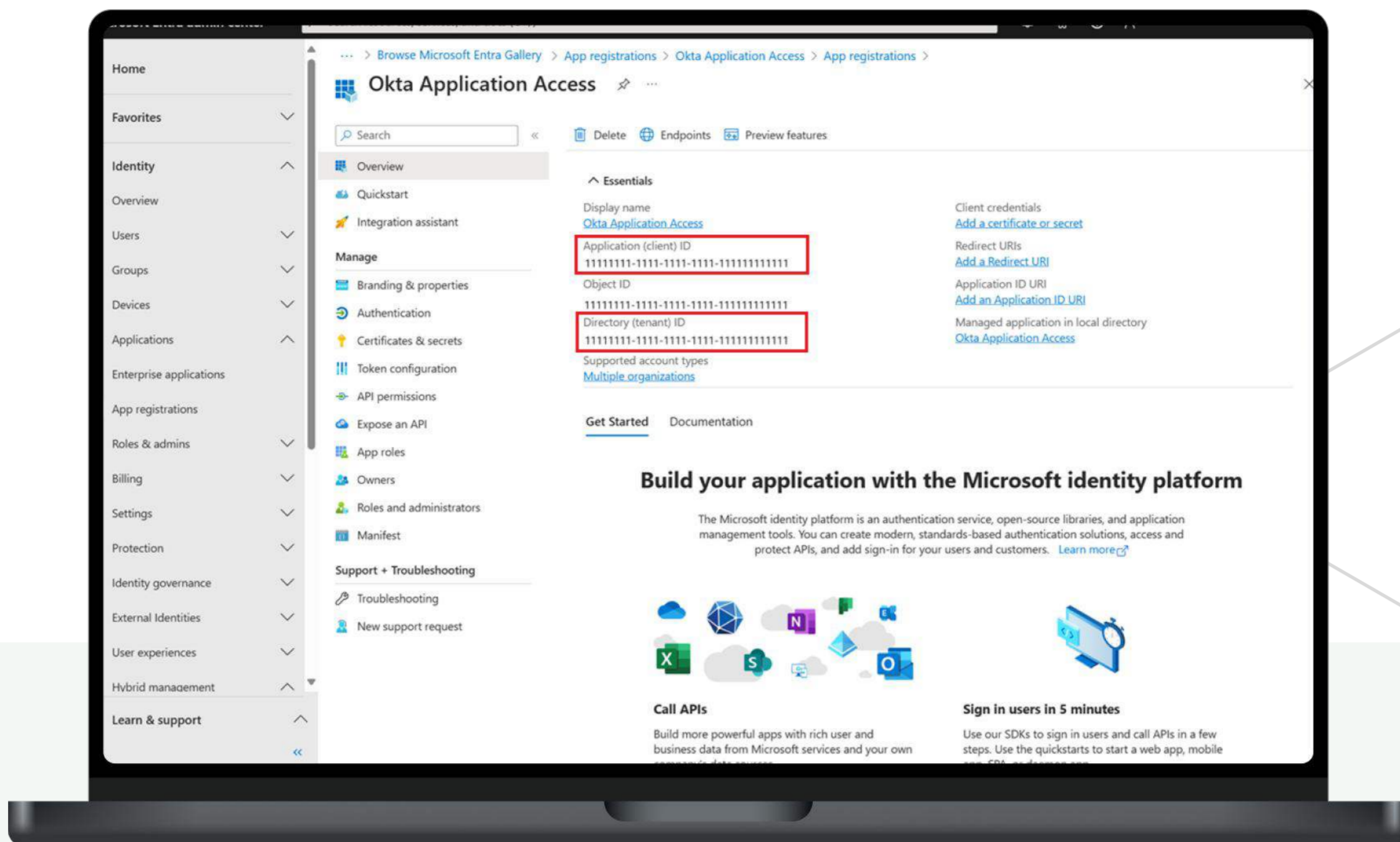


## The Customer

And Their Challenge

The State of Georgia faced a daunting challenge in managing its extensive network of over **70,000 users** dispersed across various departments and locations. With the recent implementation of **Okta**, an identity management and authentication platform, the State aimed to **streamline its IT operations and enhance security**. However, the transition presented numerous hurdles, including long lead times for user account creation and support requests.

The existing **Okta integration struggled to keep pace with the State's dynamic environment, leading to delays and inefficiencies in user management and application access**. Recognizing the need for expert assistance, the State of Georgia turned to i3solutions for a comprehensive solution to augment its IT capabilities and optimize its Okta environment.



## The Solution

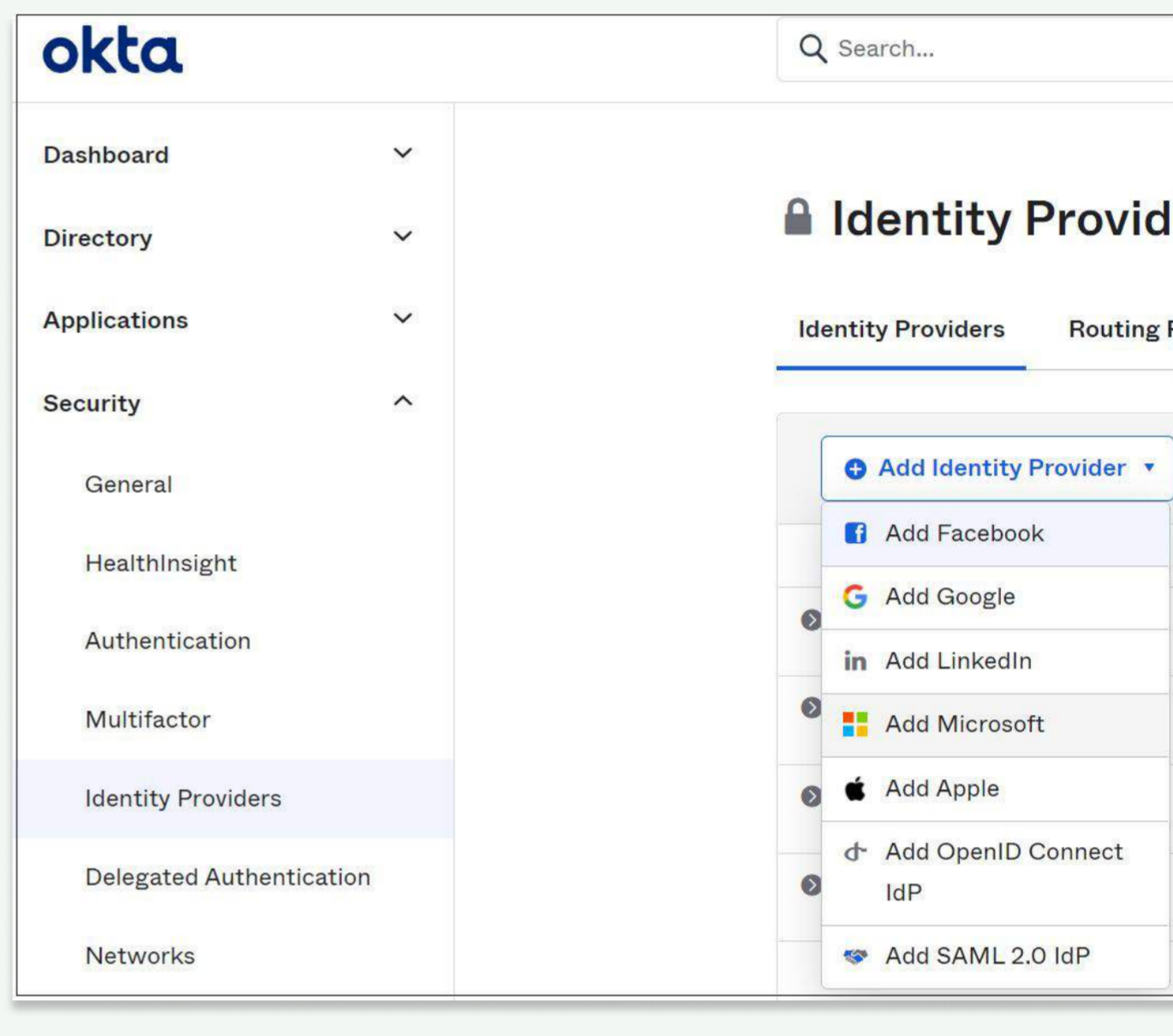
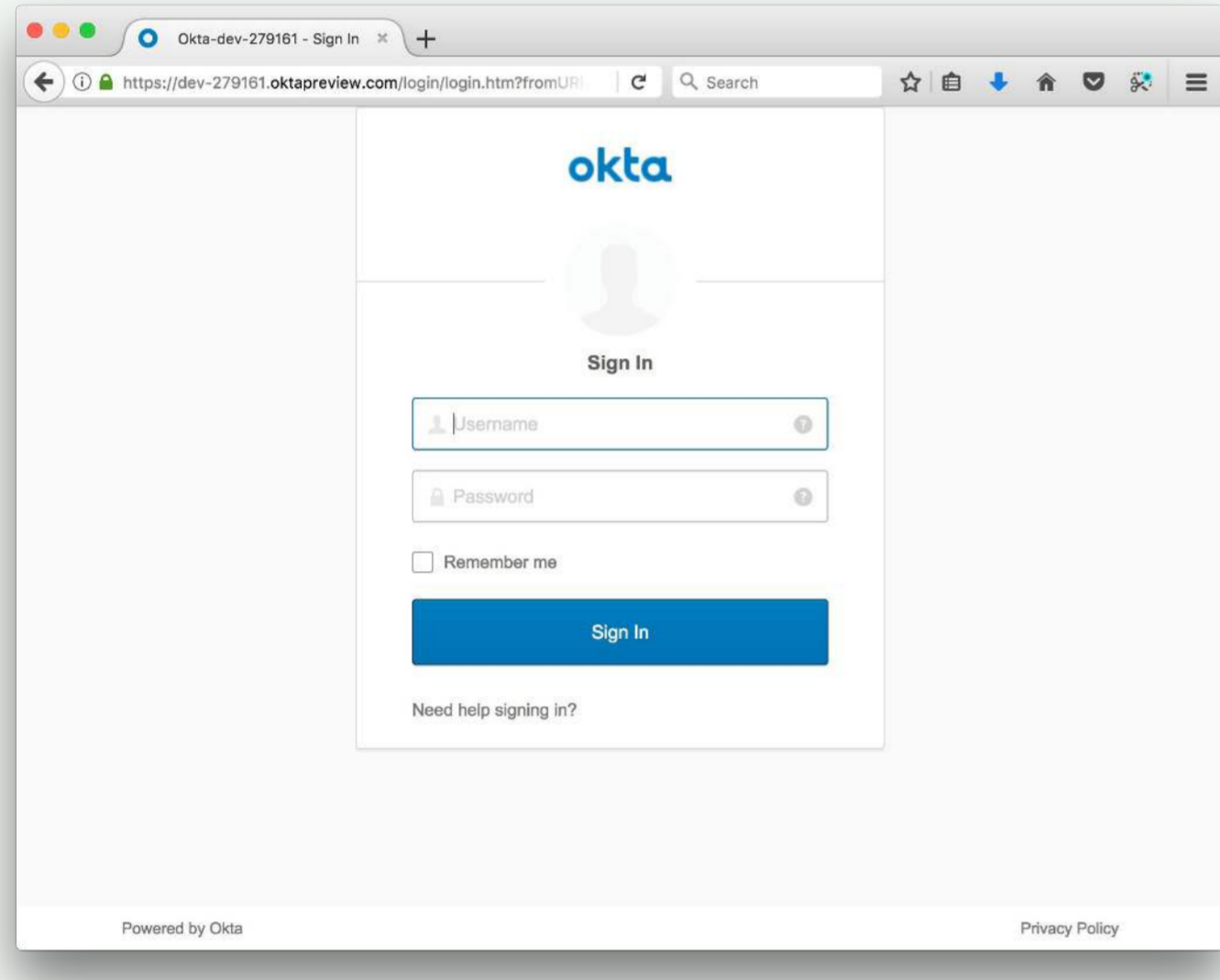
Okta Integration and Optimization

**i3solutions** embarked on a mission to overhaul the State of Georgia's Okta environment, leveraging its expertise in identity management and IT operations to address the organization's pressing needs. The scope of the project encompassed the design, implementation, and maintenance of a robust **Okta** architecture capable of supporting the State's vast user base and diverse application landscape. Drawing upon industry best practices and client requirements, **i3solutions devised a tailored approach to streamline user provisioning, authentication, and access control processes, while bolstering security and compliance measures**.

i3solutions embarked on this task with a focus on scalability, reliability, performance and security.

i3solutions designed the architecture to be flexible and easily scalable, ensuring that it could adapt to the evolving needs of the State without compromising performance or security. Given the importance of the Okta environment in facilitating secure access to critical resources and applications, i3solutions implemented robust configurations to minimize the risk of downtime and ensure continuous availability. **i3solutions carefully optimized the architecture to maximize efficiency and responsiveness, leveraging best practices and performance tuning techniques to deliver a seamless user experience.**

Designing and maintaining the architecture of the State's Okta environment was a multifaceted approach that demanded meticulous attention to detail and a comprehensive understanding of the State's unique requirements.



To facilitate a secure environment, **i3solutions configured multifactor authentication (MFA) options such as Okta Push, RSA tokens, and voice authentication**. These MFA options were applied to different departments based on Okta Groups, ensuring appropriate security measures across the organization. To bolster security further, i3solutions implemented do-not-allow lists based on country IPs. This proactive measure aimed to enhance security by preventing unauthorized access attempts originating from specific regions.

Lastly, **i3solutions played a crucial role in handling day-to-day Okta help desk tickets, providing timely support and resolution to user queries and issues**. This ensured uninterrupted access to vital resources, maintained user productivity, and fostered trust and confidence in the Okta environment among State employees.

Another significant aspect of the solution was the integration of third-party applications into Okta's authentication services to provide a single sign-on experience for users. i3solutions utilized various methods, including the Okta Integrated Network and manual integration, to seamlessly incorporate over 30 applications into the authentication framework, ensuring compatibility with the State's diverse software ecosystem and enhancing overall efficiency and user experience.

i3solutions' comprehensive solution empowered the State of Georgia to harness the full potential of its Okta environment, driving efficiency, security, and innovation across its IT ecosystem. By leveraging advanced technologies and best practices, i3solutions facilitated a seamless transition to a modernized IT infrastructure, positioning the State for sustained success and digital transformation in the years to come.

## Technologies

Used in the Solution



**Okta** is a cloud-based identity and access management (IAM) platform that provides secure access to various applications, data, and services. It provides the foundation for centralized user management, authentication, and access control, enabling the State to streamline its IT operations and enhance security across its extensive user base and application landscape.



Automation played a pivotal role in streamlining administrative tasks and workflows, improving operational efficiency and agility. i3solutions leveraged **Okta Workflow** to automate user onboarding processes, event-based workflows, and routine administrative tasks, reducing manual intervention and accelerating response times to IT requests and incidents.

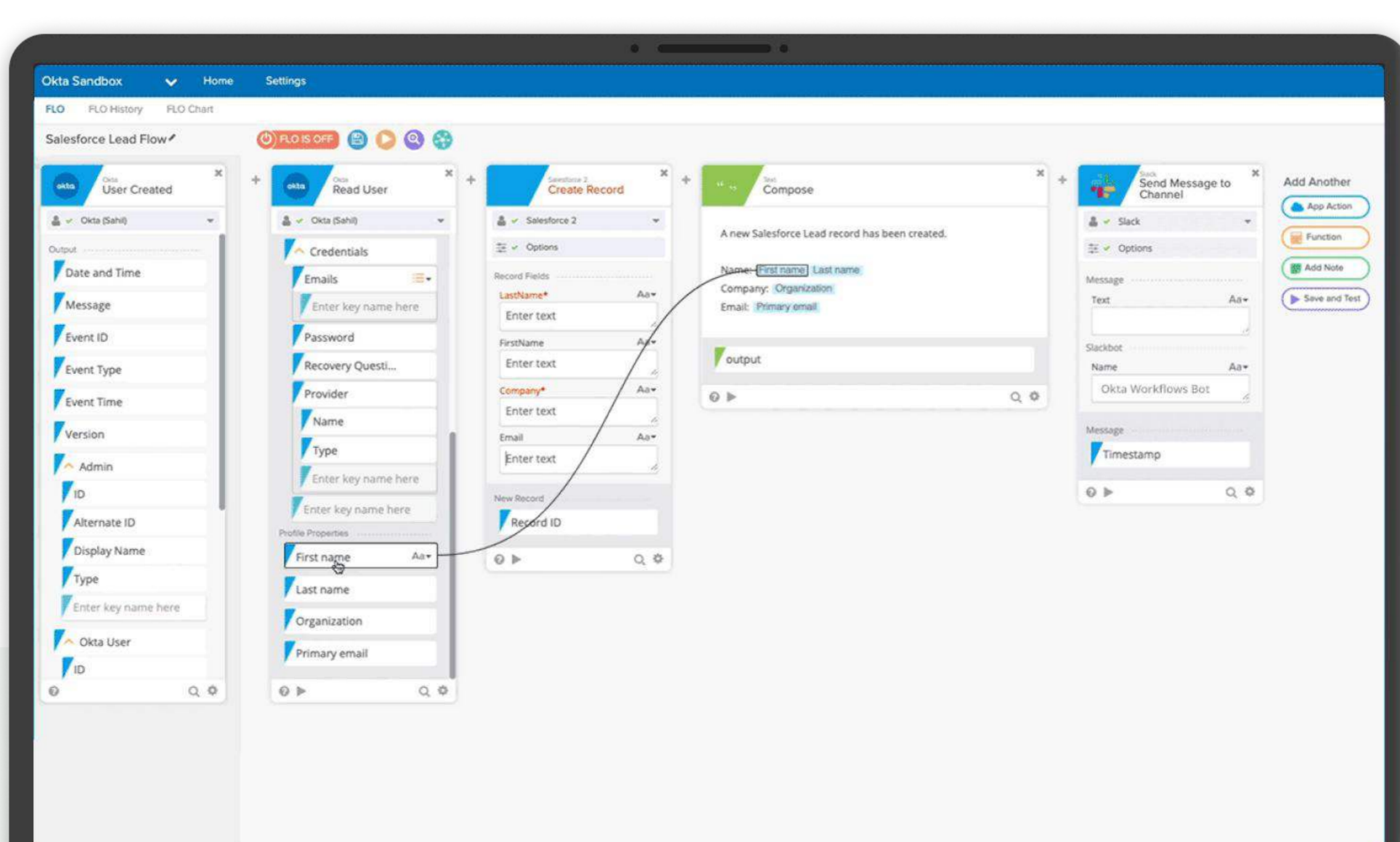


**Entra ID** (formerly Active Directory) is used to manage network resources in a Windows domain environment. Seamless integration with Entra ID facilitates user authentication and synchronization, ensuring consistency and reliability in user management across the State's IT environment. This integration empowers the State to leverage its existing infrastructure while enhancing its identity management capabilities with Okta's advanced features.



**Privileged Identities** refer to user accounts that have the authority to perform sensitive or critical tasks. The implementation of PIM principles ensures that privileged identities are monitored, managed, and audited according to the principles of least privilege. This enhances security posture and compliance, mitigating the risk of unauthorized access and privileged misuse while maintaining operational efficiency and productivity.

By leveraging these advanced technologies and best practices, **i3solutions empowered the State of Georgia to optimize its Okta environment, drive efficiency, and enhance security across its IT ecosystem**. This comprehensive solution laid the foundation for sustained success and digital transformation, enabling the State to adapt, innovate, and thrive in an ever-evolving technological landscape.



## Measurable Benefits and Business Impact



**Streamlined User Provisioning and Authentication Processes**

The implementation of Okta and associated workflows significantly reduced lead times for user account creation and authentication requests. By automating user provisioning processes and streamlining authentication procedures, the State experienced a substantial improvement in user experience and productivity. Employees now gain quicker access to essential systems and applications, leading to enhanced efficiency and operational agility.



**Enhanced Access and Security**

Integration of third-party applications into Okta's authentication services improved application access while bolstering security and compliance measures. With seamless single sign-on (SSO) capabilities and centralized access control, employees can access authorized applications and resources with ease, while robust authentication mechanisms, including multifactor authentication (MFA), mitigate security risks and safeguard sensitive data against unauthorized access and cyber threats.



**Improved IT Responsiveness**

Automation of administrative tasks and workflows using Okta Workflow enhanced IT agility and responsiveness. Routine tasks such as user onboarding, access provisioning, and incident response were automated, reducing manual intervention and accelerating response times to IT requests and incidents. This increased operational efficiency enables IT teams to focus on strategic initiatives and value-added activities, driving innovation and business growth.



**Centralized Reporting, and Alerting**

Okta's built-in capabilities for centralized reporting, analytics, and alerting provide actionable insights and enhanced visibility into IT operations. Custom reports, dashboards, and alerts enable proactive monitoring, analysis, and response to security events, operational issues, and compliance requirements. By leveraging data-driven insights, the State can identify trends, anticipate challenges, and make informed decisions to optimize its IT environment and enhance organizational performance.