

Ensuring authentication keeps pace with rapid investor growth

Learn how [Simplicity](#)—a nonprofit KiwiSaver and investment fund manager—deployed multi-factor authentication and passkeys across web and mobile with Authsignal.

Overview

Simplicity is New Zealand's nonprofit KiwiSaver and investment fund manager, serving hundreds of thousands of members through a fully digital platform. As a regulated financial services provider managing retirement savings for clients, Simplicity has a direct obligation to protect member accounts while keeping the investment experience simple and accessible. However, as membership accelerated and product offerings expanded, legacy authentication systems weren't up to the task of meeting the company's present and future security needs. Critically, at login and during sensitive actions, Simplicity required a robust authentication layer that didn't add friction to the user experience. Authsignal proved to be the cloud-native solution Simplicity needed by delivering a powerful authentication layer for today and tomorrow.

High security expectations meet frictionless user expectations

With a rapidly expanding membership base, Simplicity's legacy authentication system was no longer aligned with the security expectations of a growing financial management platform. As the membership base scaled and the product continued to evolve, the authentication layer needed to keep pace. The team sought to deploy multi-factor authentication and passkeys across the web and native mobile applications to uplift security login and at sensitive action



About Simplicity

Based in Auckland, New Zealand, [Simplicity](#) is the country's low-fee, nonprofit KiwiSaver and Investment Fund manager, is owned by the Simplicity Foundation. Founded to ensure all New Zealanders can lead dignified lives, with choices, Simplicity operates under the belief that money equals choices which equals dignity. Simplicity is a small, lean team backed by experienced volunteers who share a common desire to give back to New Zealand, to make a difference, and to do the right thing.

www.simplicity.kiwi



points (such as fund switches and withdrawal requests) without adding friction that would undermine the straightforward experience members expect. Simplicity also required an authentication partner built on [Amazon Web Services \(AWS\)](#) to maintain a consistent security posture across its infrastructure.

Of course, this is nothing new for Authsignal. Customers consistently face a common structural problem: authentication has become a bottleneck, but the effort required to fix it is disproportionate to the available resources. The financial services industry is under mounting regulatory pressure as standards like National Institute of Standards and Technology (NIST) SP 800-63B-4 have downgraded Short Message Service One-Time Password (SMS OTP) to a restricted authenticator. Meanwhile, regional mandates including Revised Payment Services Directive 2 Strong Customer Authentication (PSD2/SCA) in Europe and the UK, the UAE Central Bank's OTP ban, and Bangko Sentral ng Pilipinas (BSP) Circular No. 1213 in the Philippines are creating hard deadlines.

This means financial services organizations must deploy phishing-resistant authentication methods like passkeys, but existing identity platforms do not support them natively. Building from scratch is an unaffordable six- to twelve-month engineering project. At the same time, account takeover fraud is accelerating with deepfake voice attacks increasing by 680% year on year. For large enterprises processing millions of authentications per month, SMS OTP costs are substantial, upwards of \$350,000 to \$1 million per year for organizations with five million monthly users. These organizations must transition to lower-cost, higher-security methods without disrupting customer experience. The common thread: the authentication layer is no longer fit for current use while costs and risk of replacement are prohibitive.

Authsignal: Delivering a frictionless, modern authentication layer

The core differentiator for the Authsignal solution is its drop-in architecture. Most authentication platforms require an organization to migrate users and re-architect their identity stack, which can take six to twelve months with significant risk. Authsignal layers on top of the existing identity provider so that customers can deploy passkeys, adaptive Multi-Factor Authentication (MFA), and identity authentication in weeks without touching the underlying user directory or session management.



We process millions of events per day across multiple global AWS regions and have never had to think about capacity planning allowing customers to go live in weeks, not months. The global infrastructure and resilience of AWS mean we can focus on solving the authentication problem, not the infrastructure problem."

Justin Soong
Founder and Director
of Product
Authsignal

Further, a no-code rules engine puts authentication in the hands of product, compliance, and fraud teams, not just engineering. Omnichannel verification from a signal platform delivers constant identity verification across web, mobile, call center, and physical touchpoints from one orchestration layer. Last, transparent Monthly Active Users (MAU) pricing gives customers cost-certainty.

Simplicity partnered with Authsignal to add passkeys, biometric authentication, and adaptive MFA on top of its existing [Amazon Cognito](#) identity stack without requiring migration or re-architecture. The Authsignal platform—built entirely on AWS—integrated with Amazon Cognito custom authentication flows using [AWS Lambda](#) for serverless event-driven authentication processing. [Amazon DynamoDB](#) provides low-latency credential and session management. Authsignal's native mobile Software Development Kits (SDKs) for iOS and Android enabled Simplicity to ship passkey and biometric login into their mobile app, giving members a faster and more secure method to access their accounts. The no-code rules engine allowed Simplicity to configure authentication policies for different risk levels across the member journey without engineering dependencies.

As an AWS-native solution, Authsignal benefits from AWS scalability and reliability. Authsignal processes more than 20 million authentication events per month across enterprise customers in financial services, healthcare, aviation, and telecommunications. AWS serverless architecture means the platform scales automatically without Authsignal having to manage servers or perform capacity planning for authentication workloads. When a customer's traffic spikes, the platform scales in near real time without degradation. Operating across multiple AWS regions enables per-tenant data residency, which is a compliance requirement for customers in regulated industries. Further, Authsignal holds ISO 27001:2022 certification and SOC 2 Type 2 compliance, both built on the security controls AWS infrastructure provides.

Simplicity with Authsignal: Frictionless, secure authentication for web and mobile

Simplicity members can now log in using passkeys or biometric authentication across web and mobile, replacing credentials with phishing-resistant methods. The authentication uplift was delivered without disrupting the existing Amazon Cognito identity stack or requiring a rebuild. By choosing an AWS-native authentication partner, Simplicity maintained a unified security posture and avoided introducing additional infrastructure complexity.

Authentication

is built natively on AWS

Passkey or biometric

log on across web and mobile

Legacy credentials

are replaced by phishing-resistant methods

No rebuilding

or impact to existing identity stack

Futureproofed

authentication capabilities

The platform's modular architecture also means Simplicity can continue to adopt new authentication capabilities as their product roadmap evolves, without re-integration. In short, Simplicity with Authsignal is offering its customers a frictionless and significantly safer user experience that meets regulatory hurdles in a manner that is futureproofed as new needs and mandates emerge.

For customers across highly regulated industries, the Authsignal partnership with AWS delivers measurable outcomes across cost reduction, security improvement, and operational efficiency. One customer achieved a 90% reduction in SMS dependency after deploying Authsignal passkey authentication. Several enterprise customers have reported cutting identity program costs by 30%. Another customer realized 30% passkey opt-in within four months of deployment with broader adoption reaching 60% to 70% via optimized prompt engineering. Critically, passkey sign-in achieves a 93% success rate compared to 63% for legacy MFA methods. And average passkey login takes 8.5 seconds compared to 31 seconds for legacy authentication. And authentication handling time has been reduced by 26 seconds per call in contact centers through Authsignal Call Connect capability, which replaces knowledge-based security questions with passkey and biometric verification.

About AWS Partner Authsignal

Auckland, New Zealand, based [Authsignal](https://www.authsignal.com) is a customer authentication and identity verification platform. The company's mission is to make enterprise-grade authentication accessible to every organization without requiring them to rebuild their identity infrastructure. Authsignal provides a drop-in authentication layer that works alongside an organization's existing identity provider. Rather than replacing what a customer already has, Authsignal adds modern capabilities on top: passkeys (FIDO2/WebAuthn), adaptive multi-factor authentication, a no-code rules engine, identity verification, and omnichannel authentication spanning web, mobile, contact center, and physical touchpoints. The company serves mid-market up to enterprise organizations across financial services, airlines, healthcare, telecommunications, and government.

To learn more, visit www.authsignal.com