

Savola Foods powers the engine of its business by adding modern authentication via OneLogin by One Identity

“With OneLogin, we can enable modern security for our legacy on-premises apps and a unified access experience for all users.”
– Mohamad Kerdi, Director of IT Infrastructure and Services

SAVOLA

Location: **Middle East**

Users: **4000**

Website: [savola.com](https://www.savola.com)

Savola Foods, part of the Savola Group, manages a wide range of market-leading food brands in 50 countries. Brands such as Afia, Shams and Italiano are loved by consumers and many are market leaders in multiple countries. From humble origins selling edible oil in its local Saudi market, Savola Foods has grown to be a major regional player. The company has maintained the traditional focus on consumer staples, such as edible oil, sugar, pasta and ghee, but is expanding into new markets and higher-value product categories.

Challenges

To do their jobs, employees across Savola Foods rely on ready access to a suite of business applications. Since these applications contain sensitive financial, HR and strategic planning information – and can be a conduit for security threats entering the corporate environment – the IT team needs to ensure secure, authorized access.

Challenges

- Access to applications hosting sensitive company information wasn't secure
- The suite of legacy applications didn't support modern authentication functionality
- IT had to manually perform commissions and decommissions

Solutions

- OneLogin access management provided cost-effective Multi-Factor Authentication

Results

- Enabled modern access management for legacy apps, including Cisco VPN
- Freed IT from manual provisioning and deprovisioning
- Strengthened VPN security

The team had taken advantage of built-in security features, like single sign-on (SSO) and multifactor authentication (MFA), to secure its modern apps. However, its suite of legacy applications didn't support modern authentication functionality. As a result, IT had to manually commission users, monitor app access and manually decommission users. In addition, users sometimes had access challenges, especially factory workers who were trying to meet delivery deadlines. When COVID-19 hit, these issues were further complicated.

"We needed authentication that could be integrated with our legacy suite to enable all of our workers to do their jobs efficiently," explains Mohamad Kerdi, Director of IT Infrastructure and Services for Savola Foods.

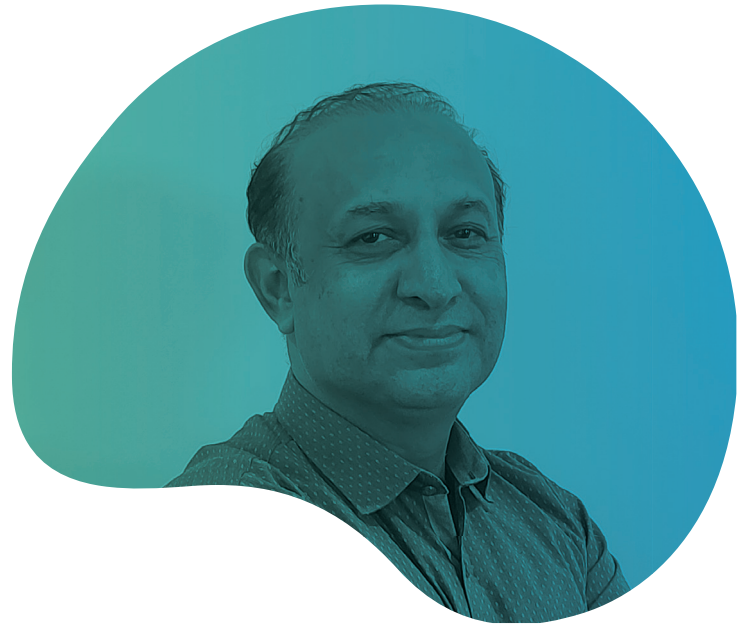
"Though we have embraced a cloud-first strategy, our business suite is decades old. The suite's vendor offers an access solution, but we wanted to go with a modern, state-of-the-art, robust solution and step into the future," continues Naeem Shah, Database and Smart Factory Transformation Senior Manager for Savola Foods.

Solutions

With a goal of incorporating its legacy business suite into its current Identity and Access Management (IAM) processes, the IT team began its search. Initially, it focused on an MFA solution for VPN that tied back to the company's on-premises Active Directory (AD) environments. After evaluating many vendors, the team discovered One Identity and the vendor's OneLogin access management solution, a cloud-managed service that serves as the central point to manage access for on-premises applications.

Not only did OneLogin by One Identity offer a cost-effective solution, Savola Foods appreciated the involvement of One Identity's technical experts. "They were very engaged in helping us figure out the right solution because our app integration is sophisticated," Kerdi said.

After conducting a proof of concept, Savola Foods was confident that OneLogin was the right solution. "It provides MFA out of the box, eliminating the need to subscribe to our suite vendor's separate MFA solution," explains Shah.



OneLogin enables our strategy to streamline access and management.

said Shah

Results

OneLogin is the mechanism that connects Savola Foods' suite of on-premises apps to Active Directory. Through it, users remotely authenticate via MFA using their AD credentials.

When the IT team enforces OneLogin for the first time, workers install OneLogin Protect, a one-time password (OTP) mobile app. SSO is enabled seamlessly between OneLogin and the suite of business applications, regardless of the user's location. That means remote users – even those in the factories without dedicated machines and email addresses – can access business apps to get their work done.

With OneLogin deployed, a single team now manages AD, and IT has eliminated duplicate monitoring efforts. Because OneLogin is integrated with AD, the IT team now uses a single directory to manage all users. At the same time, IT can monitor access through the OneLogin portal.



Kerdi said,

This enables us to continue down the path of enabling a single pane of glass for all our apps.

According to Shah, “Before using OneLogin, we called upon Active Directory for all cloud-based apps and the suite vendor’s directory for its apps. Now we can enforce real-time, smart security across the organization.”

Since enabling SSO and MFA for its suite of legacy business apps, Savola Foods has enabled 600 external users to access the company’s Cisco VPN via OneLogin. Once users are disabled from AD, they are automatically disabled from the VPN or OneLogin. “OneLogin MFA ensures an extra layer of security for our VPN,” says Kerdi.

The current plan includes adding apps from Archer, SAP SuccessFactors and CA Technologies, among others. From a strategic point of view, Savola Foods wants OneLogin to be the hub for all its SSO-based solutions and will gradually move all apps to OneLogin by One Identity.

About One Identity

One Identity delivers unified identity security solutions that help customers strengthen their overall cybersecurity posture and protect the people, applications and data essential to business. Our Unified Identity Security Platform brings together best-in-class Identity Governance and Administration (IGA), Access Management (AM), Privileged Access Management (PAM) and Active Directory Management and Security (ADMS) capabilities to enable organizations to shift from a fragmented to a holistic approach to identity security. One Identity is trusted and proven on a global scale – managing more than 500-million-plus identities for more than 11,000 organizations worldwide. For more information, visit www.oneidentity.com.