ARCON | Single Sign-on

Encryption. Federated Authentication. Authorization.

The seamless employees' access to multiple applications is important for IT efficiency. Nevertheless, the risk stemming from inadequate authentication mechanism can hinder enterprise IT efficiency and result in application misuse or data breach. ARCON | Single sign-on offers centralized management to authenticate and authorize end-users requiring access to business-critical applications.

Table of content

ARCON | Single Sign-on
Ensuring seamless enterprise AM journey with robust ARCON | SSO

The significance of Single sign-on in emerging enterprise IT use-cases

Single sign-on (SSO) has become an increasingly important security authentication tool in the overall Access Management (AM) framework. This transformation arises from the fact the number of business-critical applications are increasing.

Traditionally, Single sign-on served as a secure tool to access on-prem applications. Employees requiring one-time secure administrative access to web applications and on-prem legacy applications didn't have to bother with managing multiple login credentials to access multiple applications.

With just a single set of authentications, Single sign-on made complicated tasks: end-users remembering multiple login credentials to access multiple applications – easy by enabling an end-user to authenticate once and then be automatically authenticated to other target applications.

Nevertheless, the sudden demand for SaaS-based applications by most IT enterprise environments, if not all, has underpinned the urgent need for a Single sign-on tool that can offer seamless access to applications deployed on-cloud. It would be fair to say that Single sign-on is an essential tool to ensure seamless 'Cloud-first' journey.

Additionally, the sudden shift in the IT environment where employees access applications from remote environments has made Single sign-on 'a-must' security authentication tool to reinforce the overall IAM initiatives.

As a result, it is imperative that the SSO technology is compatible with both on-prem and on-cloud applications.

The risk involved in managing a large number of passwords

Several studies show that almost 25% of IT help desk calls from employees (or maybe more for a few organizations) are related to password management. The request could be for a password reset, new password generation for application access, sharing of password for a new privileged user among many more daily IT use-cases. While multiple help desks requests could result in IT inefficiency, managing a large number of passwords is a risky IT approach as well.

In a typical enterprise set-up that includes multiple end-users managing a large number of passwords, a password-based authentication could lead to application misuse or a data breach.

The first and foremost criteria to ensure secure and efficient IT infrastructure is to build seamless Single sign-on controls. For IT, environments that include a large number of applications, an SSO would ensure access to multiple applications using a single set of login credentials.

ARCON | SSO offers centralized management of identities

ARCON | Single sign-on acts as a centralized engine to manage end-user identities. Central management ensures secure access to all the applications from anywhere and anytime.

The solution provides a catalogue of more than 1000+ pre-integrated applications (Business, Cloud, and Web Applications) as well. This makes it easy to enable single sign-on, MFA, and user provisioning on enterprise applications.

ARCON | SSO supports industry standards and protocols for federated authentication

In addition to centralized management of identities, ARCON | SSO securely authenticate with all applications, whether on cloud or on premises, using standard one-time token-based authentication protocols.

So, when an employee (end-user) sends request to access an application, ARCON | SSO authenticates the end-user's identity with several standard identity-based authentication protocols such as 0Auth2.0, OpenID Connect (OIDC) and Security Assertion Markup Language (SAML). This way, the security and risk assessment teams can ensure a certain level of trust on end-users' access as these tools attest authentication and encryption along with authorization of identities.

Resultantly, by deploying ARCON | SSO, an enterprise can tread a balance between administrative efficiency and access control management whilst ensuring seamless end-user (employee) experience.

Directory service integration and provisions

ARCON | SSO solution seamlessly integrates with authentication repositories such as Microsoft Active Directory (AD) and Lightweight Directory Access Protocol (LDAP).

The solution enables to integrate the existing Active Directory for user provisioning and management, including sharing end-user credentials with other integrated on-cloud and on-prem applications. Besides, it allows to integrate existing Lightweight Directory Access Protocol server, enabling end-users to use their LDAP credentials to authenticate without replicating the credentials on the cloud.

Robust features

ARCON | SSO offers:

- Auto Provisioning / de-provisioning of end-users, thus helping to reduce the administrative costs involved in managing a large number of end-users
- Role-based time-bound access control to ensure only authorized employees can access business-critical applications at granular level
- User-friendly interface. ARCON | SSO portal is browser agnostic and can be accessed from various browsers such as Chrome, Firefox, Internet Explorer and many more
- ARCON also offers reliable integration for SSO to all mobile apps and web apps optimized for mobile platform with industry-standard SAML authentication and other modern protocols
- Real-time alert notifications to show successful login, invalid login, application access request
- Customized reporting with preset templates
- A wide-range of password-less authentications methods such as Facial Recognition, Mobile OTP, SMS OTP, Biometric devices, Hardware Token, Email OTP, Voice Biometric

Conclusion

ARCON | SSO Benefits:

- Federated authentication using all modern identity protocols such as Security Assertion Markup Language (SAML), OpenID Connect (OIDC), 0Auth 2.0
- Central management of employees' access to all applications: on-prem and cloud-based applications
- Overall reduction in IT administrative overheads for managing end-users (employees)
- Automated provisioning or de-provisioning of end-users
- Time-bound access on all platforms at granular level

About ARCON

ARCON is a leading enterprise information risk control solution provider, specializing in Privileged Access Management (PAM) and continuous risk assessment solutions. Our mission is to help enterprises identify emerging technology risks and help mitigate them by robust solutions that predict, protect and prevent.

PAM: ARCON | Privileged Access Management (PAM) is a highly effective solution that helps in managing, controlling and monitoring privileged user activities. The solution provides IT security team with a centralized policy framework to authorize privileges based on roles and responsibilities ensuring rule-based restricted access to target systems.

UBA: ARCON | User Behaviour Analytics (UBA) is a highly effective risk predictive & analytics tool built for daily enterprise use cases. It breaks the traditional approach of 'restrictive' access and is capable of crunching large lakes of enterprise data, spot anomalous activity and trigger alerts in real-time.

SCM: ARCON | Security Compliance Management (SCM) allows an enterprise to prioritize security and compliance efforts based on risk level. The tool enables continuous risk assessment for critical technology platforms and ensuring desired compliance levels.

Connect with us