



ZTrust: Single Sign-On

Secure Any App & Any Device on Cloud

ZTrust is your one stop solution for hassle free Identity and Access Management. It provides seamless omnichannel experience to simplify the login experience for your customers, making it quicker, effortless, secure, and more efficient to access your services. Powered by Keycloak, the OOTB Single Sign On (SSO) solution helps safeguard applications all-in-one place and unlocks accesses with just one click.

The product has been developed using an Outside-in approach, placing a strong emphasis on customer perspective and needs. Through years of practical experience and numerous success stories, our product has established a resilient presence in the market.

Simplify the customer experience, without compromising security

Today's customers expect a seamless and consistent experience—regardless of how, when and where they are interacting with your organisation. Providing a single sign-on facility, rather than requiring customers to sign-in across multiple applications and locations, is now essential.

Yet without the right tools and systems in place, facilitating single sign-on functionality can be complex and time-consuming for your IT team. If done poorly, it can also impact the customer experience, expose your organisation to security risks, and affect your data compliance.

This is where a ZTrust Single Sign-On solution (ZTrust) by Prodevans can make all the difference.

Transform how customers interact with your organisation

Powered by Keycloak Community, ZTrust offers a simple, secure and reliable way to deliver a single sign-on experience for your customers—as well as providing peace of mind for your IT team. Customers can move seamlessly through a transaction with your organisation, without needing to

login to other applications, including social media networks such as Github, Facebook, Google and LinkedIn. The login module and all notification emails your customers see, can also feature your organisation's branding, ensuring a professional experience from start to finish.

Keep your customer data safe from cyberattack

As well as incorporating a range of leading security measures, ZTrust features a mechanism to detect brute force attacks — the trial-and-error technique attackers use to discover valid credentials. The solution identifies and blocks attempts to gain unauthorised access. Customised notifications can also be set up to alert system administrators or security teams, when multiple failed login attempts are detected from a single IP address within a certain timeframe.

Whom can we serve?

Our solution can benefit any organization that needs to manage user access to multiple applications and services while improving security and simplifying the login process for its users.

- **Any Organisation with or using multiple applications & services** to streamline their logins and give their customers or employees a superior experience.
- **Government:** Government bodies to manage user access to various applications and portals.
- **Finance:** Finance companies can use SSO for their employees and customers as they often use multiple applications for different purposes.
- **Healthcare:** The healthcare industries can use SSO to simplify login process & improve security.
- **Education:** Schools & universities that use multiple learning tools & portals like learning management systems, student portals etc.
- **Super-apps:** Application having mini apps can simplify and secure their login process
- **Conglomerates:** Large corporates with diverse business units can streamline access to the applications and improve security.

SSO can be implemented in a variety of industries where there is a need for simple and secure user authentication across many systems and apps. SSO can be used by organisations of all sizes and in a variety of industries due to its adaptability and advantages.

Stakeholders we can serve:-

- **Users/Customers:** Hassle free authentication process, eliminating the need to remember multiple credentials for accessing multiple systems. This simplifies logins, saves time and enhances user convenience and productivity.
- **Business Leaders:** Streamlined diverse business units, Increased user productivity, streamlined access management, improved security, reduced operational costs, enhance user experience, meet compliance requirements and cost savings.
- **Security Teams:** Stronger authentication methods, such as multi-factor authentication (MFA), Brute Force detection, Auditing & Compliance capabilities, Tracking user activities
- **IT Teams (Admins/Developers/Leaderships):** Centrally managed user authentication, smoother user provisioning & deprovisioning, reduces the need for password resets and

support requests, resulting in cost savings and operational efficiency, developers can focus on application functionality while relying on the SSO infrastructure for user authentication.

Features:-

Features:

Multitenancy

Multi-tenancy at the realm level which allows multiple groups of users, sharing common accesses & privileges, to use the same application securely

Social Media Login

Lets you access your account by logging in with social network accounts, such as Github, Google, LinkedIn and Facebook. The user can choose which service they would like to authenticate with.

JWT Based Authentication

The solution is enabled with JWT token-based authentication along with JWE, Certificate based JWT encryption, Integration with JAVA Apps

GDPR Compliance

The solution complies with GDPR, featuring email notifications on user disable, deactivate, OTP/Authenticator login, MFA (FaceID and Fingerprint), and Captcha on Login/Registration.

Password & Session Invalidator

Password Invalidator invalidates password after first login to SSO and the session invalidator invalidates all other sessions except the current user session.

Multi factor Authentication

OTP/Authenticator based Login, Captcha on Login/Registration, Biometric Authentication and Push Notification based authentication.

One to many user mapping

Single Phone number/Email to be mapped with multiple user ids for authentication to the selected users for better monitoring and tracking purposes.

Brute Force Detection

When repeated failed login attempts to gain unauthorized access are made, the system detects this and provides customized alerts.

Disaster Recovery

The solution is enabled with a Disaster recovery environment and database to come to aid in case of outages and issues.

Customized Sign-in page & Mail templates

The SSO login page theme and notification emails can be customized to align with the customer's web page and theme design, respectively.

Identity Token Size Optimisation

The solution optimizes large ID tokens generated from the RBAC model, wrapper to optimize and retrieve roles post-authentication.

Re-Engineered cache

Cache was reengineered using Infinispan, optimising performance & integration capabilities

Inactive User Tracking

Track the irregular/inactive users of the app, Deactivate the user and inform the user to self activate using the Extended API.

Secure AD integration as user Federation

The solution integrates the customer's Active Directory system using secure LDAPS, which utilizes a self-signed certificate for secure communication between client and server, instead of a CA certificate.

Deactivation of Idle users

Deactivate Idle users in SSO after certain time period.

Extended Authentication API

Our solution enables authentication features through an API, allowing it to act on behalf of the customer or user upon receiving a direct grant.

Benefits include:

- **Ease of use** - enables you to manage your applications from a central location and unlock access for specific users with just one click.
- **Support for multiple user groups** - allows multiple groups of users, all sharing common accesses and privileges, to use the same application securely, thanks to multi-tenancy at the realm-level.
- **Industry-leading authentication** - leverages JWT token-based authentication, along with JWE, certificate-based JWE encryption and Java apps.
- **GDPR compliance** - incorporates a range of features to adhere to complex compliance requirements, including deactivate controls, multi-factor authentication, Captcha on login and registration, and more.
- **Security controls** - prevents access to sessions which aren't current, and provides customised alerts when repeated failed login attempts are made.
- **Sophisticated monitoring and tracking** - incorporates 'one-to-many' user mapping, which enables single phone numbers and emails to be mapped with multiple user IDs, to authenticate selected users.
- **Disaster recovery and backup** - includes a disaster recovery environment and database to assist in case of outages and issues.
- **Supports role-based access** - can optimise huge ID tokens, generated based on role-based access controls. Features a wrapper to optimise ID tokens and retrieve roles directly after authentication.

Contact for Demo:

Web: www.ztrust.in

Phone: +91 99029 91978

LinkedIn: <https://www.linkedin.com/showcase/ztrust-single-sign-on/>

Ready to streamline your customer's login experience? UPGRADE TO ZTRUST TODAY!!!!