AccessMatrix™ USO
unified single sign-on platform

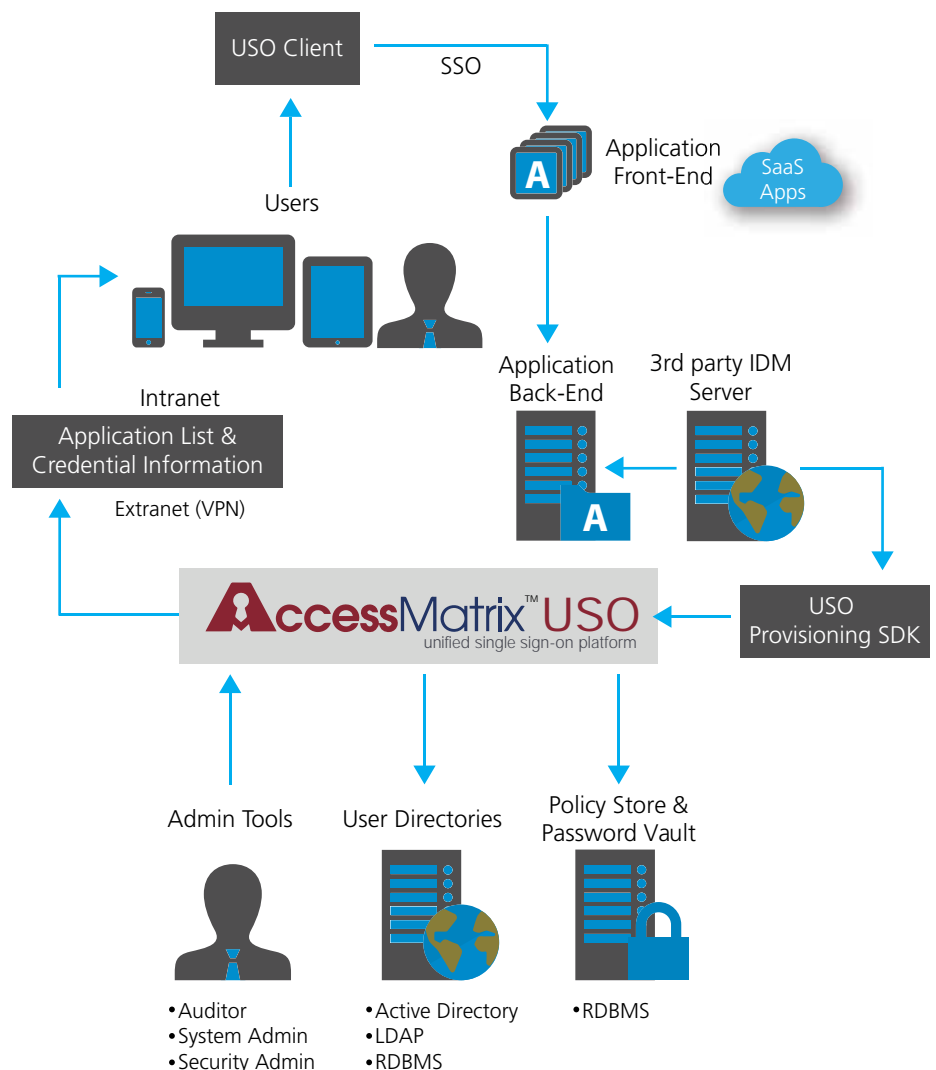## Secure Enterprise Single Sign-On solution for Employees and extended Organisations

Desktop	Mobile

Key Benefits

- Provide convenience for users and improve their productivity through faster access to applications and information

- Enhance security with flexible authentication and audit policy by supporting strong authentication methods and user-centric activity tracking

- Maximize ROI by reducing help desk costs through reduction of password reset calls and the efforts in consolidating

- Ensure compliance with powerful reporting capabilities to report user activities and security violations

- Integrate with existing Infrastructure by leveraging existing authentication methods and user registries

- Unify SSO infrastructure by providing integration with all leading Web Access Control products to provide a unified SSO environment

- Centralize Management of Information Access through integration with provisioning solutions

Supported USO Target Applications

- Windows Applications
- Web Applications
- Java/Applet Applications
- Host Applications
- Packaged Applications
- SaaS Applications

AccessMatrix™ Universal Sign-On (USO) provides sign-on automation, enhancing authentication process and enforcing consistent password management policies across applications. AccessMatrix™ USO improves user productivity by simplifying access to all applications through a single authentication while enhancing security by integrating strong authentication mechanisms and proven best security practices.

By removing the burdens of users and administrators from remembering multiple username and password combinations, AccessMatrix™ USO offers organizations the tool to tackle the password management issues by reducing the support costs, enhance security, and ensure compliance. AccessMatrix™ USO can also provide strategic values to help organizations to unify the password management processes and consolidate different login mechanisms to simplify the security infrastructure and reduce the support and operation overheads.

- Auditor
- System Admin
- Security Admin

- Active Directory
- LDAP
- RDBMS

- RDBMS

Features

- Sign On to any application
- Web Based Client Interface
- Simple Installation
- Offline Operations
- Application Login Profile Generator
- Web Based Self Service Facility
- Powerful Reporting for Audit Events
- Mobile/ Cloud Ready

Quick and Easy Deployment

Sign On to any application
Enables single sign-on for Windows® desktop application (thick client), Web application on IE, Chrome, and Edge (Chromium-based), Java™, terminal emulator for servers like Unix, Linux, AS400 or mainframe without any changes to the target applications.

Web Based Client Interface
Provides a web interface to launch and sign on to target applications.

Simple Installation
Provides installer in standard MSI format, enabling push down installation by leveraging Active Directory features and offers the smallest ESSO Client footprint in the market to simplify installation to expedite the deployment process.

Offline Operations
Provides cryptographically secured offline local cache. The password in local cache can be synchronized back to the server when connection is available.

Application Login Profile Generator
Provides an Application Trainer Software to enable sign on to applications by learning the application password usage process including sign-on, password selection and password change.

Web Based Self Service Facility
Uses a web based self-service facility to enable users to perform application enrollment and password recovery.

Powerful Reporting for Audit Events
Provides user-centric reporting capabilities to report access activities and security violations.

Policy Driven Access Management

Granular Admin Delegation with Fine Grained Admin Role
Leverages the patented Segmented Hierarchy-Based Security Administration and Authorization Framework to enable fine-grained administration delegation to address complex user administration operations for organizations with distributed locations.

Application Specific Password Management Policies
Provides better enforcement of password policy through customizable security policy for each application including password composition, minimum and maximum length, expiry, auto password generation, etc. which can also improve the security of legacy applications with weak password capabilities.

Configurable Authentication, Access Control and Audit Policies
Provides configurable access control, authentication and audit policies to meet some of the most stringent security policies and compliance requirements. It also audits both admin activities and end-user access activities including logons, application requests, failed logon attempts, etc.

Session Management

Configurable User Session Policies
Supports configurable user session settings such as idle timeout, session lifetime to provide maximum protection.

Inactivity timeout and Single Sign-Off
Automates application sign-off, when a user logs off, their session is terminated based on walk-off and inactivity timeout security policies.

Advanced Security

End to End Credential Protection
Protects password information while in storage, in transit and in desktop memory using leading encryption standards to ensure absolute confidentiality and privacy.

Forced Re-Authentication
Supports re-authentication for security sensitive applications before replaying the credential information to avoid walk-off security issues.

Strong Authentication Support
Supports a wide range of user authentication methods, from one time password tokens to smart cards to biometrics, to strengthen the login process for the AccessMatrix™ USO login and the re-authentication challenge for target applications for single sign-on.

Secured Sign-On to Trusted Applications
Launching of trusted applications (with integrity checking) to guard against phising websites and Trojan applications.

Bank-Graded Security with HSM Integration
Uses FIPS certified and tamper proof HSM devices to protect the key materials to provide maximum security protection.

Flexible Integration Options

AccessMatrix™ USO API
Provides an API Toolkit as an add-on API sets to provide common security services to extend the product functionalities and to customize the SSO Client behavior and branding requirements.

WebSSO Integration
Provides integration options with leading Web Access Control products such as IBM Tivoli Access Manager, CA SiteMinder, Oracle Access Manager, etc to provide a unified SSO environment.

User Provisioning Integration
Integrates with any provisioning system through AccessMatrix™ USO's User Provisioning API, or with certified provisioning solutions to centralize Management of Information Access.

System Requirements

- Client Platform Supported: Windows 10
- Mobile Devices Supported: Android and iOS
- Server OS: MS Windows 2012 R2, 2016 and 2019, Redhat Enterprise Linux 7.x and 8.x, Ubuntu Server 18.04
- Java Runtime: JRE 11 LTS
- Database for Policy Store: MS SQL Server, Oracle RDBMS and Oracle MySQL
- External User Store: Active Directory, LDAP v3 compliant directories and JDBC compatible databases

About i-Sprint Innovations

i-Sprint Innovations, established in the year 2000, is a premier identity, credential and access management solutions provider that enables individuals, organizations, and societies to build trust and identity assurance for powering productivity gain through digital identity and identity of things (IDoT).

i-Sprint's unique brand of security products, intellectual properties, and patents are designed to exceed regulatory requirements such as global financial services. By incorporating the latest mobility/ biometrics/ cloud/ identification technologies, i-Sprint provides solutions that ensure secure access and protection of data, transaction and assets. i-Sprint delivers trusty, versatile and strong authentication, and identity management platform to secure multiple application delivery environments based on a common security platform.

i-Sprint's digital identity product offerings include adaptive authentication (biometrics, multifactor authentication and more), single sign-on services, end-to-end encryption (E2EE) authentication and data protection for transaction data and to secure access to the web, mobile, and cloud-based applications. i-Sprint's IDoT product offerings provide the next-gen anti-counterfeiting, track and trace, and interactive consumer engagement that aims to help business in building consumer trust, improve brand protection, personalize consumer engagement and provide business intelligence.

i-Sprint's clients include leading global and regional financial service institutions, government agencies, telecommunications, public utilities, manufacturing, healthcare, education, multi-national corporations and others. Currently, i-Sprint has a direct presence and active authorized partners across Singapore, China, Hong Kong, Taiwan, Malaysia, Thailand, Japan and the United States.

20211011