



AccessMatrix™ USO

non-intrusive single sign-on approach

Enterprise SSO solution that works with leading web portal servers and also with HSMs (Hardware Security Modules) for enhanced security.

AccessMatrix™ Universal Sign-On (USO) is a non-intrusive security solution that easily enables single sign-on to multiple applications and systems without any source code changes. In most organizations today, users need to remember too many IDs and passwords that need to be changed frequently and increased. By deploying USO, our clients have improved staff productivity, customer satisfaction, while reducing administration costs.

How Does USO work?

The USO solution is built atop our AccessMatrix security server foundation layer. In this way, the user benefits from additional security features like administration, audit and application level authorization. USO's ability to auto-install, auto-configure and self service, greatly simplifies deployment and needs minimum maintenance effort.

The following are the USO specific components:

USO Trainer

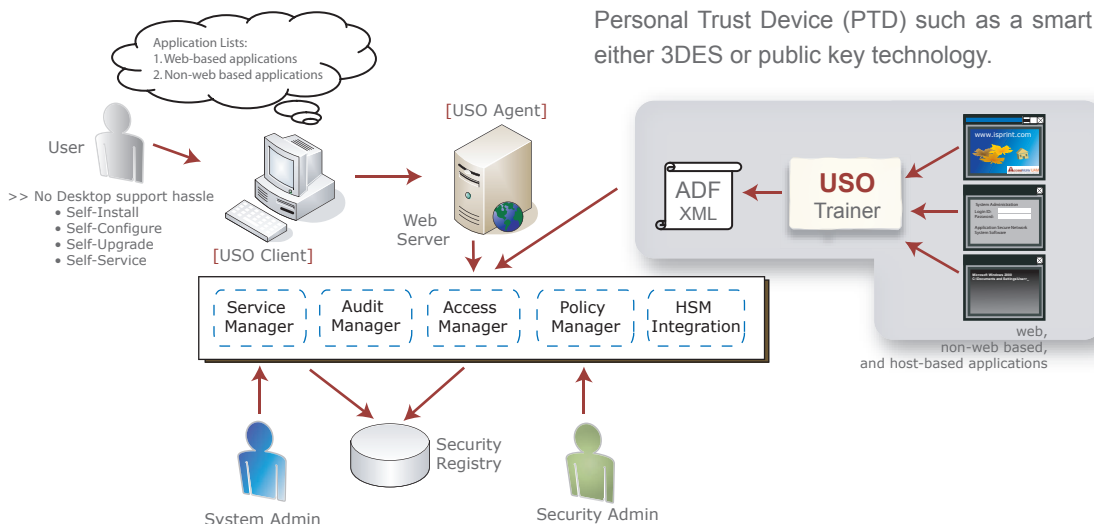
The USO Trainer learns the login and password change sequence of each application. The trainer utility records screen identification attributes and security-related field mappings and enables the appropriate credential to be automatically passed on to the application at login. It includes the default application level security policy for login behavior and password change. The trainer has an option to test the login and password change sequence that is captured. The information learnt by the trainer is then exported to an application definition file. Administrators will be able to import the application definition information into the AccessMatrix security server.

USO Agent

The USO Agent serves as a gateway between the USO Client and the security server in the online single sign-on mode. It maintains secure connections to the security server. After successful authentication, the list of applications accessible by the user is sent to the USO Client.

USO Client

The USO Client is a software component that is automatically downloaded to the user's desktop when the user logs in for the first time. The USO Client monitors the user's desktop to detect a login screen match and automatically logs in to the target application on behalf of the user. The user's login information can be stored in the Personal Security Environment (PSE) for offline access. The PSE is integrity protected and encrypted by the Personal Trust Device (PTD) such as a smart card using either 3DES or public key technology.



Features and Benefits of AccessMatrix™ Universal Sign-On (USO)

USO is built on the AccessMatrix framework. USO inherits the salient features of AccessMatrix, in addition to its own features. The features specific to USO are as follows:

Easy to Deploy

- The application's login and password screens can be trained to achieve single sign on. Application source code changes are not required. This approach greatly simplifies the integration of applications into the USO system.

Enhanced Bank-grade Security

- Encryption keys can be protected using hardware security modules from leading HSM suppliers.

Works with existing Portals

- The organization's portal can be easily integrated and secured with USO.

Automated Client Deployment to the Desktop

- Quick deployment with no disruption to the user's desktop.

Strong Authentication

- USO supports wide varieties of two-factor authentication devices from major security token vendors.

Easy-to-Manage

- The latest version of the USO Client is automatically downloaded to the user workstation.

Easy-to-Use

- USO enables users to supply their user id and password to each USO - enabled application, when they login for the first time to each application.

No Weak Links

- All communications between components of USO are secured using SSL.

Self-help Password Change Flexibility

- The Auto Password Change option enables administrators to generate new passwords based on the policy defined for each application. Manual Password Change prompts users for the new password and enables sign-on to applications, even when the security server is not available. The USO system can be configured to allow the user to reset the application password, when the password in the security database is out of sync with the target application.

Mobility

- USO's PSE (Personal Security Environment) on the user's desktop or a hardware token can be configured to store security credentials and application attributes. This unique feature enables users to have access to the USO single sign-on facility, even if they are not connected to the AccessMatrix security.

Non-disruptive Security Upgrades

- If the organization wants to deploy USO and UAM to achieve tight integration and more granular access control, the AccessMatrix security server in the USO implementation can be upgraded to the AccessMatrix security server of the Universal Access Management (UAM) product.

ABOUT ACCESSMATRIX

AccessMatrix™ is based on i-Sprint's patented Hierarchy Model technology (PCT/SG02/00027). It is the common framework on which USO is built. USO inherits the salient features of AccessMatrix security server, in addition to its own. AccessMatrix provides centralized authentication, authorization and audit services for users to securely access different e-commerce and enterprise resources e.g. web and application servers. It provides centralized and comprehensive policy management services for administrators to easily and effectively manage application permissions, user privileges, and security policy throughout the entire organization. The following are the major benefits of our AccessMatrix framework:

Simplifies User Management

The AccessMatrix hierarchical model allows organizations to designate security administrators at different levels of the organization. The administration rights of the security administrators can be defined to improve security, decentralize security administration and ensure a high level of accountability. The framework allows external organizations such as customers and business partners to manage IDs and user rights by their own security administrators. AccessMatrix further streamlines user management by integrating with existing user registries, such as LDAP or Microsoft Active Directory.

Simplify Enterprise-Wide Security Policy Enhancement

Enterprise-wide security policies are defined and managed by AccessMatrix in a segmented hierarchy that closely mirrors a company's existing organization structure. A corporate-wide security policy can be controlled and enforced from a company's headquarters.

Embedded "Best Security Practice" features from Global Banks

AccessMatrix supports the principles of dual control, least privilege and segregation of duties. These security principles are important to financial institutions and other industries. Security administrators are assigned granular administration rights appropriately to their job functions and within their organizations. Maker-Checker or dual control can be used to further ensure that modifications submitted by one administrator must be checked and approved by another administrator before the proposed changes become effective. In addition, AccessMatrix checks that the same user is not assigned to multiple roles within an application, thus avoiding a conflict of interest. Roles defined within the applications are application-specific.

Investment Protection, Scalability and Platform Independence with JAVA

The AccessMatrix security server is built using Java technology and standards and therefore can be deployed on any platform that supports the Java Run-time Environment.