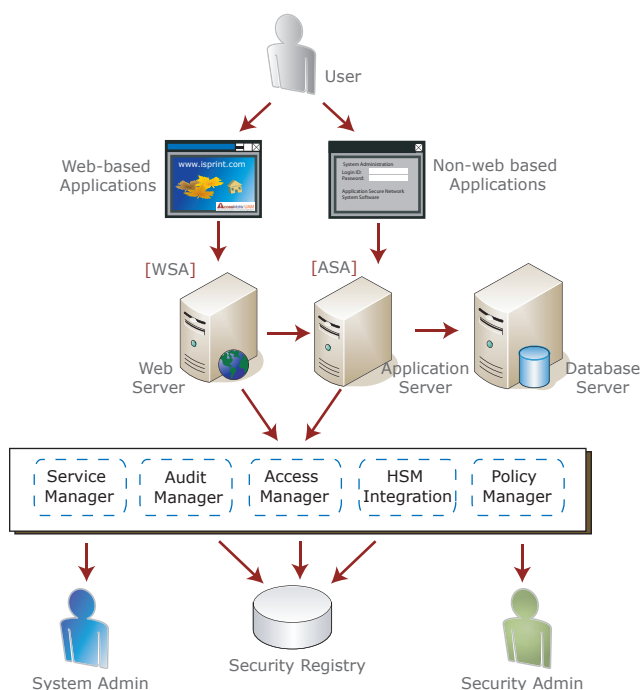


Common Security Services for Enterprise Applications Administration, Authentication, Authorization and Audit

AccessMatrix™ Universal Access Management (UAM) is a comprehensive enterprise application access control, single sign-on and security administration system. UAM controls and manages user access to all web, non-web and client server application. Leveraging on the AccessMatrix technology, UAM fulfils the most rigorous form of application security by providing security administration, authentication, authorization, and audit services (4As) to business applications within your organization. UAM enables multiple applications to access a common set of security services through tight integration with the application.



Improving Application Security

The UAM security infrastructure is designed to secure multi-tier applications, either web-based or non web-based, running on multiple heterogeneous platforms. The AccessMatrix hierarchical model allows organizations to deploy a single security infrastructure for easy integration with multiple applications. All access control decisions are made by the AccessMatrix security server. The UAM solution is highly scalable, promotes software re-use and reduces application maintenance and support efforts.

Providing Flexible Security APIs and Agent Technology

A set of security APIs is available for developers to tightly integrate web and non-web applications. UAM's Web Security Agents (WSA) and Application Security Agents (ASA), allows secure access to the resources within web servers and application servers based on the access control policy defined by the security administrators. This centralized policy-driven approach to Authentication and Authorization greatly simplifies user administration and application integration.

Features and Benefits of AccessMatrix™ Universal Access Management (UAM)

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

Secure Multi-tier Applications

- Designed for multi-tier applications running on multiple heterogeneous platforms.

Application Integration

- Open APIs are provided for ease of integration and code re-use, including Java and COM.

Fine-grained Access Controls

- Access control down to application, object, method and parameter.

Business Rules

- Access control based on the rules of the business transaction.

Application Specific Roles

- Roles are application specific.

Secure Communications

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

Personalization

- Business and security-related attributes defined within UAM can be used by applications for personalization.

Easy Deployment

- Web servers can be easily secured with the Web Security Agents of the UAM.

Portal Integration

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

Time and Location Restrictions

- Access control based on time and location.

About AccessMatrix™

AccessMatrix™ is based on i-Sprint's patented Hierarchy Model technology (PCT/SG02/00027). It is the common framework on which UAM is built. UAM 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.

Features and Benefits of AccessMatrix™ Security Server

SECURITY

Pluggable Authentication

- Different authentication methods can be defined depending on the risk level and registry.

Integrity Protection of Audit Logs

- Audit trails are digitally signed.

Pluggable Cryptographic Module

- The crypto software package used by the implementation can be specified by the customer based on their security standards and / or regulatory requirements.

Security and System Alerts

- Selected security and system events are delivered to system management utilities, via SNMP, if required.

Support Multiple External Registries

- Each segment can be interfaced to either different registries or the same registry for authentication.

SCALABILITY AND HIGH AVAILABILITY

High Availability

- Multiple instances of the AccessMatrix security server components can be configured to support fail-over.

Load Balancing (optional)

- The AccessMatrix security server can be configured to support load balancing to ensure superior performance for large user populations.

MANAGEABILITY

Segmented Hierarchy

- Security policies, applications and users are defined in a central server, based on the organization's structure.

Policy Driven

- The corporate security policy can be enforced automatically throughout the enterprise in real-time for all applications running on heterogeneous platforms.

Granular Administration Rights

- Security administrators are assigned granular administration rights and their scope is defined within the organization's hierarchy.

Easy User Management

- The user credentials, privileges and attributes of a large user population can be easily managed via the Policy Editor GUI.

Dual Control

- Administration-related change requests submitted by one security administrator (maker) must be approved by another administrator (checker).

Provisioning

- The AccessMatrix security server can be integrated with multiple external registries e.g. Microsoft Active Directory, LDAP and databases.

Delegation

- An administrator can be given the option to delegate administration rights to other administrators.