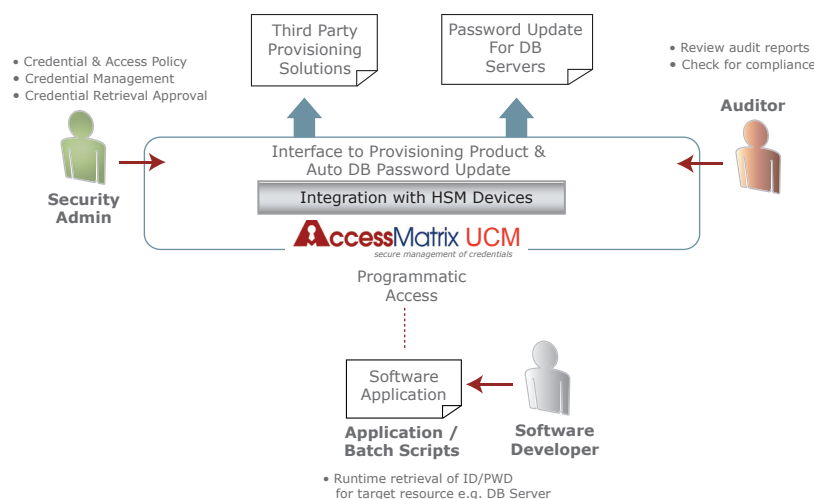


AccessMatrix™ Universal Credential Manager (UCM) address the major audit challenges faced by organizations having to hard code clear text IDs and Passwords for accessing enterprise information resources, e.g. database connection pools in applications servers and database scripts for accessing data in databases. Organizations can now avoid the vulnerabilities and operational challenges in handling IDs and passwords that are currently being manually hard coded in applications and command files.

Eliminating Hard Coding of IDs and Passwords

i-Sprint's UCM is based on patented AccessMatrix technologies. 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 UCM solution is highly scalable, promotes software re-use and reduces application maintenance and support efforts.



What does UCM offer?

UCM enables organizations to retrieve user IDs and passwords for specific applications during run time so that the user credential information does not need to be hard-coded in applications or command files.

UCM also enables organizations to now enforce password policies through its advanced features to enable password quality checks, automated password change policies, storing encrypted passwords using proven and published encryption algorithms. Stronger security is available with the integration of HSM (Hardware Security Module) to provide key management and encryption services.

How does the integration work?

UCM provides two integration approaches that enables software developers to rapidly integrate their applications with UCM:

- **Application APIs** - A set of flexible and simple APIs retrieves the current IDs and Passwords from the UCM server.
- **Command line utility (UCMRun)** - Enables dynamic replacement of IDs and Passwords in command files with no coding effort.

Features and Benefits of AccessMatrix™ UCM

Features	Descriptions	Benefits
Common Security Infrastructure for password management and encryption	UCM provides the flexibility to manage multiple Ids and Passwords for each application	Enable organizations to easily manage IDs and passwords for multiple applications
Automated Password Change Policy	UCM provides the facility to automate the password change process based on the password policy defined	Enable organizations to enforce the password policy
Flexible APIs and Secure Utility for dynamic replacement of ID/PWD parameters	UCM provides simple APIs for organizations quickly to deploy UCM to manage Ids and Passwords and utility software dynamic replacement of ID/PWD parameter at runtime	Enable organizations to have quick deployment to address the password challenges
Secured Communication	All connections among UCM components of the access management system are secured using SSL, which provides PKI-based mutual authentication	Enable organizations to ensure message confidentiality and integrity for all messages exchanged between AccessMatrix components
Patented technology - Hierarchy model for Administration and Delegation	UCM provides the flexibility to enables security administrators to be appointed at every level of the organization structure to manage user access to computing resources in the enterprise with full accountability	Enable organizations to control the administration rights of the local security administrators by defining at a granular level to improve security and reduce administration costs
Policy Driven Approach	UCM provides a facility to enforce automatically enterprise-wide security policies governing passwords, authentication methods, time and access restrictions	Enables organizations to apply consistent security policy across the organizations based on the defined security policy
Secured Audit Log and Activity Reporting	UCM provides the logging features to record all events in a dedicated audit log servers and allows auditors to use predefined reports to review user administration activities	Enables organizations to provide auditors with a complete audit trail information and reduces the time in consolidating information for user account management
HSM for Key Management & Crypto Processing	UCM can integrate with HSM to protect the master key for encrypting the confidential information such as password as well as provider optimal cryptographic processing performance	Enables organizations to protect their confidential information stored inside the AccessMatrix security registry
Maker / Checker Controls	UCM provides Maker-Checker control to ensure that modification submitted by one administrator must be approved by another administrator before the proposed changes become effective	Enables organizations to achieve accountabilities in performing security sensitive tasks in managing the security infrastructure and avoid any potential security exposure
Least Privilege and Segregation of Duties	UCM supports the principle of least privilege and segregation of duties and this clearly segregates the job function between the security administration and the system administration	Enables organizations to limit the scope of the security administration rights to the segment and subordinate segments and avoids any potential conflict of interests
Scalability & Availability	UCM provides the scalability and high availability features by running multiple instances of the AccessMatrix server components across multiple machines	Enables organizations to achieve better system up time and minimize unplanned system downtime

Further details about i-Sprint's products are available at www.i-sprint.com. To reach us, please email to enquiry@i-sprint.com or contact any of the offices or our resellers in your area.