

AccessMatrix™ Universal Credential Manager (UCM) addresses the major audit and operational challenges faced by organizations in managing the storage and retrieval of privileged IDs and Passwords during normal operations and emergency situations for accessing enterprise information resources, e.g. database, critical servers, network devices, etc.

Interactive Access to Privileged Credentials

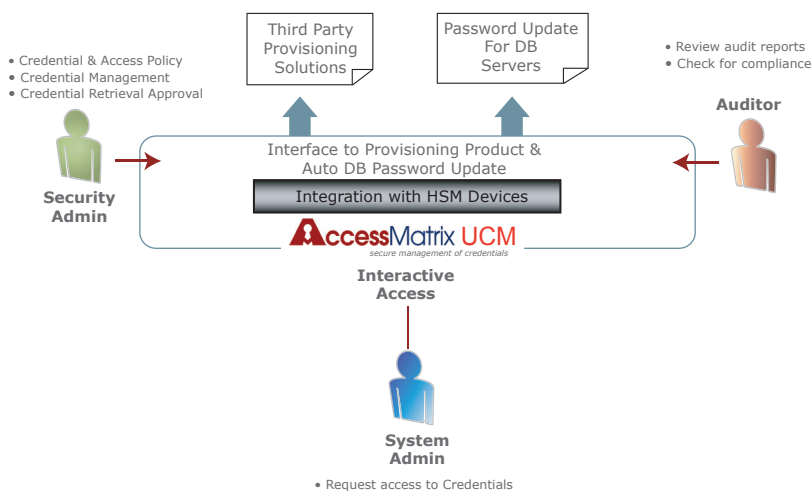
Often, such confidential information is written on paper, is sealed in a envelope and is physically placed inside a physical safe deposit box to prevent unauthorized access or use of the information. Although this is a common practice, it creates many limitations:

- Lack of authorization check to ensure that only authorized staff is able to access the passwords;
- Lack of Audit Trail for password change, check in and check out;
- Lack of enforcement of normalization after the password has been checked out;
- Physical constraints for remote access from different locations.

What does UCM offer?

AccessMatrix UCM overcomes the above limitations by providing a secure password repository with a management infrastructure and interactive access with workflow approval for authorized users to retrieve the privileged passwords during emergency or support requirements. Some of the key features include:

- Access control for specific credentials;
- Audit Trail and reporting for critical activities;
- Strong Authentication with multi-factor authentication support;
- Workflow approval;
- Auto Password Update to target resource e.g. database, servers, etc;
- Flexible APIs for integration with external workflow software.



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
Work flow Integration	UCM provides a built-in workflow to enable administrators to perform self service to retrieve confidential credentials and it also tracks credential owners in performing password reset after the credential information has been used.	UCM is out-of-the-box solution to enable quick deployment and provides an open interface to integrate with other workflow software to handle complex workflow requirements.
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.