AccessMatrix™ UCM
secure management of credentials

Universal Credential Manager (UCM) is a Next Gen Privileged Account Activity Management (PAAM) solution with Agentless Connectors, Visual Recording and SSO Integration

Key Benefits

- Improve IT reliability and reduce operational costs and complexity
- Scalable and reliable Common Authentication Platform with bank grade security for handling Complex Authentication Requirements, Access Control, Tamper-evident Audit Storage and Credential Vaults
- Detailed accountability with Visual Recording and Text Based Audit logs
- Provides Centralized Management Console to Manage Privilege Accounts End-to-End and Unified Reporting
- Simple integration and deployment with options for plugable customized module
- Eliminate hard coding to improve security

Features

Flexible and Fine-Grained Administration

- Patented Hierarchy Model for Administration and Delegation
- Policy Driven Approach
- Support to count abnormal accounts based on asset attribute
- Dynamic password change, supporting flexible and dynamic password change rules based on credentials and safe
- Support global pause and start of batch password change plans
- Maker / Checker, Least Privilege and Segregation of Duties among various Admin Roles

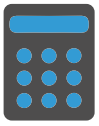
Common Platform for Privileged Credential Management

AccessMatrix™ Universal Credential Manager (UCM) provides a virtual password safe deposit box with strong encryption using HSM devices to store privileged account IDs and passwords (aka credentials). UCM provides the security features to address the major audit and operational challenges faced by organizations in managing credentials and its session activities. The common challenges are:

- Manual Management of IDs and Passwords
- Lack of Privileged Session Activities Tracking and Control
- Hard-coded Privileged IDs and Passwords in batch jobs and applications
- Provide forensic trails and visual recording of privileged access to critical servers and computing resources

Comprehensive PAAM Features

Built-in workflows for office hours / non-office hours or integrate with external ticketing system



Support various authentication options

Workflow-driven credentials Check-in / Check-out with auto password update on check-in

SSO to target resource with session video recording

Tagging credentials (privileged passwords) e.g by project, UAT, production, OS

Agent & Agentless Integration with databases, Unix, windows, routers, firewalls

CSV import and backup PDF versioning of credentials

Native Integration to existing Enterprise user store or target resource data store

Use encryption key, security policies from Safe with optional HSM protection

Secure access and seamless connection from any location on any device (desktop, laptop,mobile)

Easy of Deployment and Manageability

- Grouping of credentials for ease of administration
- Bulk import of target resource information
- Integration with existing user directories
- Auto Account Discovery

Securing Privileged Access

- Customized Approval Workflow and credential management
- Command filtering to restrict administrator activities
- Single Sign-On to target resources without revealing the password
- Strong Authentication using 2nd Factor Authentication to access target resources

Comprehensive Audit Logs and Detail Reporting

- Session logging using visual recording and command text-based audit logs
- Secured Audit Log and Activity Reporting

Advanced Security Features

- FIPS Certified HSM for Key Management
- Comprehensive APIs for customization
- Customize rules to detect weak passwords
- Support batch export of credentials in case of emergency

What Does UCM Offer?

Privileged User Access (PUA) Module: UCM provides a secure approach with multi-level approval flow and empowers organizations to manage security administrators to retrieve and deposit privileged credentials. This enables authorized users to check in and check out privileged credentials to perform their duties or during emergency situations. Interactive features include:

- Flexible access control for credentials based on reporting hierarchy
- Audit trail with command captures and video session recordings
- Strong authentication with multi-factor authentication support
- Multi-level dual control workflow approval
- Manual, single-sign-on or auto login into target resource after check-out
- Automatic password management using agent-less technologies
- Flexible APIs for integration with external workflow or ticketing software

Privileged Session Manager (PSM) Module: UCM provides add-on Windows RDP Gateway Recorder to monitor and record privileged sessions. It supports video recording playback for forensic analysis. It also supports command access control for selected protocols.

Application Password Manager (APM) Module: 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 provides two integration approaches:

- Application APIs - a set of flexible and simple APIs retrieves the current IDs and password from the UCM server
- Audit Password Consumers - Enables dynamic and transparent replacement of IDs and Passwords in command protocols such as JDBC, ADO.NET, Windows and Unix scripts

Patented Hierarchy Model for Administration and Delegation

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

- Enforce Automatically enterprise-wide security policies governing passwords, authentication methods , time and access restrictions
- Enable organizations to apply consistent security policy across the organizations based on the defined security policy

Maker / Checker, Least Privilege and Segregation of Duties among various Admin Roles

Enable organizations to deploy the UCM solution without a super user and limit the scope of security administration rights to the segment and subordinate segments to avoid any potential conflicts of interests.

Auto Account Discovery

Provide automatic account discovery report and notify administrators of new accounts not managed by UCM.

Workflow Approval

- Provide 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
- Provide Multiple Workflow types to suit different types of organizations and scenarios: Multi-level approval, After Office Hours, Manager-Subordinate Workflow

Command Filtering

Provide the capabilities to restrict the commands which can be used by an administrative user during a privilege access session. This can achieve using agent or agentless approach.

Session Logging

Provide bulletproof forensic and activity logging using visual recording and command logs.

Secured Audit Log and Activity Reporting

Provide logging features to record all events to enable auditors with complete audit trail information and reduce the time in consolidating information for credential management.

FIPS Certified HSM for Key Management & Crypto Processing

Enable organizations to deploy the UCM solution without a super user and limit the scope of security administration rights to the segment and subordinate segments to avoid any potential conflicts of interest.

Easy to Manage

- Support tagging of credentials for ease of management and retrieval of credentials
- Dynamic tag by target resource type and safe

Password Consumers & Flexible APIs

Enable organizations to have quick deployment to address the password challenges with APIs and password consumers for dynamic replacement of ID / password parameters.

Web-Based Self-Service Portal

Web portal that enables request submission, check in, check out and approval functionalities with role-based access control.

Flexible Request Approval Process

Support different types of request approval processes and allow access control by policy based on safe and resource type, credential-oriented or reporting hierarchy based approvers.

Approval via Mobile Terminal

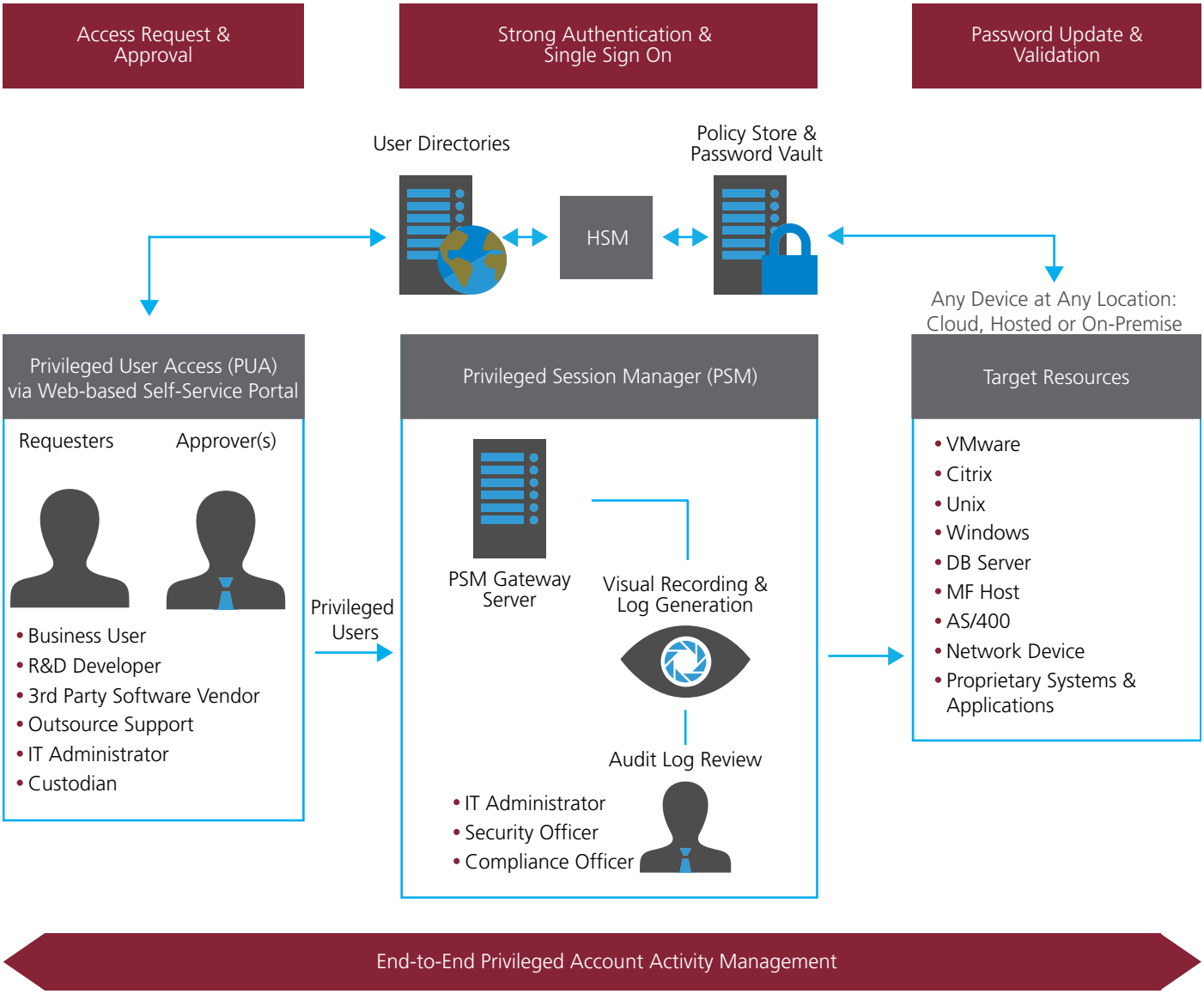
Support approval of check-out requests via mobile phone or tablet computer to increase productivity and service level.

UCM Programmatic / UCM Hard-coded

Most applications write credentials (such as username and password to connect to the database) in the application side or configuration file, which is actually an insecure practice. UCM provides programmatic features to minimize security risks.

System Requirements

- UCM Server / UCM Gateway: MS Windows 2012 R2, 2016 and 2019, 2022
- Java Runtime: JRE 1.8 and above
- Database for Policy Store: MS SQL Server, Oracle RDBMS, IBM DB2 and Oracle MySQL
- External User Store: Active Directory, LDAP v3 compliant directories and JDBC compatible databases
- Supported Target Resources: JDBC database servers, UNIX Servers, Windows Servers, Active Directory, AS400, IBM RACF Mainframe, Cisco / Array, Cisco ACS, Scriptable SSH / Telnet-based network devices e.g TopSec, Juniper, Huawei, H3C and RuiJie, http, https, Z/OS, Weblogic, Websphere and Webportal, AWS, Azure AD, InforSuite AS, MongoDB and Rest API
- Supported clients for UCM Gateway: database clients, VNC, rdp, web-based consoles, PuTTY, Tera Term, secureCRT and CuteFTP, WinSCP, SSH Secure File Transfer, IBM Data Studio, PComm, Exceed, vSphere Client, BeyondCompare



Global Headquarters
Blk 750D Chai Chee Road #08-01
ESR BizPark@Chai Chee (Lobby 1)
Singapore 469004
Global: +65 6244 3900
enquiry@i-sprint.com
www.i-sprint.com

For a complete list of our offices in
China, Hong Kong, Japan, Malaysia, Thailand & United States, please visit
www.i-sprint.com/contactus

20220614