AccessMatrix™ UAS

future proof universal authentication server

UAS Out-of-Band One Time Password is designed for easy integration with existing applications without having to synchronize user information

Key Benefits

- Rapid deployment of strong OTP authentication solution via the AccessMatrix™ UAS flexible integration framework and granular security policies
- Enhance security with OOB authentication to mitigate phishing attacks
- Leverage HSM hardware to provide the advance OTP generation and comparison options
- Maximize ROI by reducing implementation costs and project risks by deploying a proven security solution with solid track records
- Ensure compliance with powerful reporting capabilities to report user activities and security violations

Features

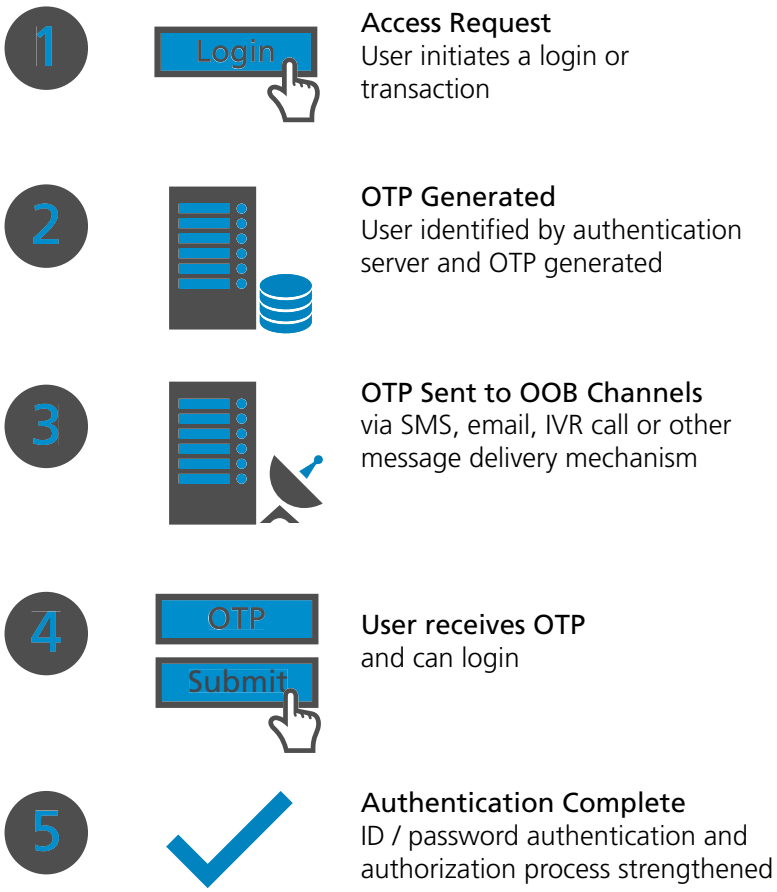
- Flexible OTP policies
- Audit Trail
- Multiple Delivery Mechanisms
- Flexible integration SDKs
- Built-In RADIUS Server
- Native Integration
- Key Management & Crypto Processing
- Operational Standard - Meet the most stringent service level and operational requirements for large-scale deployments.

Future Proof Versatile Authentication Solution

AccessMatrix™ Universal Authentication Server (UAS) is a versatile authentication server which enables organizations to unify their different authentication mechanisms and simplify integration complexities by providing off-the-shelf strong authentication modules for common applications.

AccessMatrix™ Out-of-Band (OOB) One Time Password (OTP) Module provides a secure authentication solution by using two separate channels to authenticate a user. This solution delivers an OTP to users via GSM Short Message Service (SMS), email, IVR or any message delivery mechanism which is different from the channel that the users interact with the applications. When a user tries to access a website, an OTP will be sent to his mobile phone via SMS or email which has been determined by the user in advance. Mobile devices can now become security tokens to receive OTPs that will strengthen the existing ID/ Password authentication and authorization process.

The complexity (length and format) and expiration of the generated OTP can be configured to comply with security policies of the organization.



System Requirements

- Server OS: MS Windows Server 2012/ 2016 and Red Hat Enterprise Linux 7
- Application Server: Oracle WebLogic, IBM WebSphere, Apache Tomcat and JBoss Web Server
- Java Runtime: JRE 1.8 and JRE 11 LTS
- Database for Policy Store: MS SQL Server, Oracle RDBMS and Oracle MySQL
- External User Store: Active Directory, LDAP v3 compliant directories and JDBC compatible databases
- FIPS Certified HSM

Flexible OTP Policies

- Expiry time
- OTP format (length, number, alpha, alphanumeric)
- Outgoing message template
- One-time use vs Multi-use
- Restriction to number of retries
- Personal Authentication Code to improve user experience

Audit Trail

AccessMatrix™ UAS - OOB OTP provides comprehensive tamper-evident audit trail information to track the usage of OTP and address the transaction audit requirements. It offers flexible reporting capabilities for administration, user activities and security violations.

Multiple Delivery Mechanisms

UAS supports delivery of OOB OTP via SMTP, SMPP, HTTP/S POST/ GET, Web Services based APIs.

Flexible Integration SDKs

UAS provides comprehensive SDKs with REST APIs to various kinds of applications to be easily integrated.

Built-In RADIUS Server

Built-in server offers RADIUS Server for strong authentication to firewalls, network devices, VPN servers or any server platforms and applications that support the RADIUS authentication protocol.

Native Integration

- Security Server supports a number of user registries such as LDAP and Active Directory as external user stores via LDAP protocol or JDBC
- Organizations can integrate the Security Server with their existing user registries without the need to synchronize user information
- AccessMatrix™ UAS can access the external user store(s) directory to simplify the integration efforts. No schema change is required and no information needs to be written to the external user stores

Key Management & Crypto Processing

AccessMatrix™ UAS has proven integration with HSM devices to protect the master key and support for OTP generation and comparison inside the HSM for high security needs.

Operational Standard

AccessMatrix™ UAS provides proven scalability and reliability features to meet the most stringent service level and operational requirements for large scale deployments.

Global Headquarters
Blk 750D Chai Chee Road
#08-01 Viva Business Park
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