

Users create weak passwords frequently

Multiple users shares an account & password

Staff leaks account & password

App management and maintenance become complex and difficult

Servers and hardware token cost is high

SecurLogin solves all these challenges for you!



Strong Authentication

Reduce risks caused by weak password and the cost of maintenance & equipments



Cloud Services

Easy-used Cloud service and simple deployment



Unified Management

Unified platform for effective & central management

SecurLogin - Strong Authentication

SecurLogin offers real time Second Factor Authentication (2FA) service on the Cloud to strengthen enterprise user login process. There is no need for enterprises to purchase any equipment. SecurLogin client app is required for some SecurLogin supported authentication methods, so enterprise staff needs to download and install it to support desired authentication methods. i-Sprint's strong authentication solutions are deployed to over 200 banks, and it provides enterprise reliable and leading strong authentications.

• Strong Authentication Methods



OTP via SMS or Email



Push messages via app built-in token



OTP generated by app built-in token



Scanning codes using app

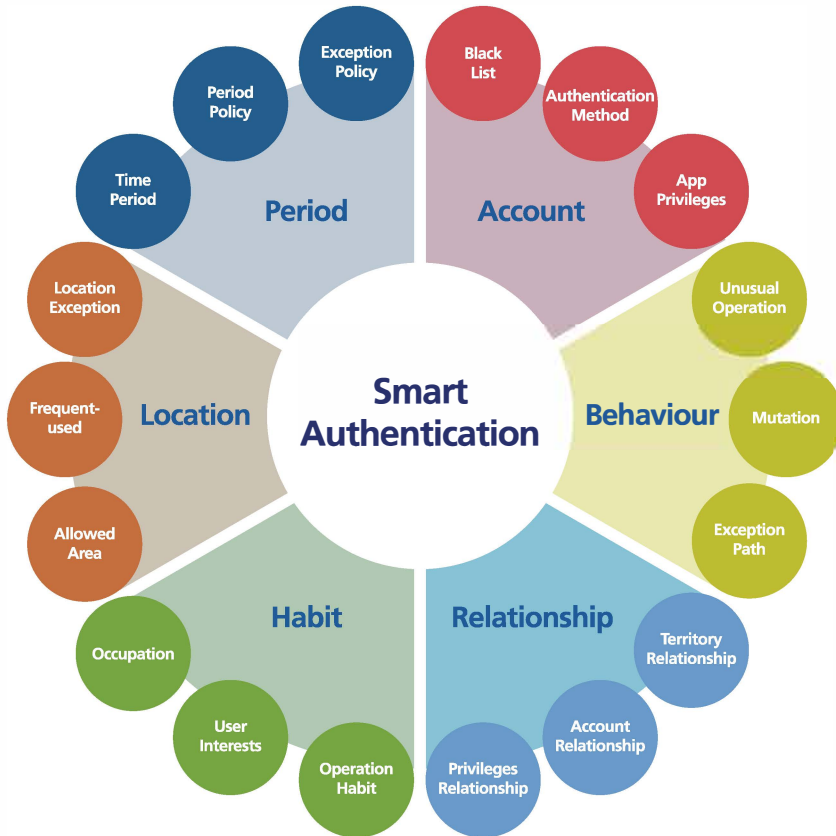


Telephone voice notification



Biometrics Authentications

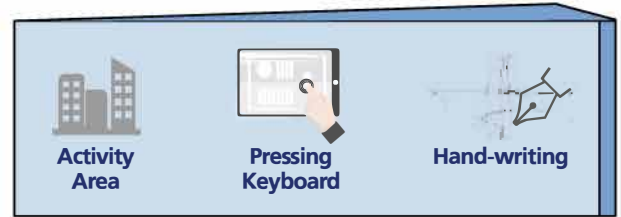
- **Smart Authentication (Contextual Authentication):** Auto adjusts the authentication level according to multiple factors, e.g. user accounts, habits, locations



- **Combination Authentication:** To improve the security and conveniences of authentication by combining user action and biometrics features



Biometrics Features



Action Features

SecurLogin - Unified Management

SecurLogin contains powerful unified management platform which can support multiple authentication methods to provide comprehensive identity authentication solution for enterprise information mobilization.

Various Management Functions • Enterprise Self-control • Big Data Analysis

- Apply unified management and strong authentication for multiple app systems by creating apps in SecurLogin system.
- Data-backup secures enterprise data.
- Enterprise/ Individual user can manage the 2FA authentication methods of apps by accessing Cloud service portal.

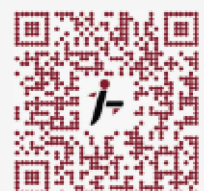
No.	Supported App & Devices	Supported Authentication Methods
1.	Radius Client, Juniper VPN, Fortigate VPN and CISCO ACS	SecurLogin Token (Push and OTP), SMS OTP, MAIL OTP
2.	App System Integration (API and Plug-in)	SMS OTP, MAIL OTP, SecurLogin Token (Push and OTP), Telephone call, Biometrics (Face & Fingerprint etc)
3.	Microsoft Apps (Email OWA, Office365)	SecurLogin Token (Push and OTP), SMS OTP, MAIL OTP
4.	Cloud App (Google App, DropBox , etc)	SecurLogin Token (Push and OTP), SMS OTP, MAIL OTP
5.	Web App (JIRA, Confluence, Jenkins, tikiwiki)	SecurLogin Token (Push and OTP), SMS OTP, MAIL OTP

Global Headquarter

Blk 750D Chai Chee Road
#08-01 Viva Business Park
Singapore 469004
☎ +65 6244 3900
✉ enquiry@i-sprint.com

For a complete list of our offices in

United States, Malaysia, Thailand, China,
Hong Kong & Japan, please visit
www.i-sprint.com/contactus



Scan for more information

©2000-18 i-Sprint Innovations Pte Ltd. All rights reserved.

A Hierarchy Model is a patent of i-Sprint Innovations Pte Ltd. i-Sprint, i-Sprint logo, AccessMatrix, AccessMatrix logo are registered trademarks of i-Sprint Innovations Pte Ltd. All other trademarks and registered trademarks are property of their respective owners. i-Sprint reserves the right to make changes to the specifications or other product information at any time and without prior notice.