Alliance Two Factor Authentication
Data Sheet

Two Factor Authentication on the IBM i with Validation via SMS or Voice

Two Factor Authentication (2FA), sometimes known as Multi-Factor Authentication, is helping organizations to improve the security of their core business applications. This technology helps reduce the security weakness of relying on passwords or passphrases as the primary and only authentication mechanism. Passwords suffer from numerous security issues including:

- Weak passwords (easily guessed, inadequate entropy)
- Lost passwords
- Exposed passwords (sticky notes)
- Multi-use passwords

Two Factor Authentication helps reduce the security threat by requiring an additional authentication mechanism beyond just a memorized password. Alliance Two Factor Authentication provides the IBM i security administrator an easy-to-use method of implementing a Two Factor Authentication mechanism based on voice and mobile SMS text technologies.

Townsend® SECURITY

Benefits of Two Factor Authentication

Improved Security
Many passwords use familiar details that can either be guessed or easily found out. The use of Two Factor Authentication ensures only authorized individuals obtain access to your systems and sensitive data.

Lower Risk
Two Factor Authentication reduces the potential for someone to guess or find out another users password, lowering the risk for an-authorized access.

Reduce Data Theft
Unauthorized access to information can lead to theft of valuable data which can damage your brand and result in lost business and customers taking legal action to redress their personal loss.

Compliance
Two Factor Authentication addresses compliance requirement issues (e.g. PCI, HIPAA, etc.) and audit requirements.

www.townsendsecurity.com

724 Columbia Street NW, Suite 400, Olympia, WA 98501 | 800 357 1019 +1 360 359 4400 Fax 360.357.9047

Features

- User logon authentication
- Application Program Interfaces (APIs)
- Store up to five phone numbers per user (voice and mobile)
- Up to five One-Time Codes (OTC) when away from phone
- User-defined maximum number of authentication attempts
- User preview mode before activation
- Automatic logoff on authentication failure
- Optionally disable user profile (account) on authentication failure
- Identify highly privileged users and enable 2FA
- Security audit journal (QAUDJRN) logging of all configuration changes
- Security audit journal (QAUDJRN) logging of all authentication failures
- Integrated diagnostic logging

SMS & Voice Authenticaiton

- SMS text authentication delivery to mobile devices
- Voice authentication delivery to standard phones
- No additional hardware or servers required (native IBM i application)
- No key fobs or biometric readers required
- Software-only solution

Network Infrastructure

- Telesign global network provider
- 200+ countries supported for SMS text and voice delivery
- 80+ languages
- Network and delivery redundancy
- 2.5+ billion users worldwide
- Flexible pricing plans

IBM i Services

- IBM i logon two factor authentication
- Application enablement for two factor authentication (APIs)

System Requirements

- IBM i operating system V5R4 or later
- Any IBM PowerSystems hardware platofrm

Evaluation

- Fully functional 30-day evaluation available

Support

- Software maintenance
- Technical support
- 24/7/365 support available
- On site installation available
- Contract services available