syncsort

PRODUCT SHEET

Alliance Two Factor Authentication

Security Beyond Names and Passwords for IBM i

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 or mobile Authy technologies.

Benefits

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 unauthorized access.

Reduce Data Theft

Unauthorized access to information can lead to theft of valuable data, damaging your brand and resulting in lost business or legal action by customers seeking to redress their loss.

Compliance

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

Two Factor Authentication (2FA)

Two Factor Authentication improves security by requiring more than one type of authentication from the list below:

- **A knowledge factor** - something you know (like a password)
- **A possession factor** - something you have (like your cell phone)
- **An inheritance factor** - something that is a part of you (like a fingerprint or retina)

Access to most computer systems is based on something you know - a password or passphrase. Passwords and passphrases are easy to lose, and password cracking software is getting much better even on long and complex passwords and passphrases.

By adding in another authentication factor, you can dramatically improve your security posture. Alliance Two Factor Authentication implements an additional possession factor - your mobile phone or voice telephone - to achieve true two factor authentication.

Twilio Global Authentication Service

Two Factor Authentication based on mobile and voice technologies is only as good as the service that delivers the authentication information. Alliance Two Factor Authentication integrates with authentication services from Twilio, a mature, global provider of 2FA services to large and small organizations. With the ability to deliver voice and mobile messages to every country, even multi-national organizations can rest assured that their 2FA needs will be met regardless of the location of their international sites.

Voice and Mobile Authentication

Alliance Two Factor Authentication lets your users select to receive authentication messages as voice or mobile Authy messages. You can define up to five phone numbers to receive messages, and the user can select which phone number to use each time they perform an authentication. Because some IBM i users have poor mobile cell phone coverage when away from work, you can easily define a home phone number or alternative number for authentication. Alliance Two Factor Authentication will remember your preferred phone number and method of delivery.

IBM i Logon Two Factor Authentication

The primary way that users authenticate to the IBM i platform is through the 5250 terminal logon panel. A user types a user profile name (account) and a password or passphrase. You can easily change the user profile to use the initial program provided in the Alliance Two Factor Authentication solution.

Alliance Two Factor Authentication makes it easy for a security administrator to implement 2FA for a user. A list of users is displayed with their current security level (high, medium, low) and the current setting for their initial program. Typing a single option next to the user profile will install the Alliance 2FA initial program on the user profile. The next time the user logs on, the 2FA authentication will be in effect.

For IBM i customers who have created their own Initial Programs for user profiles, you can easily call the Townsend Security logon initial program from your own application to implement 2FA logon security.

Security administrators can choose one of two options for 2FA failures:

1. Immediately log the user off

2. Disable the user profile and log the user off

When activating 2FA security, security administrators have the option of using a “Preview” mode. When in

preview mode a user will be prompted for two factor authentication, but a 2FA failure will not prevent them from continuing to their normal application. They will have the ability to contact the security administrator and resolve any problems. Once in normal 2FA activation mode, 2FA failures will not allow use of the system.

IBM i Application Program Interfaces for Two Factor Authentication

Many IBM i customers want to implement Two Factor Authentication for critical or sensitive application functions. You might want to use 2FA when financial transactions are above a certain amount. Or you might want to use 2FA when critical system restore functions are initiated. For any sensitive application requirement you can call the Alliance Two Factor Authentication API to force a 2FA sequence. Your application will receive notification of the success or failure of the 2FA operation and can take appropriate action.

Web Applications and Two Factor Authentication

IBM i web applications can also perform Two Factor Authentication by using the Alliance 2FA application program interfaces. Java, RPG, and other web application languages can easily call the application program interfaces to retrieve the valid phone numbers for a user, then perform authentication. If authentication fails, the web application can take the appropriate steps to prevent access.

Meet PCI DSS Compliance

Companies are increasingly required to secure their network access with two-factor authentication. Two factor authentication meets specific access controls standards such as those specified within the PCI DSS.
The requirement states:

8.3 Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (For example, remote authentication and dial- in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication.)

Security Logging

Alliance Two Factor Authentication performs two levels of security logging:

1. Application configuration

2. Authentication failures

All changes to the configuration of Alliance Two Factor Authentication are logged to the IBM security audit journal, QAUDJRN, providing a non-modifiable audit trail. Additionally, when a user fails to enter a valid two factor authentication code, this security failure is also logged to the IBM security audit journal.

In addition to the logging performed by the Alliance Two Factor Authentication solution, IBM i users can implement both object level auditing and user level auditing to record access to 2FA configuration functions.

IBM i customers using the Alliance LogAgent solution can immediately move all IBM i security audit journal entries to a log collection server or SIEM solution for active monitoring of the IBM i platform.

syncsort