Multi-Factor Authentication MFA

Overview

Imagine what could happen if someone captures your username and password… With iSecurity/MFA this nightmare disappears / will not become a reality.

Authenticating logins with usernames and passwords alone isn't enough. Systems need more advanced authentication to be sure of a user's identity.

An increasing number of regulations now require Multi-Factor Authentication (MFA), an authentication method with which users can connect more safely. Since July 2018, for example, the PCI-DSS 3.2 standard has required that anyone signing in to systems that handle credit card data must authenticate using MFA.

MFA requires authentication by a combination of:

- Something that the user knows (Knowledge). This can be the person's IBM i user profile name and password.
- Something that the user has (Possession), such as a smartcard, smartphone or YubiKey. To verify that a user has a smartphone, for example, MFA can send a time-based one-time password via SMS or email, or by splitting the password between the two.
- Something that the user is (Inherence), as proven via fingerprints or other biometric information.

The authentication factors and devices used can vary among users. Some might use a fingerprint scanner on their PC. Some might use facial recognition on a mobile device. Others might prefer a YubiKey.

Until recently, companies worked hard to implement this factor by themselves, without agreement on a standard. In March 2019, the W3C recommended a standard WebAuthn Level 1, also known as FIDO2.

The Multi-Factor Authentication Solution

The iSecurity/MFA interface is straightforward and effective without being overly complex. The process won't frustrate end users or slow them down. MFA can be activated for only those users who require it, such as administrators and people who handle sensitive data.

Administrators can always see a list of active sessions that use MFA. A command can also check whether a job can only run under MFA, providing extended verification of the security that it requires.

For each login session for each user who requires Multi-Factor Authentication, iSecurity MFA provides:

- Logs of activity
- Commands entered during the session
- Database activities done during the session, displaying the Before and After information for all affected fields
- Recordings of all screens that the user has seen during the session (produced by iSecurity Capture)

When the user signs off, iSecurity/MFA automatically produces a session summary including all the collected information. The summary is saved for future auditing and can be automatically sent by email. A comprehensive query generator with a report scheduler can also be used on the data.

Regulations and proper business procedures require solid security and verification. By combining Knowledge (what the user knows), Possession (what the user has), and Inherence (who the user is) with the latest standards, iSecurity/MFA verifies that users are who they say they are and keeps your data safe.

Normal Login

(Option 1) Token / OTP

(Option 2) Biometrics

Key Features

- MFA for IBM i
- Composes
  - Something user knows (Knowledge)
  - Something user has (Possession)
  - Something that the user is (Inherence)
- Supports PCI-DSS 3.2 standard
- WebAuthn Level 1 (known as FIDO2)
- Straightforward end user interface
- Full online administrators control
- Full logs of activity
- Automatic summary of each session, including:
  - Commands entered during the session
  - Database activities done during the session, displaying the Before and After information for all affected fields
  - Recordings of all screens that the user has seen during the session (produced by iSecurity Capture)