WHITE PAPER

Multi-Factor Authentication for IBM i

How We Got Here

The basic IBM i password policies that served in years past are no longer sufficient. Security breaches caused by passwords stored in unsecured locations (such as written on sticky notes), guessed passwords, or brute-force password attacks have compelled IT shops to implement stronger password management controls. Fear of such breaches, coupled with best practices and regulatory requirements, have driven companies to adopt multi-factor authentication (MFA) procedures that require users to enter an additional form of identification beyond passwords, especially when accessing systems that hold valuable or sensitive data.

Compliance Regulations and the Push for Multi-Factor Authentication

Today an ever-growing number of compliance regulations that affect the retail, banking/finance, healthcare, and other industries are either mandating or strongly recommending that companies implement MFA. These regulations include:

- **PCI DSS**—The Payment Card Industry (PCI) Standards Council defines the Data Security Standard (DSS) that companies handling credit card information must meet. PCI DSS 3.2 calls for all users connecting remotely to the CDE be secured by MFA, including administrators, general users or outside vendors. It also requires that all administrators attempting non-console access to the cardholder data environment (CDE) provide multiple factors of authentication. In the past, MFA was required only for any remote access to the CDE, but the new requirement means any administrative access via internal networks must also be validated with MFA. At some companies, this could include quite a few people because a typical IBM i environment has several user profiles that are technically at the administrator level and who can access the CDE—for instance, anyone with *SECADM or *ALLOBJ authority.

- **23 NYCRR 500**—Many financial and insurance institutions are required to meet the requirements defined by the State of New York Department of Financial Services in its cybersecurity regulation that covers companies providing financial services within the state. The regulation applies to institutions that do business in New York, regardless of where they are headquartered. Section 500.12(b) of the regulation states: "Multi-Factor Authentication shall be utilized for any individual accessing the Covered Entity's internal networks from an external network, unless the Covered Entity's CISO has approved in writing the use of reasonably equivalent or more secure access controls."
- **FFIEC**—The Federal Financial Institutions Examination Council (FFIEC) provides guidance for the use of MFA in an Internet-banking environment, providing minimum expectations for authentication of "high-risk" online transactions involving customer access to critical information and/or movement of assets. Specifically, it states: "The agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties."
- **And Others**—There are more compliance regulations that mention or imply the benefits of MFA, including HIPAA, Swift Alliance Access, GDPR, SOX, GLBA, and others.

Perhaps your company isn't being pushed by compliance regulations to implement MFA today, but the odds are good that it will be in the not-too-distant future. Even without a regulatory mandate, security best practices would have you consider adding this technology to further protect sensitive data from being accessed in an unauthorized manner. Given the significant cost and disruption of a breach, it is the prudent thing to do.

How Multi-Factor Authentication Works

MFA requires a user to authenticate with at least two different pieces of evidence (beyond a user name) that prove one's identity. In order to qualify as MFA, these pieces of evidence must come from two of the following three categories, known as authentication factors:

- Something the user knows (e.g.: password, PIN, passphrase)
- Something the user possesses (e.g.: email account, smartphone, code-generating device)
- Something inherent to the user (e.g.: fingerprint, iris scan, voice recognition)

Because MFA requires users to provide at least two authentication factors, the chances of a hacker gaining access to a system is substantially reduced. In other words, there is a very low likelihood that a hacker could both guess/find/steal a user's password and obtain the use of the second authenticating factor—for instance, the user's smartphone that receives an authentication code.

It is also important to emphasize that a second use of the same authentication factor doesn't constitute MFA. In other words, having users provide the answer to a security question or enter a PIN once their password is validated only amounts to single-factor authentication because the user is providing two forms of the same type of authentication factor: something they know. To be true MFA, a user must provide two or more of the different authentication factors that were just mentioned—for instance, something the user knows (such as a password) and something the user possesses (such a code delivered thorough their smartphone).

Multi-Factor Authentication and Two-Factor Authentication: What's the Difference?

Two-factor authentication (2FA) is a term that is often used interchangeably with MFA, and various compliance regulations use this term instead of MFA. However, the difference between MFA and 2FA is that 2FA refers to the use of two authentication factors only, while MFA refers to the use of two or more authentication factors.

Single-Step vs. Multi-Step Authentication

Depending on how the MFA solution is designed, it could be configured to ask the user for authentication factors in a single step (single-step authentication) or in multiple steps (multi-step authentication). Single-step authentication prompts the user for all authentication factors on a single screen or window and then typically validates all factors at one time. Multi-step authentication prompts for one authentication factor on one screen or window (such as password) and, if accepted, then prompts the user to provide the next authentication factor on another screen or window.

There are various reasons companies might use each, but multi-step authentication is considered to be less secure since it reveals that the first factor was correct if the user is prompted for the subsequent authentication factor. Single-step authentication is the most secure route as long as it validates both factors at the same time, and should the login fail, it doesn't tell the person who is logging in which authentication factor failed. In other words, no useful information is divulged to a would-be hacker. Because of this, many entities don't consider multi-step authentication to be true MFA. For instance, PCI DSS regulations recognize only single-step authentication to be a valid form of MFA, and then only if it is implemented in such a way that the user can't see the cause of a login failure should one occur.

Secondary Authentication Factors and Methods

Let's look more closely at the two authentication factors and methods that are used beyond the first authentication factor (which is usually something known, like a password).

Something That the User Possesses

Through the use of a landline phone, a smartphone, email, or a special hardware device, a second factor of authentication is in most instances delivered as a special code (sometimes referred to as a token). In order to prevent codes from being saved and reused, they are typically created in a way that they can be used only once and will expire if not used within a set period of time. The code is usually generated via a separate authentication system or third-party authenticator service (more about these services in the next section). The most common methods for the delivery of codes are:

- **Smartphone app**—A variety of mobile authenticator smartphone apps exist that interface to the system to be accessed and generate single-use codes.
- **Email**—Codes are sent to the user's email address. For this method to be secure, it is essential that users have a different login for email than for the IBM i.
- **Telephone call to landline or mobile number**—Codes are sent as an audio message to one or more designated phone numbers associated with a user.

- **SMS/text message**—Codes are sent by text message to a designated mobile phone. Although this continues to be a common way to deliver codes, a number of recent high-profile hacking incidents involving this method is causing many agencies, including the National Institute of Standards and Technology (NIST), to discourage the use of this method.
- **Special hardware devices**—Usually in the form of a small device that can be attached to a key ring, these have a range of features and methods for delivering authentication codes. Some are as simple as showing a code on a small screen on the device, which is then entered by the user. Hardware-specific delivery of codes is more secure than delivery by telephone, smartphone app, or email. However, this method can be costlier to deploy and, like smartphones, these devices can be lost or stolen.

Something That's Inherent to the User

In some organizations, the secondary or even the tertiary factor of authentication is made through something that is inherent to the user, such as fingerprint, iris scan, face recognition, etc. Depending on the method used, the cost of implementing this as a factor of authentication can be high, so it is mostly used by organizations that have particularly sensitive data.

Authenticator Services

The special authentication code that is generated for the user can come from a variety of sources, depending on the authentication method and level of security needed. Some examples of third-party authenticator services that can integrate with IBM i MFA solutions to supply authentication codes include:

- **RADIUS**—Generates codes for a variety of computing platforms within an organization via a special enterprise server.
- **RSA SecurID**—Provides codes using hardware or software, or on demand via smartphone. Generates a one-time code that expires in 60 seconds. This solution can be optionally coupled with a user's PIN.
- **Authy from Twilio**—Installs on a mobile device or in a browser and provides time-based, single-use codes on demand. Doesn't require a cell connection because it works through a standalone mobile app. Can also deliver codes to a mobile or landline phone.
- **TeleSign**—Provides authentication codes by mobile and voice.
- **YubiKey**—Provides codes via a thumb-drive device.

It should be noted that some MFA software offerings provide their own authentication code–generating functions, but these are generally utilized only in low-risk environments.

MFA is Integrated with IBM i Processes in Various Ways

Multiple third-party vendors, with Syncsort among them, provide MFA solutions for IBM i, and IT shops often choose to buy and implement one of these rather than going to the trouble to create their own. Regardless of whether the MFA solution comes from a third party or is developed in-house, it is important that it provide flexibility in how MFA is invoked since users access the IBM i from different places and processes.

The most common way MFA is presented to users is from the 5250 sign-on screen a user sees when logging onto a system. Nonetheless, you may not need to require MFA for all users or in all situations. For this reason, your MFA solution should provide the ability either to select individual users or groups of users that require MFA or to define specific situations in which users require MFA. And it should go a step further by allowing you to set a variety of rules for when MFA is invoked; for instance, you may want to enable or disable MFA based on special authorities, IP addresses, device type, dates/times, and a variety of other criteria.

Your solution should also provide a way to integrate MFA into your IBM i applications and processes at a granular level. In some cases, you might want to invoke MFA when a user accesses a sensitive application, and/or you might want to trigger MFA when a user is about to change sensitive data. For some IBM i shops, it is also important to have the ability to integrate MFA into web applications.

Logging MFA Activity

Like other security-related IBM i operations in which it is important to log activity, it is essential that your MFA application also provide comprehensive logging. A secure file or journal (such as QAUDJRN) is often utilized to provide an audit trail that cannot be altered. Of course, if your enterprise uses a SIEM console to capture enterprise-wide security events, you'll want to integrate the logging from your MFA solution with your SIEM solution.

There are two different types of events that should be logged: MFA application configuration changes and MFA authentication failures.

- **Logging MFA Application Configurations**—Object-level auditing and user-level auditing should be in place to record any changes to MFA configuration functions.
- **Logging MFA Authentication Failures**—Not only should authentication failures be logged but, in some cases, it might be important for administrators or security officers to receive alerts when failures occur. Some MFA solutions provide the ability to automatically disable user profiles in the event of certain kinds of MFA authentication failures.

Additional Functions That Incorporate MFA

Some MFA solutions provide added functionality that can be used in specialized situations:

- **The "Four Eyes" Principle for Supervised Changes and Operations**—For operations that could have significant risk or for data changes that are so sensitive they must be supervised by another person, some MFA offerings provide the ability to enforce what is called a "four eyes" policy. Here's how it works: when a user wishes to perform a sensitive change or operation, a designated administrator receives an email with a single-use code along with information on the identity of the user making the request. The administrator can then enter the code into the user's screen and observe the change or operation while it is being made.
- **Self-Service Profile Re-Enablement and Password Changes**—Multi-factor authentication technology can be used to help users re-enable their profiles or change a forgotten password without the intervention of an administrator, thus freeing administrators to focus their time on other priorities. For instance, a user can answer preconfigured security questions and/or receive a single-use code via pop-up window, email, or hardware device before making changes to their profile.

Syncsort Can Help

MFA is a powerful technology for protecting sensitive data from being accessed by external and internal actors with bad intentions, and there are numerous approaches and features to consider when choosing an MFA solution that's best for your organization. This is why it's important to work with a trusted company to deliver an adaptable MFA solution that will work seamlessly with your IBM i environments and that is backed by expert services and responsive support. Having brought together the top security solutions in the industry, Syncsort provides end-to-end security solutions and services for IBM i, including powerful options for MFA that support a range of authentication services. Let our team of IBM i security experts help you solve your MFA needs.

Learn more at www.syncsort.com.

About Syncsort

Syncsort is the global leader in Big Iron to Big Data software. We organize data everywhere to keep the world working – the same data that powers machine learning, AI and predictive analytics. We use our decades of experience so that more than 7,000 customers, including 84 of the Fortune 100, can quickly extract value from their critical data anytime, anywhere. Our products provide a simple way to optimize, integrate, assure and advance data, helping to solve for the present and prepare for the future. Learn more at syncsort.com.

syncsort