Introducing IBM Z Multi-Factor Authentication 2.1

Now expanded across z/VM operating system, and beyond the boundary of a Sysplex cluster

Mainframe systems are the foundation of trusted digital experiences for most of the world's largest companies and organizations. But, passwords protecting critical users, data and applications are a relatively simple point of attack for hackers to exploit because passwords rely on user education and compliance for both implementation and control. Using a variety of methods such as social engineering and phishing, criminals have exploited employees, partners, and general users to hack into even the most secure platforms.

IBM Z Multi-Factor Authentication 2.1 (IBM Z MFA) raises the level of assurance of your mission-critical systems with expanded authentication capabilities and options for a comprehensive, user-centered strategy to help mitigate the risk of compromised passwords and system hacks. Our designers are also IBM Z MFA users. Across every new version, we incorporate their growing knowledge and expertise of real-world mainframe security scenarios.

A layered defense for mission critical workloads

The IBM Z MFA solution implements multiple authentication factors and is tightly integrated with IBM z/OS Security Server RACF programs to help create a layered defense beyond simple password authentication. These factors generally include:

- *Something they know* – Such as a password or security question
- *Something they have* – Such as an ID badge, a cryptographic token device, or a one-time code sent to their phone or email
- *Something they are* – Such as a fingerprint or other biometric attribute

Highlights

- Expanded across z/VM operating system
- Supports production of secure credentials within and beyond the Sysplex boundary
- Extensive integration with RACF
- RSA SecurID, Gemalto SafeNet, and generic RADIUS factor support
- Compound in-band and out-of-band support
- Native Yubikey support
- IBM Cloud Identity Verify integration
- IBM Security Access Manager integration

IBM Z MFA Advantages

IBM Z Multi-Factor Authentication provides key advantages including, short time to value and low total cost of ownership (TCO), flexible authentication options, strong security, and more:

Short time to value and low total costs of ownership

- Tight, direct RACF integration lets customers set up in as little as a day when installed by experienced system programmers, as compared to weeks or even months with other solutions
- Simple integration with existing IBM Z MFA infrastructure, including access control and authentication (token) systems management interfaces
- Easy authentication management, wherein RACF personnel can administer with a minimal learning curve, thanks to a consistent set of commands and interfaces
- Saves time for integrating critical legacy applications that aren't MFA-aware but need to be secured
- Delivers self-service password change capabilities to help cut back on help desk calls
- Provides scalability and performance, with an extensible architecture that allows it to grow with clients
- Resides on and written for the mainframe, making it easier and less complex for mainframe staff to manage mainframe security

Support for popular authentication factors and protocols

- RSA SecurID hard and soft tokens
- IBM TouchToken app for Time-based One-Time Passwords (TOTP) PassTicket support and application-level granularity
- Smartcard certificate-based authentication (PIV/CAV and more) Generic RADIUS (works with generic RADIUS servers)
- SafeNet RADIUS (works with Gemalto SafeNet Authentication Service Servers) RSA SecureID RADIUS
- Generic TOTP (works with generic TOTP token applications, including standard-compliant TOTP third-party applications on Android and Microsoft Windows devices)
- Yubico Yubikey tokens capable of generating one-time passcodes using Yubico's OTP algorithm.
- IBM Security Access Manager (ISAM) Integration
- IBM Cloud Identity Verify Integration

Strong security

- Reduced potential points of failure: A native mainframe solution written in standard programming languages and specifically designed for mainframe environments; no “leaky” Windows-based proxies or Java code
- Integrated with RACF: Stores all MFA configuration information within the RACF database
- Improved access control: Administrators can specify a mix of authentication factors down to the individual user level, not just groups or domains

High levels of scalability

- IBM Z MFA can scale to hundreds of thousands of authentication requests per second, making it suitable for high-throughput business transaction, e-commerce back-end, or machine-driven environments

Tight RACF support

- Integrates closely with z/OS Security Server RACF and centralizes authentication factor information in the RACF database
- Relies on the RACF Security Administrator to identify users subject to MFA policy
- Works with RACF define policies for the authentication factors, apply them to specific IDs, and authenticate users
- Provides extensions to RACF for auditing and provisioning

Flexible Authentication

- Enables clients to add one or more authentication factors for IBM z/OS systems
- Provides built-in support for popular authentication tokens and protocols, as listed above Includes PIV and CAC card support
- Includes support for application bypass
- BM HTTP Server Powered by Apache integration

Compliance facilitation

- Provides the most complete IBM Z MFA solution, and helps installations meet compliance standards such as PCI, DFARS 800-171, NIST.SP.800-171, and HSPD-12. For example, it enables the configuration of Multi-Factor Authentication in a strict PCI-compliant mode.

Key authentication capabilities

IBM Z MFA also supports the following capabilities:

- Running multiple instances of the Multi-Factor Authentication Web Services started task in a sysplex

- Integration through an SAF API that enables Express Logon Facility to work with Multi-Factor Authentication
- Compound authentication, which allows the specification of more than one authentication factor in the authentication process
- Compound in-band authentication, which requires the user to supply a RACF credential (password or password phrase) in conjunction with a valid MFA credential
- RACF Identity Tokens (JSON Web Tokens support), where a set of authentication API calls can be linked together to appear as a single authentication transaction

IBM Z MFA 2.1 Highlights

Extended to z/VM External Security Managers

IBM Z MFA adds support for strong user authentication to z/VM systems protected by IBM z/VM 7.1 RACF:

- A separate installation of IBM Z MFA (IBM Z MFA for z/VM) is installed on an LPAR running a supported distribution of Linux for IBM Z.
- MFA user accounts associated with z/VM users are configured and maintained within IBM Z MFA for z/VM.
- Entries for z/VM ESM clients are configured within IBM Z MFA for z/VM.
- The user initially authenticates to IBM Z MFA for z/VM to acquire a secure credential, and then uses that credential instead of their z/VM password when accessing their protected z/VM system.

Protection beyond the z/OS sysplex boundary

IBM Z MFA adds supports to produce secure credentials that can be used both within and beyond the boundary of the Sysplex where the credential was generated.

- The user is configured via familiar IBM Z MFA techniques in the primary (credential generating) system or Sysplex.
- The user is configured to require a new AZFCKCTC factor in multiple secondary (consuming) systems or Sysplexes.
- In secondary (consuming) environments, the AZFCKCTC factor is configured to direct credential processing toward IBM Z MFA Web Services APIs hosted in the primary (generating) environment.

Why IBM?

IBM Security Services professionals can offer virtually unparalleled IAM expertise, broadened by their access to IBM's research and development team. Available worldwide, IBM specialists can tailor their recommendations to your region's unique circumstances. Their approach to IAM strategy and assessment examines impact at every level of your organization—from business strategy to applications to IT infrastructure — to help you implement an IAM program designed to meet your business and IT objectives.

For more information - IBM

To learn more about IBM Identity and Access Management Services for identity and access strategy and assessment, please contact your IBM representative or IBM Business Partner, or visit the following website: ibm.com/services/security

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: ibm.com/financing

---