IBM Z Multi-Factor Authentication 2.3

Enhance logon security with extended mainframe user and token authentication, now with SSO support

Highlights

Short time to value and low cost of ownership

Support for popular authentication factors and protocols

Strong Security

High levels of scalability

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 2.3 (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.

The latest version of IBM Z MFA brings a host of new features such as single sign-on support for OIDC-compliant tokens, user-driven fallback voting, Search Before Bind user provisioning for LDAP authentication and more.

"Thanks to IBM Z MFA we can now support very flexible authentication options more easily. These new, cutting-edge login capabilities enhance the security for our tax applications without substantial changes in costs for us."

Kurt Garner
ICT System Engineer
Abraxas Informatik AG[1]

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 (Resource Access Control Facility) 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

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

- Generic RADIUS (works with generic RADIUS servers)
- Single sign-on support for tokens issued by external OpenID Connect (OIDC)-compliant identity providers
- Generic Time-based One-Time Passwords (TOTP)
- Smartcard certificate-based authentication (PIV/CAV and more)
- Lightweight Directory Access Protocol (LDAP) authentication (LDAP Simple Bind)
- Yubico Yubikey tokens capable of generating one-time passcodes using Yubico's OTP algorithm
- RSA SecurID hard and soft tokens & PassTicket support and application-level granularity
- SafeNet RADIUS (works with Gemalto SafeNet Authentication Service Servers) RSA SecureID RADIUS
- IBM Security Verify integration

7000

Number of users that Abraxas Informatik AG has enabled single sign-on for without having to manually update any of their individual programs[1]

Learn more

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

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
- 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

*Fully supports ACF2™ and Top Secret®

IBM Z MFA Recent Updates

IBM Z MFA 2.3 Highlights

Now with support for a new single sign-on pattern:

- Single sign-on support for tokens issued by external OIDC-compliant identity providers
- User-driven password fallback voting
- Remote CTC checking
- Search Before Bind user provisioning for LDAP authentication
- In-memory storage of IBM Z MFA-issued CTCs

IBM Z MFA 2.2 Highlights

Enhances authentication modes and support to strengthen enterprise security:

- Pluggable authentication modules
- Configuration of multiple instances of select MFA factors
- Addition of a “Console Modify” command
- Documentation and formal support for customer use of policy authentication
- MFA configuration option to request that browser clients receiving cache token credentials mask the display of such credentials
- Support for RSA SecurID authentication
- Web-based ESM password reset feature

For more information
To learn more about IBM Z Multi-Factor Authentication, contact your representative or IBM Business Partner, or visit https://www.ibm.com/z/security

1. “Boosting IT security and simplifying user management” https://www.ibm.com/case-studies/abraxas-informatik-ag

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
July 2024