IBM Z Multi-Factor Authentication V2.0

Go beyond passwords for authentication and to meet compliance needs.

Highlights

- Deep integration with RACF
- RSA SecurID, Gemalto SafeNet, and generic RADIUS factor support
- Compound in-band and out-of-band support
- Native Yubico support
- IBM Cloud Identity Verify integration
- IBM Security Access Manager integration

Mainframe systems are the foundation for trusted digital experiences for the world's largest companies and governments. 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 security controls. Using a variety of methods such as social engineering and phishing, criminals have exploited employees, partners and general users of corporate systems that require passwords to hack into the even the most secure platforms.

IBM Z Multi-Factor Authentication v2.0 (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 IBM Z system hacks. IBM Z MFA was designed for IBM Z users, by IBM Z users, and encapsulates the knowledge and expertise of real-world mainframe 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. By requiring multiple authentication factors, user accounts are much, much harder to compromise. 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 MFA provides key advantages that include short time to value, flexible authentication options, low total cost of ownership (TCO), and more.

Short time to value

- 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

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

Low TCO

- 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

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
- IBM 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 V2.0 Highlights

IBM Security Access Manager (ISAM) integration:

In addition to the existing factor support, IBM Z MFA V2.0 adds support for ISAM integration:

The user initially authenticates to ISAM, uses the “pick-up One-Time Passcode (OTP) procedure,” and then uses that OTP instead of their password when logging on to z/OS

- The ISAM integration supports compound in-band authentication, where the ISAM-generated OTP can be used in conjunction with the user's RACF password or passphrase

- The user initially authenticates to ISAM, uses the “pick-up One-Time Passcode (OTP) procedure,” and then uses that OTP instead of their password when logging on to z/OS
- The ISAM integration supports compound in-band authentication, where the ISAM-generated OTP can be used in conjunction with the user's RACF password or passphrase

IBM Cloud Identity Verify integration:

In addition to the existing factor support, IBM Z MFA includes CIV integration using the CIV RADIUS gateway and IBM Z MFA generic RADIUS protocol factor:

- The user initially authenticates to z/OS using their Cloud Identity Verify password
- A RADIUS challenge is returned, asking the user to provide their Cloud Identify Verify credential which may be an OTP delivered by SMS or email, or a TOTP token from the IBM Verify mobile application
- The Cloud Identity Verify integration supports compound in-band authentication, where the Cloud Identity Verify-generated OTP can be used with their RACF password or password phrase

Native Yubico OTP support:
IBM Z MFA delivers support for a variety of Yubikey devices that support the Yubico OTP algorithm. This does not require an external authentication server, and all OTP evaluation is performed on the z/OS system by the IBM Z MFA started task.

LDAP simple bind support:
IBM Z MFA supports authenticating to a variety of LDAP servers, such as Microsoft Active Directory, using an LDAP simple bind.

Self-service password change:
The out-of-band server provides a generalized RACF password change.

Policy-first out-of-band pre-authentication workflow:
The out-of-band pre-authentication workflow has been improved in IBM Z MFA 2.0 to require the end user to supply the policy name before the user ID and other credentials, either by entering the policy name into a web form or by navigating to a bookmarkable web address. The end user then enters the user ID and relevant credentials to obtain a Cache Token Credential.

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors more than one trillion events per month in more than 130 countries, and holds more than 3,000 security patents.

Next steps

→ Learn about IBM mainframe security

→ Watch the Rise of MFA webcast

For more information

For more information about IBM Z Multi-Factor Authentication and mainframe security contact your IBM representative or IBM Business Partner.

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