IBM Multi-Factor Authentication for z/OS V1R3

Highlights

- A generic RADIUS factor that enables interoperability with generic RADIUS servers
- A SafeNet RADIUS factor that is designed to operate with Gemalto SafeNet Authentication Service servers
- An RSA SecurID RADIUS factor that is optimized to communicate with RSA Authentication Manager servers using the RADIUS protocol
- Generic TOTP
- Compound In-band Authentication
- Support for IBM Express Logon Facility
- Bulk provisioning
- Strict PCI compliance mode
- Enables deep integration with the Resource Access Control Facility (RACF)

Attacks on computer systems have been increasing in sophistication and persistence. Companies have concerns about privileged insider abuse, misconfiguration, down-level maintenance and defects in privileged code, which can create exposures and potential attack vectors.

Companies are required to comply with ever-increasing, rigorous compliance and regulatory requirements, but assessor skills are lacking, and some are not familiar with IBM® z Systems®, raising the difficulty and expense of audits.

Passwords are a relatively simple point of attack for hackers to exploit. For systems that rely on passwords to be secure, they must enforce password controls and provide user education. Users tend to pick common passwords, write down passwords and unintentionally install malware that can key log passwords. Companies are looking for ways to raise the assurance level of their systems by requiring additional authentication factors for users.

IBM Multi-Factor Authentication for z/OS® (IBM MFA) raises the level of assurance of IBM z/OS systems by requiring users to authenticate with multiple authentication factors during the logon process. The main support components for MFA on z/OS are IBM MFA for z/OS and the Resource Access Control Facility (RACF) enablement infrastructure.

RACF is enhanced to provide an infrastructure that enables IBM MFA for z/OS to integrate directly with the security server. This MFA solution is designed to be very flexible because it is not locked to any particular authentication factors. As new authentication factors become available, they can be added to MFA for z/OS without requiring changes to the RACF MFA infrastructure.

MFA for z/OS raises the level of assurance of mission-critical systems with a flexible and tightly integrated solution. MFA for z/OS and the RACF security server infrastructure creates a layered defense by requiring selected z/OS users to log on with more than one authentication factor including:

- Something they know, such as a password or security question
- Something they have, such as an ID badge or cryptographic token device
- Something they are, such as a fingerprint

By requiring multiple authentication factors, users' accounts cannot be compromised, even if one of their factors is discovered.

RACF MFA support introduces extensions to a variety of components of RACF user-related commands. It allows the provisioning and definition of acceptable MFA tokens for a user and supports command extensions for MFA.

- Extensions to the Security Authorization Facility (SAF) programming interfaces allow supported tokens to be specified during user authentication requests, which enables MFA-aware applications to allow the specification of factors in addition to a RACF password or password phrases.
- Auditing extensions track which factors are used during the authentication process for a given user.

Multi-Factor Authentication for z/OS, V1.3 (IBM MFA) is enhanced with new functionality and support.

New RADIUS-based factors

In addition to the existing RSA SecurID support, IBM TouchToken support, and Personal Identity Verification and Common Access Card support, IBM now includes support for three new RADIUS-based factors:

- A generic RADIUS factor that enables interoperability with generic RADIUS servers
- A SafeNet RADIUS factor that is designed to operate with Gemalto SafeNet Authentication Service servers
- An RSA SecurID RADIUS factor that is optimized to communicate with RSA Authentication Manager servers using the RADIUS protocol

Generic TOTP support

The time-based, one-time password factor has been enhanced to support more generic TOTP token applications. This introduces support for standard-compliant TOTP third-party applications that run on Android and Microsoft Windows devices.

Compound In-band Authentication support

In some cases, it may be desirable to authenticate with both an IBM MFA credential and a RACF password. If this support is activated, the user enters their token code and their RACF password or password phrase into the password phrase field of applications.

IBM MFA Express Logon Facility support

New integration has been provided, through a new SAF API, that enables Express Logon Facility users to interface with the IBM MFA smart card support. This enhancement requires the presence of a user's smart card when authenticating. It prevents RACF user ID-only authentication attempts.

High-Availability IBM MFA Web Services support

IBM MFA now supports running multiple instances of the IBM MFA Web Services started task in a sysplex. Thus, if an LPAR running IBM MFA Web Services must be rebooted or is otherwise out of service for planned maintenance, users can continue to pre-authenticate with IBM MFA Web Services on one of the remaining instances running within the sysplex. Additionally, this eliminates the need to explicitly configure the host name of the LPAR for IBM MFA Web Services and IBM TouchToken registration.

Bulk provisioning support

IBM MFA now includes scripts that enable a large number of users to be easily provisioned. In particular, this simplifies provisioning PIV/CAC users who can be provisioned and enabled immediately, eliminating the self-service provisioning step available in IBM MFA V1.2. Note that the self-service provisioning capability is still available for sites that are unable to use the new bulk provisioning capability.

Strict PCI compliance support

IBM MFA now includes the ability to configure IBM MFA to operate in a strict PCI-compliant mode. When this mode is activated, messages that "leak" information are not returned, and the out-of-band pre-authentication process always requires entry of all factor credential data before returning any information about the pre-authentication attempt.

Where are workloads that require the utmost security, and are too critical to fail, deployed? Most of the world's largest financial, government and retail institutions use IBM z Systems to run their most mission-critical workloads and to protect their most sensitive data.

IBM z Systems are highly secure servers designed for digital business and are one of the most reliable servers commercially available today. Together, the servers and software offer built-in enterprise-grade security capabilities to help you simplify and improve complex operational security processes.

For more information

To learn more about the IBM Multi-Factor Authentication for z/OS, please contact your IBM representative or IBM Business Partner, or visit the following website: **ibm.com**/systems/z/solutions/security.html

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

IBM Systems
Route 100
Somers, NY 10589

Produced in the United States of America
February 2018

ZSS03139-USEN-04