White Paper

A New Approach to Mainframe Passwords: Get Rid of Them

A New Approach to Mainframe Passwords: Get Rid of Them

Passwords are a corporate necessity. Their job is to ensure that only authorized users can access your most precious commodity—information. Given this critical role, not just any password will do. The ideal password is long and complex. It's different for every application. And it requires regular updates.

Passwords are also a corporate menace. Creating, remembering, and constantly changing passwords puts a burden on users. Trying to manage and enforce password policies puts a burden on IT. Fortunately, modern NetIQ Identity and Access Management (IAM) systems, along with Single Sign-On (SSO), have helped to ease the pain. Users need only log on once to access most of their enterprise resources.

Most, but not *all*. Unfortunately, IAM and SSO don't work with your most critical systems—the ones that actually runs your business. Your mainframe systems.

"Give Us Anytime, Anywhere, Any Device Access to the Mainframe"

Users today expect anytime, anywhere, any device access to all their enterprise resources, including the mainframe. But giving unrestricted access to the mainframe keeps both IT Network Administrators and Mainframe Systems Administrators up at night.

Why? Because when it comes to providing secure access, the network and the mainframe are like two autonomous islands. Each uses its own system for controlling access. Each has its own ruler. And neither ruler wants to relinquish any control of their domain to accommodate the other.

Despite their mutual dependencies and the benefits to be gained by working together, the rulers of each island see no way around the integration obstacles.

Network Island

IT Network Admins have a vested interest in beefing up security for mainframe access because they manage the terminal emulation applications that make access possible. But there's no feasible way to extend the strong network security, featuring strong passwords facilitated by IAM, to Mainframe Island.

Most mainframe applications were written decades ago, in a safer time. Open networks, service-oriented architectures, and malicious hackers didn't exist. Mainframe applications were hard-coded with weak eight-character passwords because that was good enough. Not anymore.

Rewriting your mainframe applications now—even if you somehow stumble upon a still-employed mainframe programmer—is risky, disruptive, and expensive. The only other way to enforce a single password for access to all network resources, including the mainframe, is to dumb down enterprise-wide passwords to eight characters. No one wants to move in that direction.

Mainframe Island

Mainframe Systems Admins know that after decades of being largely ignored by the hacker community, the mainframe now wears a target on its back. They don't have IAM, but they do have RACF or Top-Secret for authenticating and authorizing mainframe access. That's all good, except they're still stuck with weak eight-character passwords.

Much as they'd like to strengthen their passwords—and access control—Mainframe Systems Admins are adamant about one thing: Under no circumstances will they jeopardize the 99.999 percent reliability record of the mainframe. But in their minds, that's exactly what they'd be doing if they tried to integrate mainframe access with network servers on Network Island. And they simply can't afford the constant downtime commonly associated with network security issues.

Mainframe-Password Problems

Capable as they are, mainframes have some quirks that make them odd-man-out in the modern enterprise. One of those quirks is the mainframe application password. Here's why it's a problem:

- **Weak authentication**
  Ask any security expert if they think eight-character, case-insensitive passwords are strong enough to protect sensitive data. The answer will be a resounding "No!" Strict policies are associated with enterprise passwords. But for the reasons stated above, these policies cannot be applied to mainframe access.

Defense-in-Depth with MSS

You can add even more layers of security by pairing MSS with these add-on components:

- **MSS Security Proxy Add-On**
  Deliver end-to-end encryption and enforce access control at the perimeter with patented security technology.
- **MSS Advanced Authentication Add-On**
  Enable multifactor authentication to authorize access to your valuable host systems.
- **MSS Automated Sign-On for Mainframe Add-On**
  Enable automated sign-on to IBM 3270 applications via your identity and access management system.
- **MSS PKI Automated Sign-On Add-On**
  PKI-enable automated application sign-on to your critical enterprise systems.
- **MSS Terminal ID Management Add-On**
  Dynamically allocate terminal IDs based on username, DNS name, IP address, or address pool.

With MSS and its add-on products, there's finally a practical way to modernize mainframe security without any recoding.

- **Risky user behavior**
  In this instant-access era, the extra logon step required for mainframe access is a waste of time for most users. Think about it. Who wants to enter a different password every time you open a new app, especially if you open five or six a day? So users look for convenient workarounds—such as neglecting to log out or leaving their workstations turned on (and unprotected) when they leave.
- **Mainframe password resets—ugh!**
  Users who access multiple applications on multiple mainframes have multiple passwords to remember. No one can do it, so they resort to security no-nos—sticky-note reminders or small password changes at update time. But users do forget, and then their passwords must be reset. Unlike network passwords, mainframe passwords can't be reset by the user. An expensive IT person must stop whatever he or she is doing to perform this mundane and time-consuming task.

From security risks to usability and IT management headaches, logging on to the mainframe with an eight-character password is a practice in need of an update.

How Automated Sign-On for Mainframe Works

Working with the IBM z/OS Digital Certificate Access Server (DCAS), Automated Sign-On for Mainframe obtains a time-limited, single-use R PassTicket for the target application. It returns the mainframe user ID and the PassTicket to the terminal emulator's logon macro, which sends the credentials to the mainframe to sign on the user to the application.

The Bridge to Security Happiness

Our two islands have not evolved in parallel. On Network Island, security for accessing enterprise applications has grown stronger to meet increasingly sophisticated threats. On Mainframe Island, the security written into those decades-old critical applications has stood still for decades.

Fortunately, there's finally a way to extend strong, centrally managed security to your mainframe applications—without jeopardizing business operations. It's called OpenText™ Host Access Management and Security Server (MSS). MSS integrates your mainframe with your IAM system, building a bridge between the two islands.

More specifically, MSS works with your IAM system to centrally manage and secure mainframe access via your Micro Focus terminal emulators. Sitting between the user and the mainframe, it uses your existing LDAP authentication structure to validate a user's credentials before granting mainframe access. In other words, users can't get near the host logon screen until they've been authenticated and authorized with strong IAM credentials—that is, strong, complex passwords.

Teamed with one of its add-on components—Automated Sign-On for Mainframe—MSS also eliminates the need for mainframe passwords. That's right. Users no longer need to take the additional step of entering a password to log on to their mainframe applications after authenticating to MSS. MSS handles that for them. It's a win-win solution for users—no more risky eight-character passwords to remember—and security-conscious IT—who can finally get out of the password-management game.

MSS can be installed on a server or on the mainframe—whatever works best for your business. It provides a flexible, scalable, highly secure solution for mainframe access that eliminates the need for mainframe passwords.

Safe, Manageable, and Economical

Once upon a time, your valuable mainframe data traveled a protected path to and from a trusted terminal. Not anymore. Today, shielding it from bad guys on the Internet highway requires the strongest protection there is. It's time to leave weak eight-character passwords in the past where they belong. Instead, build a bridge to the strongest authentication there is, ensuring that only authorized users can access your most valuable data. MSS offers a safe, manageable, and economical way to do it.

Learn more at
www.microfocus.com/opentext

Connect with Us

OpenText CEO Mark Barrenechea's blog

opentext™